



Bundesministerium
des Innern

Deutscher Bundestag
Untersuchungsausschuss
18. Wahlperiode

MAT A BMI-1/7k-8

zu A-Drs.: 5

POSTANSCHRIFT

Bundesministerium des Innern, 11014 Berlin

1. Untersuchungsausschuss 18. WP
Herrn MinR Harald Georgii
Leiter Sekretariat
Deutscher Bundestag
Platz der Republik 1
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
POSTANSCHRIFT 11014 Berlin

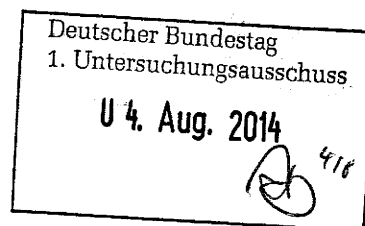
TEL +49(0)30 18 681-2750
FAX +49(0)30 18 681-52750

BEARBEITET VON Sonja Gierth

E-MAIL Sonja.Gierth@bmi.bund.de
INTERNET www.bmi.bund.de
DIENSTSITZ Berlin
DATUM 1. August 2014
AZ PG UA-200017#2

BETREFF
HIER
ANLAGEN

1. Untersuchungsausschuss der 18. Legislaturperiode
Beweisbeschluss BMI-1 vom 10. April 2014
35 Aktenordner (offen und VS-NfD)



Sehr geehrter Herr Georgii,

in Teilerfüllung des Beweisbeschlusses BMI-1 übersende ich die in den Anlagen ersichtlichen Unterlagen des Bundesministeriums des Innern.

In den übersandten Aktenordnern wurden Schwärzungen oder Entnahmen mit folgenden Begründungen durchgeführt:

- Schutz Mitarbeiterinnen und Mitarbeiter deutscher Nachrichtendienste
- Schutz Grundrechtlicher Dritter
- Fehlender Sachzusammenhang zum Untersuchungsauftrag und
- Kernbereich exekutive Eigenverantwortung.

Die einzelnen Begründungen bitte ich den in den Aktenordnern befindlichen Inhaltsverzeichnissen und Begründungsblättern zu entnehmen.

Soweit der übersandte Aktenbestand vereinzelt Informationen enthält, die nicht den Untersuchungsgegenstand betreffen, erfolgt die Übersendung ohne Anerkennung einer Rechtspflicht.

Ich sehe den Beweisbeschluss BMI-1 als noch nicht vollständig erfüllt an.

Mit freundlichen Grüßen

Im Auftrag

Hauer

ZUSTELL- UND LIEFERANSCHRIFT
VERKEHRSANBINDUNG

Alt-Moabit 101 D, 10559 Berlin
S-Bahnhof Bellevue; U-Bahnhof Turmstraße
Bushaltestelle Kleiner Tiergarten

Titelblatt

Ressort

BMI

Berlin, den

28.07.2014

Ordner

144

Aktenvorlage

an den

**1. Untersuchungsausschuss
des Deutschen Bundestages in der 18. WP**

gemäß Beweisbeschluss:

vom:

BMI-1

10. April 2014

Aktenzeichen bei aktenführender Stelle:

ÖS I 3 - 52000/4#1 Bd. 2 von 2

VS-Einstufung:

VS-NUR FÜR DEN DIENSTGEBRAUCH

Inhalt:

[schlagwortartig Kurzbezeichnung d. Akteninhalts]

ÖS I 3 - 52000/4#1 - Maßnahmen auf EU-Ebene i.Z.m.
„PRISM“ / „Tempora“

Bemerkungen:

Inhaltsverzeichnis

Ressort

BMI

Berlin, den

28.07.2014

Ordner

144

Inhaltsübersicht

zu den vom 1. Untersuchungsausschuss der
18. Wahlperiode beigezogenen Akten

des/der:

Referat/Organisationseinheit:

BMI	ÖS I 3
-----	--------

Aktenzeichen bei aktenführender Stelle:

ÖS I 3 - 52000/4#1

VS-Einstufung:

VS-NUR FÜR DEN DIENSTGEBRAUCH

Blatt	Zeitraum	Inhalt/Gegenstand [stichwortartig]	Bemerkungen
1-446	19.09.2013 - 05.03.2014	Maßnahmen auf EU-Ebene i.Z.m. „PRISM“ / Tempora	VS-NfD: S. 1-6, 155-161, 164-192, 199-202, 223-229, 305-318 Schwärzung: S. 295 (DRI-N) Entnahme: S. 296-304 (DRI- N) Schwärzung: S. 212, 214- 216, 219, 240-242 (BEZ) Entnahme: S. 213, 243 (BEZ) S. 51, 74, 150 Leerseiten drucktechnisch bedingt

noch Anlage zum Inhaltsverzeichnis

Ressort

BMI

Berlin, den

28.07.2014

Ordner

144

VS-Einstufung:

VS-NfD

Abkürzung	Begründung
DRI-N	<p>Der vorliegende Ordner enthält Unkenntlichmachungen von Namen externer Dritter.</p> <p>Namen von externen Dritten wurden unter dem Gesichtspunkt des Persönlichkeitsschutzes unkenntlich gemacht. Im Rahmen einer Einzelfallprüfung wurde das Informationsinteresse des Ausschusses mit den Persönlichkeitsrechten des Betroffenen abgewogen. Das Bundesministerium des Innern ist dabei zur Einschätzung gelangt, dass die Kenntnis des Namens für eine Aufklärung nicht erforderlich erscheint und den Persönlichkeitsrechten des Betroffenen im vorliegenden Fall daher der Vorzug einzuräumen ist.</p> <p>Sollte sich im weiteren Verlauf herausstellen, dass nach Auffassung des Ausschusses die Kenntnis des Namens einer Person doch erforderlich erscheint, so wird das Bundesministerium des Innern in jedem Einzelfall prüfen, ob eine weitergehende Offenlegung möglich erscheint</p>
BEZ	<p>Fehlender Bezug zum Untersuchungsauftrag</p> <p>Das Dokument weist keinen Bezug zum Untersuchungsauftrag bzw. zum Beweisbeschluss auf und ist daher nicht vorzulegen.</p>

Dokument 2014/0067382

Von: BMIPoststelle, Postausgang.AM1
Gesendet: Donnerstag, 19. September 2013 10:39
An: PGNSA
Cc: OESII3_ ; OESIII3_ ; GII1_ ; UALGII_ ; IT3_ ; IDD_
Betreff: BRUEDIP*123: Empörung über großangelegten Hackerangriff bei Belgacom

Vertraulichkeit: Vertraulich

erl.: -1
erl. : -1

-----Ursprüngliche Nachricht-----

Von: frdi [mailto:ivbbgw@BONNFMZ.Auswaertiges-Amt.de]
Gesendet: Donnerstag, 19. September 2013 10:21
Cc: Zentraler Posteingang BMI (ZNV); 'reg.4@bpa.bund.de'
Betreff: BRUEDIP*123: Empörung über großangelegten Hackerangriff bei Belgacom
Vertraulichkeit: Vertraulich

WTLG
Dok-ID: KSAD025508960600 <TID=098535120600>
BMI ssnr=4517
BPA ssnr=1539

aus: AUSWAERTIGES AMT
an: BMI, BPA

aus: BRUESSEL DIPLO
nr 123 vom 19.09.2013, 1017 oz
an: AUSWAERTIGES AMT

Fernschreiben (verschlusselt) an E10
eingegangen: 19.09.2013, 1018
auch fuer BMI, BPA, BRUESSEL EURO, BRUESSEL NATO, DEN HAAG DIPLO,
LUKSEMBURG DIPLO, PARIS DIPLO

013
Verfasser: Margret Pollmeier
Gz.: Pr 312.08/2 191014
Betr.: Empörung über großangelegten Hackerangriff bei Belgacom
hier: deutliche Verdächtigungen gegenüber den USA
Bezug: ohne

-zur Unterrichtung-

I. Zusammenfassung

Nachdem am 16.9. die flämischsprachige Zeitung De Standaard als erste berichtete, dass die amerikanische NSA bereits seit 2011 das Computernetzwerk der Belgacom durch "hacking" infiltriert, gehen die Wogen der Empörung in den belgischen Zeitungen hoch. Nach übereinstimmenden Meldungen von De Standaard, Le Soir, l'Echo, De Tijd und den beiden Metrozeitungen hatte Belgacom bereits am 19. Juli bei der Staatsanwaltschaft Klage gegen unbekannt wegen unerlaubten Zugangs zu ihrem Computersystem erhoben.

Während Belgacom Chef Didier Bellens abwiegele, dass es keinen Hinweis darauf gebe, dass Kundendaten betroffen seien, sehe die Staatsanwaltschaft aufgrund des hohen technischen und finanziellen Niveaus des "hacking" Anzeichen dafür, dass internationale staatliche Spionage dahinterstehe, wobei alle Hinweise Richtung USA deuteten. Am 18.9. erhielt die Affaire eine neue Wendung, da z.B. laut Le Soir und De Standaard Belgacom Chef Didier Bellens den zuständigen Minister für öffentliche Unternehmen

Jean-Pascal Labille (PS) belogen habe, indem er noch am 10. Juli 2013 vorgegeben habe, es gebe bei Belgacom keinen Verdacht auf Datendiebstahl. Die Diskussion dauert an.

II. Im einzelnen:

1. Am 16.9. berichtete De Standaard unter dem Titel "NSA verdacht van hacken Belgacom" dass Belgacom bereits seit 2011 durch "hacking" von der NSA infiltriert sei und dass die Verantwortlichen bei Belgacom schon seit Mitte 2012 darüber informiert gewesen seien. Laut einer in Le Soir und der französischsprachigen Metrozeitung veröffentlichten Chronologie der Ereignisse habe Belgacom im Nachgang der Enthüllungen Edwards Snowdens über die Spionagetätigkeiten der NSA ein niederländisches Spezialunternehmen gebeten, zu untersuchen, ob es Hinweise auf Datendiebstahl bei Belgacom gebe. Dieses Unternehmen habe dann im Juli diesen Jahres das Virus lokalisiert, worauf Belgacom am 19. Juli 2013 Klage gegen unbekannt eingereicht habe. Die Angelegenheit sei geheim gehalten worden, damit das Virus analysiert und entfernt werden konnte, ohne die Hacker zu warnen.
2. Während Belgacom selbst die Angelegenheit herunterzuspielen versuche (z.B. Zitat in l'Echo vom 17.9.: "Le virus a été éradiqué avec succès. Les conséquences seraient minimales"), sehe die Generalstaatsanwaltschaft Anlass zur Besorgnis (z.B. Zitat auch in l'Echo vom 17.9.: "Vu la complexité et l'ampleur du hacking l'enquête s'oriente vers une opération internationale d'espionnage").
3. Alle großen Zeitungen verdächtigen relativ unverblümt die NSA, wobei De Tijd vom 17.9. unter der Überschrift "Ook Israel dreigt Belgacom te bespioneren" auch die israelischen Geheimdienste ins Spiel bringt. Grund für den deutlichen Verdacht gegen die USA ist die Tatsache, dass sich die Hacker v.a. für das weltweite Telekommunikationssystem Bics und hier besonders für Nummern aus Ländern des nahen und mittleren Ostens interessiert hätten. In all der Empörung lässt allein De Morgen eine ironische Nuance einfließen, indem er am 17.9. kommentiert: "Enn spionagevirus bij Belgacom leidt in dit land niet tot een steekvlam van opwinding.... Vooreerst weten Belgen allang dat we onze privacy hebben afgestaan aan de Amerikaanse cybermaffia".
4. Am 18.9. nahm die Angelegenheit eine politische Wendung, als der Abgeordnete Roel Deseyn von den flämischen Christdemokraten (CD&V) Belgacom Chef Bellens beschuldigte, noch im Juli 2013 im Rahmen der Beantwortung einer parlamentarischen Anfrage den zuständigen Minister Jean-Pierre Labille (PS) nicht über den Datendiebstahl bei Belgacom informiert zu haben (De Standaard: "CD&V boos over 'vals informatie' van Belgacom"; Le Soir: "CD&V attaque Didier Bellens").
5. Laut übereinstimmenden Pressemeldungen habe die Regierung di Rupo das unerlaubte Eindringen in das Computersystem der Belgacom verurteilt, halte sich aber mit direkten Anschuldigungen gegen die USA zurück. So zitiert z.B. Le Soir vom 17.9. den zuständigen Minister Labille mit den Worten: "lorsque la ou les organisations à l'origine de ce piratage seront connues, le gouvernement entamera avec la plus grand fermeté les démarches appropriées". Die Écolos sind da weniger zurückhaltend und haben

laut der französischen Metrozeitung vom 17.9. MP di Rupo nahegelegt, den amerikanischen Botschafter einzubestellen. Laut l'Echo vom 17.9. forderten zudem mehrere parlamentarische Gruppen, dass sich sowohl Belgacom Chef Didier Bellens als auch der amerikanische Botschafter vor dem Parlament verantworten sollten.

III. Wertung:

Die großangelegte Infiltration des Computersystems der Belgacom findet in der belgischen Öffentlichkeit ein schockiertes Echo, wobei die Opposition und die Zeitungen im Gegensatz zur belgischen Regierung kein Blatt vor den Mund nehmen, was den Verdacht gegen die USA betrifft. Kritische Stimmen mahnen aber auch die Duplizität der europäischen Staaten an. So zitiert Le Soir vom 17.9. die liberale niederländische Europaabgeordnete Sophie in't Veld mit den Worten: "Le problème principale, c'est ... la duplicité des Etats membres de l'Union, qui s'indignent d'un côté de ce que font les Américains, et que de l'autre côté font la même chose - et collaborent même avec les Américains". Die Diskussion über diesen speziellen Aspekt der Cyberkriminalität dürfte interessant werden.

Im Auftrag

Margret Pollmeier

Dokument 2014/0067379

Von: Weinbrenner, Ulrich
Gesendet: Dienstag, 22. Oktober 2013 12:27
An: PGNSA
Betreff: WG: BRUEEU*4863: 2470. AStV-2 (2. Teil) am 21.10.2013

Vertraulichkeit: Vertraulich

erl.: -1

Mit freundlichem Gruß
Ulrich Weinbrenner
Bundesministerium des Innern
Leiter der Arbeitsgruppe ÖS I 3
Polizeiliches Informationswesen, BKA-Gesetz,
Datenschutz im Sicherheitsbereich
Tel.: + 49 30 3981 1301
Fax.: + 49 30 3981 1438
PC-Fax.: 01888 681 51301
Ulrich.Weinbrenner@bmi.bund.de

-----Ursprüngliche Nachricht-----

Von: Kotira, Jan
Gesendet: Montag, 21. Oktober 2013 17:18
An: Weinbrenner, Ulrich; Lesser, Ralf; Kutzschbach, Gregor, Dr.
Betreff: WG: BRUEEU*4863: 2470. AStV-2 (2. Teil) am 21.10.2013
Vertraulichkeit: Vertraulich

Z.K.

Gruß
Jan

-----Ursprüngliche Nachricht-----

Von: Schönthal, Ute
Gesendet: Montag, 21. Oktober 2013 15:40
An: OESI3AG_
Betreff: WG: BRUEEU*4863: 2470. AStV-2 (2. Teil) am 21.10.2013
Vertraulichkeit: Vertraulich

Aus Postfach UAL ÖS I weitergeleitet.

Mit freundlichen Grüßen
Ute Schönthal
Vorzimmer UAL ÖS I (030-18-681-1368)
Ute.Schoenthal@bmi.bund.de

-----Ursprüngliche Nachricht-----

Von: frdi [mailto:ivbbgw@BONNFMZ.Auswaertiges-Amt.de]
 Gesendet: Montag, 21. Oktober 2013 10:33
 Cc: 'krypto.betriebsstell@bk.bund.de'; Zentraler Posteingang BMI (ZNV); 'poststelle@bmwi.bund.de'; 'eurobmwi@bmwi.bund.de'
 Betreff: BRUEEU*4863: 2470. AStV-2 (2. Teil) am 21.10.2013
 Vertraulichkeit: Vertraulich

 VS-Nur fuer den Dienstgebrauch

WTLG

Dok-ID: KSAD025546820600 <TID=098961970600> BKAMT ssnr=1616 BMI ssnr=5252 BMWI ssnr=8340
 EUROBMWI ssnr=4132

aus: AUSWAERTIGES AMT
 an: BKAMT, BMI, BMWI, EUROBMWI

 aus: BRUESSEL EURO
 nr 4863 vom 21.10.2013, 1028 oz
 an: AUSWAERTIGES AMT

 Fernschreiben (verschlusselt) an E05
 eingegangen: 21.10.2013, 1031
 VS-Nur fuer den Dienstgebrauch
 auch fuer ATHEN DIPLO, BKAMT, BMI, BMJ, BMWI, EUROBMWI, LISSABON DIPLO, LONDON DIPLO,
 WASHINGTON

 im AA: DE iv, E-B-2, E01, E02, EKR, E03, E04
 Verfasser: Dieter
 Gz.: Pol 420.10 211028
 Betr.: 2470. AStV-2 (2. Teil) am 21.10.2013
 hier: TOP Sonstiges: Zusammensetzung der EU-US-Gruppe zum Datenschutz
 Bezug: keiner

--- Zur Unterrichtung ---

1. GBR unterrichtete den AStV unter "Sonstiges" darüber, dass man beabsichtige, anstelle des ursprünglich benannten Experten eine andere Person zu dem am 24. und 25.10. vorgesehenen Treffen der EU-US-Datenschutzgruppe zu entsenden. Dieser neue Experte werde selbstverständlich über die notwendigen Sicherheitsermächtigungen verfügen. Trotz dieser Zusage schein es jetzt Probleme mit der Kommission zu geben, die gegen das von GBR vorgesehene Verfahren Bedenken erhoben habe. Dies stoße auf Unverständnis. Schließlich habe man sich im Rahmen der Entscheidung über das Mandat der Gruppe darauf geeinigt, dass an dem Treffen 10 Mitgliedstaaten - u. a. GBR - vertreten seien. Man könne daher sein Mitglied der Gruppe durch eine andere Person ersetzen, sofern diese die Sicherheitsanforderungen erfülle.

2. PRT widersprach GBR-Position: AStV-Eingung über die Zusammensetzung der europäischen Teilnehmer der Datenschutzgruppe habe ausdrücklich klargestellt, dass die Mitgliedschaft an dieser Gruppe personengebunden sei. Die Mitglieder der Gruppe seien nicht Vertreter ihrer jeweiligen Staaten. Deshalb müsse jede Änderung der Zusammensetzung der Gruppe erneut durch den AStV gebilligt werden.

3. Es erfolgte keine weitere Aussprache zu diesem Punkt.

4. Präsidentschaft erklärte, die Angelegenheit prüfen zu wollen.

Tempel

Dokument 2014/0067389

Von: Peters, Reinhard
Gesendet: Freitag, 25. Oktober 2013 10:59
An: ALOES_; Kaller, Stefan; StabOESII_; Engelke, Hans-Georg; Weinbrenner, Ulrich; Taube, Matthias; Stöber, Karlheinz, Dr.; Jergl, Johann; PGNSA; Grosse, Stefan, Dr.
Betreff: Schlussfolgerungen ER zum Thema Ausspähen

am Ende des Dok. (S. 13).

Mit besten Grüßen
Reinhard Peters



~~2025 Pflanz ER&E...~~



EUROPEAN COUNCIL

Brussels, 24 October 2013

EUROPEAN COUNCIL

24/25 October 2013

Part I paragraphs 1-18, and part III paragraphs 32-43 of the European Council conclusions and Statement of Heads of State or Government (already adopted).

I. DIGITAL ECONOMY, INNOVATION AND SERVICES

1. A strong digital economy is vital for growth and European competitiveness in a globalised world. To this end, all efforts must be made for Europe's industry to regain momentum in digital products and services. There is an urgent need for an integrated single digital and telecoms market, benefiting consumers and companies. As part of its growth strategy, Europe must boost digital, data-driven innovation across all sectors of the economy. Special consideration should be given to supporting the reduction of the digital gap among Member States.

Investing in the digital economy

2. To tap the full potential of the digital economy, to boost productivity and create new economic activity and skilled jobs, Europe needs investment and the right regulatory framework. New investments should be promoted to accelerate the roll-out of infrastructure capable of achieving the broadband speed targets of the Digital Agenda for Europe, and to accelerate the deployment of new technologies, such as 4G, maintaining technology neutrality. Legislative measures to reduce the cost of broadband roll-out should be adopted rapidly.
3. Several strategic technologies such as Big Data and Cloud computing are important enablers for productivity and better services. Cloud computing should improve access to data and simplify their sharing. Big Data aims to process, collect, store and analyse large amounts of data. EU action should provide the right framework conditions for a single market for Big Data and Cloud computing, in particular by promoting high standards for secure, high-quality and reliable cloud services. The European Commission and the Member States, with the support of the "European Cloud Partnership", should continue to make every effort to put Europe at the forefront of cloud adoption. The European Council calls for the establishment of a strong network of national digital coordinators which could play a strategic role in Cloud, Big Data and Open Data development.

4. The ongoing work to tackle tax evasion, tax fraud, aggressive tax planning, tax-base erosion and profit shifting is also important for the digital economy. Member States should further coordinate their positions where appropriate in order to achieve the best possible solution for Member States and the EU in the OECD/BEPS (Base Erosion and Profit Shifting) framework. In its ongoing VAT review, the Commission will also address issues which are specific to the digital economy, such as differentiated tax rates for digital and physical products. The European Council welcomes the Commission's initiative to set up an expert group on taxation of the digital economy. The European Council will return to taxation-related issues at its December 2013 meeting.

Promoting a consumer and business-friendly Digital Single Market

5. Overcoming fragmentation, promoting effective competition and attracting private investment through an improved, predictable and stable EU-wide legal framework is crucial, while ensuring high level of consumer protection and allowing Member States a degree of flexibility to take additional consumer protection measures. In this context, the European Council welcomes the presentation by the Commission of the "Connected Continent" package and encourages the legislator to carry out an intensive examination with a view to its timely adoption. It underlines the importance of better coordinating the timing and conditions of spectrum assignment, while respecting national competences in this area.
6. The commitment to complete the Digital Single Market by 2015 has to be delivered on: today's market fragmentation hampers the release of the digital economy's full potential. This requires a comprehensive approach fostering innovation and competition in digital services.

7. No efforts should be spared to accelerate work on the pending legislative proposals, in particular the proposals on e-identification and trust services and on e-invoicing and payment services, so that they can be adopted by the end of the legislative period. There is also a need to address the bottlenecks in accessing one's "digital life" from different platforms which persist due to a lack of interoperability or lack of portability of content and data. This hampers the use of digital services and competition. An open and non-discriminatory framework must therefore be put in place to ensure such interoperability and portability without hindering development of the fast moving digital sphere and avoiding unnecessary administrative burden, especially for SME's. Providing digital services and content across the single market requires the establishment of a copyright regime for the digital age. The Commission will therefore complete its ongoing review of the EU copyright framework in Spring 2014. It is important to modernise Europe's copyright regime and facilitate licensing, while ensuring a high level of protection of intellectual property rights and taking into account cultural diversity.
8. It is important to foster the trust of citizens and businesses in the digital economy. The timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015.
9. The modernisation of public administrations should continue through the swift implementation of services such as e-government, e-health, e-invoicing and e-procurement. This will lead to more and better digital services for citizens and enterprises across Europe, and to cost savings in the public sector. Open data is an untapped resource with a huge potential for building stronger, more interconnected societies that better meet the needs of the citizens and allow innovation and prosperity to flourish. Interoperability and the re-use of public sector information shall be promoted actively. EU legislation should be designed to facilitate digital interaction between citizens and businesses and the public authorities. Efforts should be made to apply the principle that information is collected from citizens only once, in due respect of data protection rules.

Improving skills

10. Users must have the necessary digital skills. Many European citizens and enterprises currently do not use IT sufficiently. This results in a growing difficulty in filling digital jobs. In 2011, the European Union was faced with 300 000 unfilled vacancies in the ICT sector; if this trend is not checked, there could be as many as 900 000 unfilled vacancies by 2015. This skills mismatch is detrimental to our economic and social policy objectives.

11. Concrete steps should be taken in order to redress this situation:
 - a) part of the European Structural and Investment Funds (2014-2020) should be used for ICT education, support for retraining, and vocational education and training in ICT, including through digital tools and content, in the context of the Youth Employment Initiative;
 - b) a higher degree of integration of digital skills in education, from the earliest stages of school to higher education, vocational education and training and lifelong learning should be ensured;
 - c) the Grand Coalition for Digital Jobs should be strengthened to address skills mismatches by supporting targeted labour mobility schemes and the use of the newly developed classification of European Skills/Competences, Qualifications and Occupations (ESCO);
 - d) the Commission will further intensify work on the basis of the EU Skills Panorama for digital jobs in order to accelerate progress on pan-European competences frameworks for digital skills.

12. In all three areas - investments, Digital Single Market and improving skills - a strong commitment is vital if the objective of enhancing growth, competitiveness and jobs is to be achieved. The European Council calls on the Council and the Commission to take forward this agenda and will return to the matter in the course of 2014.

Innovation

13. Investment in research and innovation fuels productivity and growth and is key for job creation. Member States that have continued to invest in research and innovation have fared better in the current crisis than those that have not.
14. In February 2011, the European Council called for a strategic and integrated approach to boost innovation and take full advantage of Europe's intellectual capital. It set out specific steps to achieve this. Two years on, a significant number of them are on track. Joint programming in research and innovation is developing. Annual monitoring of progress on innovation is taking place in the framework of the Europe 2020 strategy. The establishment of a Research and Innovation Observatory by the Commission is under way. A number of programmes providing funding to research and innovation are being finalised. As requested, the Commission recently proposed a single Indicator of Innovation Output which should allow for better monitoring.
15. The Union's intellectual and scientific potential does not always translate into new products and services that can be sold on markets. The main reasons for this commercialisation gap are: difficulties in accessing finance, market barriers and excessive red tape. The grouping of research institutes and industry ("clusters") can provide the ground for fruitful interaction between them and for the emergence of new products, services and industries.

16. Europe needs a better-coordinated use of tools such as grants, pre-commercial public procurement and venture capital, and an integrated approach from research and innovation to market deployment. Special attention should be paid to the role of the public sector in enabling systemic innovations, especially in the cleantech and biotech sectors. The 2010 Innovation Union flagship initiative provides a number of valuable instruments which, combined with financing programmes, such as Competitiveness of Enterprises and SMEs (COSME) and Horizon 2020, including the Risk-Sharing Finance Facility, can support innovation and its impact on the market. The proposals for Joint Technology Initiatives in pharmaceuticals, new energy technologies, aeronautics, the bio-based economy and electronics should be adopted as soon as possible. Efforts should also continue at national level.
17. In order to obtain a full European Research Area by the end of 2014, it is important to accelerate structural reforms of national systems and to strengthen progress monitoring based on robust data provided by Member States. The progress report submitted by the Commission identifies some areas which require more efforts. In particular, we must improve the mobility and career prospects of researchers through adequate pensions solutions, transnational access to research infrastructures and open access to publicly funded research results and knowledge transfer as part of innovation strategies at national and European levels.
18. The European Council invites the Commission and the Member States to continue their efforts in the area of innovation and research. It will take stock of progress at its meeting in February 2014.

III. ECONOMIC AND MONETARY UNION

32. Following the December 2012 and June 2013 European Council meetings, the European Council has focused its discussion on banking and economic union but will return to all issues in December 2013. This process builds on the EU's institutional framework, in full respect of the integrity of the single market, while ensuring a level playing-field between EU Member States, including via a fair balance between home and host Member States. It will be open and transparent towards Member States not using the single currency.

Strengthened economic policy coordination

33. Strengthening economic governance is an ongoing process in which significant progress has been achieved in recent years. The European Semester brings the elements together in an integrated process leading to the formulation of policy recommendations.
34. To promote strong, sustainable and inclusive economic growth in the Euro area, the coordination of economic policies needs to be further strengthened, notably by increasing the level of commitment, ownership and implementation of economic policies and reforms in Euro area Member States, underpinned by strong democratic legitimacy and accountability at the level at which decisions are taken and implemented.

35. The European Council underlines that closer coordination of economic policies should be focused on policy areas where positive effects on competitiveness, employment and the functioning of the EMU are most prominent.

As a first step, the European Council will make a shared analysis of the economic situation in the Member States and in the Euro area as such. To this end, it will already hold a discussion in December following the publication of the Commission's Annual Growth Survey and the Alert Mechanism Report with the aim to agree, on the basis of the relevant indicators, on the main areas for coordination of economic policies and reforms.

This shared analysis will be based on an assessment of growth and job-enhancing policies and measures, including the performance of labour and product markets, the efficiency of the public sector, as well as research and innovation, education and vocational training, employment and social inclusion in the Euro area.

The Commission will also provide a first overview of the implementation of country-specific recommendations that will be a basis for the further monitoring of their implementation.

Work will be carried forward to strengthen economic policy coordination, with the objective of taking decisions in December on the main features of contractual arrangements and of associated solidarity mechanisms. This would engage all Euro area Member States but non-Euro area Member States may also choose to enter into similar arrangements. Any such measures must be fully compatible with the Single market in all aspects.

Social dimension

36. The European Council welcomes the European Commission's Communication on the social dimension of the EMU as a positive step and restates the importance of employment and social developments within the European Semester. The use of an employment and social scoreboard in the Joint Employment Report and of employment and social indicators along the lines proposed by the Commission should be pursued, following appropriate work in the relevant Committees, for decision by the Council in December with the objective of using these new instruments as early as the 2014 European Semester. This wider range of indicators has the purpose of allowing a broader understanding on social developments.
37. The coordination of economic, employment and social policies will be further enhanced in line with existing procedures while fully respecting national competences. This requires more work to strengthen cooperation between the various Council configurations in order to ensure consistency of those policies in line with our common objectives.
38. The strengthened economic policy coordination and further measures to enhance the social dimension in the Euro area are voluntary for those outside the single currency and will be fully compatible with the Single Market in all aspects.
39. Finally, the European Council underscores the importance of enhancing the social dialogue involving the social partners both at Member State and European level, in particular in the context of the European Semester, with the objective of enhancing the ownership of its conclusions and recommendations across the Union.

Banking Union

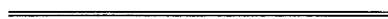
40. The European Council has been actively steering the process of establishing the Banking Union. It welcomes the final adoption by the Council of the Single Supervisory Mechanism and the European Banking Authority (EBA) Amending Regulations. This represents a decisive step towards the Banking Union. The European Council reiterates the principle of non-discrimination of Member States regarding banking supervision and resolution as stated by the European Council in October 2012 and reconfirms the agreed new voting arrangements in the EBA regulation for these matters, which is reflecting an appropriate balance between the participating and non-participating Member States. The European Council also reconfirms its agreement that the review on the operation of the voting arrangements will take place from the date on which the number of non-participating Member States reaches four.

41. The Single Supervisory Mechanism is the first step towards the Banking Union. In November, the European Central Bank will launch a comprehensive assessment of the credit institutions of the Member States participating in the Single Supervisory Mechanism in line with the Regulation conferring specific tasks on the European Central Bank. This will be followed by a stress test of banks across the EU. The European Council considers that this exercise is key to reinforce confidence in the EU banking sector and to restore normal lending conditions to firms and households. The European Council expects full support and cooperation by the national authorities to ensure complete transparency and a rigorous approach, which is key for the credibility of the exercise.

42. In this context, the European Council recalls the urgency, for the Member States taking part in the Single Supervisory Mechanism, of establishing a coordinated European approach in preparation for the comprehensive assessment of credit institutions by the European Central Bank. Member States should make all appropriate arrangements, including national backstops, applying state aid rules. European instruments are available according to their agreed rules. The European Council asks the Council to develop this approach as a matter of urgency and to communicate it by the end of November, in line with the goal that the European Central Bank completes the comprehensive assessment of credit institutions in a timely manner.

It also calls on the Eurogroup to finalise guidelines for European Stability Mechanism direct recapitalisation so that the European Stability Mechanism can have the possibility to recapitalise banks directly, following the establishment of the Single Supervisory Mechanism.

43. Completing the Banking Union is urgent and requires not only a Single Supervisory Mechanism but also a Single Resolution Mechanism. The European Council calls on the legislators to adopt the Bank Recovery and Resolution Directive and the Deposit Guarantee Directive by the end of the year. The European Council underlines the need to align the Single Resolution Mechanism and the Bank Recovery and Resolution Directive as finally adopted. It also underlines the commitment to reach a general approach by the Council on the Commission's proposal for a Single Resolution Mechanism by the end of the year in order to allow for its adoption before the end of the current legislative period.



ANNEXSTATEMENT OF HEADS OF STATE OR GOVERNMENT

The Heads of State or Government discussed recent developments concerning possible intelligence issues and the deep concerns that these events have raised among European citizens.

They underlined the close relationship between Europe and the USA and the value of that partnership. They expressed their conviction that the partnership must be based on respect and trust, including as concerns the work and cooperation of secret services.

They stressed that intelligence gathering is a vital element in the fight against terrorism. This applies to relations between European countries as well as to relations with the USA. A lack of trust could prejudice the necessary cooperation in the field of intelligence gathering.

The Heads of State or Government took note of the intention of France and Germany to seek bilateral talks with the USA with the aim of finding before the end of the year an understanding on mutual relations in that field. They noted that other EU countries are welcome to join this initiative.

They also pointed to the existing Working Group between the EU and the USA on the related issue of data protection and called for rapid and constructive progress in that respect.

Dokument 2014/0067390

Von: GII2_
Gesendet: Freitag, 25. Oktober 2013 11:37
An: PGNSA; OESIII3_
Cc: GII2_; PGDS_; IT3_; OESI3AG_; OESI4_; OESII2_; Hübner, Christoph, Dr.; Wolf, Katharina; Popp, Michael
Betreff: Europäischer Rat am 24./25.10.2013; hier: ANNEX zum *vierter* Entwurf ER-Schlussfolgerungen (ER-SF)
Anlagen: sn00040.en13.doc

Nachstehender Hinweis auf den „aus aktuellem Anlass“ hinzugekommenen „Annex“ zum 4. Entw. ER-SF

auch an Sie

Beste Grüße
 i.A.
 Roland Arhelger

BMI-Referat G II 2
 EU-Grundsatzfragen einschließlich
 Schengenangelegenheiten;
 Beziehungen zum Europäischen Parlament;
 Europabeauftragte
 Bundesministerium des Innern
 Alt-Moabit 101 D,
 10559 Berlin
 Tel. +49 (0)30 18 681 - 2370
 Fax +49 (0)30 18 681 - 52370
 e-mail: roland.arhelger@bmi.bund.de

Von: GII2_
Gesendet: Freitag, 25. Oktober 2013 10:10
An: PGDS_
Cc: GII2_; IT3_; OESI3AG_; OESI4_; OESII2_; Hübner, Christoph, Dr.; Wolf, Katharina; Popp, Michael
Betreff: Europäischer Rat am 24./25.10.2013; hier: *vierter* Entwurf ER-Schlussfolgerungen (ER-SF)

ZUSATZ für PG DS,

d.h. gesonderter Hinweis auf den „aus aktuellem Anlass“ hinzugekommenen „Annex“ zum 4. Entw. ER-SF

ANNEX

STATEMENT OF HEADS OF STATE OR GOVERNMENT

The Heads of State or Government discussed recent developments concerning possible intelligence issues and the deep concerns that these events have raised among European citizens.

They underlined the close relationship between Europe and the USA and the value of that partnership. They expressed their conviction that the partnership must be based on respect and trust, including as concerns the work and cooperation of secret services.

They stressed that intelligence gathering is a vital element in the fight against terrorism. This applies to relations between European countries as well as to relations with the USA. A lack of trust could prejudice the necessary cooperation in the field of intelligence gathering.

The Heads of State or Government took note of the intention of France and Germany to seek bilateral talks with the USA with the aim of finding before the end of the year an understanding on mutual relations in that field. They noted that other EU countries are welcome to join this initiative.

They also pointed to the existing Working Group between the EU and the USA on the related issue of data protection and called for rapid and constructive progress in that respect.

Beste Grüße
i.A.
Roland Arhelger

BMI-Referat G II 2
EU-Grundsatzfragen einschließlich
Schengenangelegenheiten;
Beziehungen zum Europäischen Parlament;
Europabeauftragte
Bundesministerium des Innern
Alt-Moabit 101 D,
10559 Berlin
Tel. +49 (0)30 18 681 - 2370
Fax +49 (0)30 18 681 - 52370
e-mail: roland.arhelger@bmi.bund.de

Von: GII2_

Gesendet: Freitag, 25. Oktober 2013 09:59

An: GIII5_ ; OESI4_ ; MI5_ ; B4_ ; PGDBOS_ ; PGDS_ ; VI4_ ; IT1_ ; IT3_ ; O1_ ; O2_ ; O4_ ; O5_

Cc: GIII1_ ; GII2_ ; GII3_ ; GII4_ ; GII5_ ; GIII4_ ; OESI2_ ; OESI3AG_ ; OESII2_ ; MI1_ ; MI3_ ; MI4_ ; VII4_ ; IT5_ ; Hübner, Christoph, Dr.; Wolf, Katharina; Popp, Michael; Gitter, Rotraud, Dr.; Schlender, Katharina; Bratanova, Elena; Köpke, Jörg; AA Konther, Michael

Betreff: Europäischer Rat am 24./25.10.2013; hier: *vierter* Entwurf ER-Schlussfolgerungen (ER-SF)

Liebe Kolleginnen und Kollegen,

anbei übermittle ich den aktuellen vierten Entwurf der ER-SF „vor Beginn des zweiten Tages des Okt.-ER“.

Zitat aus anliegendem Word-Dokument (Arbeitshinweis im 4. Entw. ER-SF):

„Part I paragraphs 1-18, and part III paragraphs 32-43 have been adopted by the European Council on 24 October“.

BMI-interne Hinweise:

- Abschnitt „**MIGRATION FLOWS**“ beginnt nunmehr in den Ziff. 45. bis 48. Entw. ER-SF (für Textvergleich s.u.)
- **Ziff. 8** im Vergleich (Ziff. 8 im 4. Entw. ER-SF ist laut anl. Word-Dokument bereits angenommen):

Auszug <u>3.</u> Entw. ER-SF	Auszug <u>4.</u> Entw. ER-SF
<p>8. It is important to foster the trust of consumers and businesses in the digital economy through the adoption next year of a strong EU General Data Protection framework and the Cyber-security Directive, which are essential for the completion of the Digital Single Market.</p>	<p>8. It is important to foster the trust of citizens and businesses in the digital economy. The timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015.</p>

- Abschnitt “**EASTERN PARTNERSHIP**” (Ziff. 44.) lautet im 4. Entw. ER-SF nun wie folgt:

44. The European Council looks forward to the Eastern Partnership Summit in Vilnius on 28 and 29 November 2013. It underlines the importance of the Eastern Partnership for building a common area of democracy, prosperity and stability across the European continent. The European Council reiterates the European Union's willingness to sign the Association Agreement, including the Deep and Comprehensive Free Trade Area, with Ukraine at the Vilnius Summit, provided there is determined action and tangible progress in line with the Council Conclusions of 10 December 2012, and to launch its provisional application. It confirms the European Union's readiness to initial similar agreements with the Republic of Moldova and Georgia at the Vilnius Summit, with the aim of signing them by Autumn 2014.

- Gegenüberstellung Abschnitt „MIGRATION FLOWS“ (nunmehr in den Ziff. 45. bis 48. Entw. ER-SF):

Auszug 3. Entw. ER-SF	Auszug 4. Entw. ER-SF
<p data-bbox="268 461 632 495"><u>V. MIGRATION FLOWS</u></p> <p data-bbox="316 539 847 1021">43. The European Council expresses its deep sadness at the recent and dramatic death of hundreds of people in the Mediterranean which shocked all Europeans. Based on the imperative of prevention and protection and guided by the principle of solidarity and fair sharing of responsibility, determined action should be taken in order to prevent the loss of lives at sea and to avoid that such human tragedies happen again.</p> <p data-bbox="316 1066 847 2040">44. The European Council underlines the importance of addressing root causes of migration flows by enhancing cooperation with the countries of origin and transit of illegal migration, including through appropriate EU development support and an effective return policy. It also calls for closer cooperation with the relevant international organisations, in particular UNHCR and the International Organisation of Migration in the third countries concerned. Not only in the territory of the EU Member States but also in the countries of origin and transit, the fight against trafficking and smuggling of human beings should be stepped up. Furthermore, the European Council calls for the reinforcement of Frontex activities in the Mediterranean. Swift implementation by Member States of the new European Border Surveillance System (EUROSUR) will be crucial to help detecting</p>	<p data-bbox="874 461 1238 495"><u>V. MIGRATION FLOWS</u></p> <p data-bbox="922 539 1437 1021">45. The European Council expresses its deep sadness at the recent and dramatic death of hundreds of people in the Mediterranean which shocked all Europeans. Based on the imperative of prevention and protection and guided by the principle of solidarity and fair sharing of responsibility, determined action should be taken in order to prevent the loss of lives at sea and to avoid that such human tragedies happen again.</p> <p data-bbox="922 1066 1437 2040">46. The European Council underlines the importance of addressing root causes of migration flows by enhancing cooperation with the countries of origin and transit, including through appropriate EU development support and an effective return policy. It also calls for closer cooperation with the relevant international organisations, in particular UNHCR and the International Organisation of Migration in the third countries concerned. Not only in the territory of the EU Member States but also in the countries of origin and transit, the fight against trafficking and smuggling of human beings should be stepped up. Furthermore, the European Council calls for the reinforcement of Frontex activities in the Mediterranean. Swift implementation by Member States of the new European Border Surveillance System (EUROSUR)</p>

vessels in order to protect and save lives at the EU's external borders.

45. The European Council invites the newly established Task Force for the Mediterranean, led by the European Commission and involving Member States, EU agencies and the EEAS, to identify -based on the principles of prevention, protection and solidarity- priority actions for a more efficient use of European policies and tools. The Commission will report to the Council at its meeting of 5-6 December 2013 on the work of the Task Force. The Presidency will report to the European Council in December.

46. The European Council will return to asylum and migration issues in a broader and longer term policy perspective in June 2014, when strategic guidelines for further legislative and operational planning in the area of freedom, security and justice will be defined.

will be crucial to help detecting vessels in order to protect and save lives at the EU's external borders.

47. The European Council invites the newly established Task Force for the Mediterranean, led by the European Commission and involving Member States, EU agencies and the EEAS, to identify -based on the principles of prevention, protection and solidarity- priority actions for a more efficient use of European policies and tools. The Commission will report to the Council at its meeting of 5-6 December 2013 on the work of the Task Force. The Presidency will report to the European Council in December.

48. The European Council will return to asylum and migration issues in a broader and longer term policy perspective in June 2014, when strategic guidelines for further legislative and operational planning in the area of freedom, security and justice will be defined.

Beste Grüße
i.A.
Roland Arhelger

BMI-Referat G II 2
EU-Grundsatzfragen einschließlich
Schengenangelegenheiten;
Beziehungen zum Europäischen Parlament;
Europabeauftragte
Bundesministerium des Innern
Alt-Moabit 101 D,
10559 Berlin
Tel. +49 (0)30 18 681 - 2370

Fax +49 (0)30 18 681 - 52370
 e-mail: roland.arhelger@bmi.bund.de

Von: .BRUEEU POL-IN1-1-EU Schumacher, Andrea [<mailto:pol-in1-1-eu@brue.auswaertiges-amt.de>]
Gesendet: Freitag, 25. Oktober.2013 08:04
An: GII2_ ; MI5_
Cc: AA Kaba, Sarah; AA Konther, Michael
Betreff: WG: Schlussfolgerungen des ER - Zwischenstand Donnerstag/Freitag - ENG-Version EN**Draft
 Conclusions of the European Council 24-25 October 2013 - PROJET DES CONCLUSIONS DU CONSEIL
 EUROPEEN 24-25 OCTOBRE 2013

Gruß
 Andrea Schumacher

Von: .BRUEEU POL-EU2-1-EU Dieter, Robert [<mailto:pol-eu2-1-eu@brue.auswaertiges-amt.de>]
Gesendet: Freitag, 25. Oktober 2013 06:34
An: .BRUEEU *ASTV2-AR (extern)
Betreff: Schlussfolgerungen des ER - Zwischenstand Donnerstag/Freitag - ENG-Version EN**Draft
 Conclusions of the European Council 24-25 October 2013 - PROJET DES CONCLUSIONS DU CONSEIL
 EUROPEEN 24-25 OCTOBRE 2013

Anliegend der aktuelle Entwurf der SF des Europäischen Rates vor Beginn des zweiten Tages des ER.

Gruß
 Robert Dieter

Von: COORDINATION PROGRAMMATION [<mailto:coordination.programmation@consilium.europa.eu>]
Gesendet: Freitag, 25. Oktober 2013 02:13
An: ALMEIDA Alexandra; 'Tomas Kozak'; 'Kristina Bizjak (kristina.bizjak@gov.si)'; 'Virginia Pina (mvp@reper-portugal.be)'; 'claude.bonello@gov.mt'; 'angele.dacruz@mae.etat.lu'; 'antici@rpue.esteri.it'; 'Fergal MYTHEN (anticiteam2@dfa.ie)'; 'Cyril Piquemal (cyril.piquemal@diplomatie.gouv.fr)'; 'antici FI (Sari.lehtiranta@formin.fi)'; 'fernando.nogales@reper.maec.es'; 'g.karasiotou@rp-grece.be'; 'Klen JÄÄRATS (marika.linntam@mfa.ee)'; .BRUEEU *Antici; 'Eva Yiasemidou (eyiasemidou@mfa.gov.cy)'; WIMMER Michael; 'antici AT (maximilian.hennig@bmeia.gv.at)'; NELEN Sarah; 'BE Antici (axel.kenes@diplobel.fed.be)'; SAMCOVA Lucie; 'Uk Antici (jain.frew@fco.gov.uk)'; 'Cs Antici (jakub.uteseny@mzv.cz)'; 'BG Antici (bg-antici@bg-permrep.eu)'; 'Antici DA (sojaco@um.dk)'; 'HU Antici (adrien.muller@mfa.gov.hu)'; 'LV Antici (antici@mfa.gov.lv)'; 'PL Antici (michal.mazur@msz.gov.pl)'; 'RO Antici (mihaela.stefan@rpro.eu)'; 'SV Antici (efraim.gomez@gov.se)'; FLORINDO Gijon Fernando; 'Antici HR (predrag.rugani@mvep.hr)'; DE NORRE Brigitte; 'NL antici (Eeuwke.faber@minbuza.nl)'; CORSEPIUS Uwe; MORA Marek; CHAVES BENEROSO Pilar; DHONDT Chantal; DE NORRE Brigitte; CLOOS Jim; 'Maja.Peternel@gov.si'; VAN ELST Jan; GITONA Natasha; GRANET Marie-France; 'LT Antici (antici@eu.mfa.lt)'
Cc: SERVICE BUREAU CENTRAL
Betreff: EN**Draft Conclusions of the European Council 24-25 October 2013 - PROJET DES
 CONCLUSIONS DU CONSEIL EUROPEEN 24-25 OCTOBRE 2013

Dear Sir/Madam,

Please find attached the English version of **DRAFT** conclusions.

Kind regards,
Coordination Programmation

Monsieur/Madame,

Veillez trouver ci-joint la version anglaise du **PROJET** des conclusions.

Cordialement,
Coordination Programmation

DRAFT

CONCLUSIONS

EUROPEAN COUNCIL

24/25 October 2013

Part I paragraphs 1-18, and part III paragraphs 32-43 have been adopted by the European Council on 24 October.

Signs of economic recovery are visible but the EU needs to pursue its efforts to increase growth potential, enhance job creation and boost European competitiveness. Today the European Council focused on the digital economy, innovation and services. These areas have a particular potential for growth and jobs which must be rapidly mobilized. The European Council provided concrete guidance so as to take full advantage of the existing potential.

The European Council also looked at different economic and social policy areas. It took stock of the implementation of the initiatives taken in June in the fight against youth unemployment and the financing of the economy, in particular of small and medium-sized enterprises, and agreed on additional measures. It gave a new impetus to better regulation.

The European Council held an in-depth discussion on completing the Economic and Monetary Union. It focused in particular on enhanced economic policy coordination, strengthening the social dimension of the Economic and Monetary Union and completing the Banking Union. As decided in June, the European Council will return to all these elements in December with a view to taking decisions.

The European Council looked ahead to the Eastern Partnership Summit which will be held in Vilnius on 28 and 29 November 2013.

The European Council expressed its deep sadness at the recent tragic events in the Mediterranean in which hundreds of people lost their lives and decided to step up the Union's action so as to prevent such tragedies from happening again.

I. DIGITAL ECONOMY, INNOVATION AND SERVICES

1. A strong digital economy is vital for growth and European competitiveness in a globalised world. To this end, all efforts must be made for Europe's industry to regain momentum in digital products and services. There is an urgent need for an integrated single digital and telecoms market, benefiting consumers and companies. As part of its growth strategy, Europe must boost digital, data-driven innovation across all sectors of the economy. Special consideration should be given to supporting the reduction of the digital gap among Member States.

Investing in the digital economy

2. To tap the full potential of the digital economy, to boost productivity and create new economic activity and skilled jobs, Europe needs investment and the right regulatory framework. New investments should be promoted to accelerate the roll-out of infrastructure capable of achieving the broadband speed targets of the Digital Agenda for Europe, and to accelerate the deployment of new technologies, such as 4G, maintaining technology neutrality. Legislative measures to reduce the cost of broadband roll-out should be adopted rapidly.
3. Several strategic technologies such as Big Data and Cloud computing are important enablers for productivity and better services. Cloud computing should improve access to data and simplify their sharing. Big Data aims to process, collect, store and analyse large amounts of data. EU action should provide the right framework conditions for a single market for Big Data and Cloud computing, in particular by promoting high standards for secure, high-quality and reliable cloud services. The European Commission and the Member States, with the support of the "European Cloud Partnership", should continue to make every effort to put Europe at the forefront of cloud adoption. The European Council calls for the establishment of a strong network of national digital coordinators which could play a strategic role in Cloud, Big Data and Open Data development.

4. The ongoing work to tackle tax evasion, tax fraud, aggressive tax planning, tax-base erosion and profit shifting is also important for the digital economy. Member States should further coordinate their positions where appropriate in order to achieve the best possible solution for Member States and the EU in the OECD/BEPS (Base Erosion and Profit Shifting) framework. In its ongoing VAT review, the Commission will also address issues which are specific to the digital economy, such as differentiated tax rates for digital and physical products. The European Council welcomes the Commission's initiative to set up an expert group on taxation of the digital economy. The European Council will return to taxation-related issues at its December 2013 meeting.

Promoting a consumer and business-friendly Digital Single Market

5. Overcoming fragmentation, promoting effective competition and attracting private investment through an improved, predictable and stable EU-wide legal framework is crucial, while ensuring high level of consumer protection and allowing Member States a degree of flexibility to take additional consumer protection measures. In this context, the European Council welcomes the presentation by the Commission of the "Connected Continent" package and encourages the legislator to carry out an intensive examination with a view to its timely adoption. It underlines the importance of better coordinating the timing and conditions of spectrum assignment, while respecting national competences in this area.
6. The commitment to complete the Digital Single Market by 2015 has to be delivered on: today's market fragmentation hampers the release of the digital economy's full potential. This requires a comprehensive approach fostering innovation and competition in digital services.

7. No efforts should be spared to accelerate work on the pending legislative proposals, in particular the proposals on e-identification and trust services and on e-invoicing and payment services, so that they can be adopted by the end of the legislative period. There is also a need to address the bottlenecks in accessing one's "digital life" from different platforms which persist due to a lack of interoperability or lack of portability of content and data. This hampers the use of digital services and competition. An open and non-discriminatory framework must therefore be put in place to ensure such interoperability and portability without hindering development of the fast moving digital sphere and avoiding unnecessary administrative burden, especially for SME's. Providing digital services and content across the single market requires the establishment of a copyright regime for the digital age. The Commission will therefore complete its ongoing review of the EU copyright framework in Spring 2014. It is important to modernise Europe's copyright regime and facilitate licensing, while ensuring a high level of protection of intellectual property rights and taking into account cultural diversity.
8. It is important to foster the trust of citizens and businesses in the digital economy. The timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015.
9. The modernisation of public administrations should continue through the swift implementation of services such as e-government, e-health, e-invoicing and e-procurement. This will lead to more and better digital services for citizens and enterprises across Europe, and to cost savings in the public sector. Open data is an untapped resource with a huge potential for building stronger, more interconnected societies that better meet the needs of the citizens and allow innovation and prosperity to flourish. Interoperability and the re-use of public sector information shall be promoted actively. EU legislation should be designed to facilitate digital interaction between citizens and businesses and the public authorities. Efforts should be made to apply the principle that information is collected from citizens only once, in due respect of data protection rules.

Improving skills

10. Users must have the necessary digital skills. Many European citizens and enterprises currently do not use IT sufficiently. This results in a growing difficulty in filling digital jobs. In 2011, the European Union was faced with 300 000 unfilled vacancies in the ICT sector; if this trend is not checked, there could be as many as 900 000 unfilled vacancies by 2015. This skills mismatch is detrimental to our economic and social policy objectives.

11. Concrete steps should be taken in order to redress this situation:
 - a) part of the European Structural and Investment Funds (2014-2020) should be used for ICT education, support for retraining, and vocational education and training in ICT, including through digital tools and content, in the context of the Youth Employment Initiative;

 - b) a higher degree of integration of digital skills in education, from the earliest stages of school to higher education, vocational education and training and lifelong learning should be ensured;

 - c) the Grand Coalition for Digital Jobs should be strengthened to address skills mismatches by supporting targeted labour mobility schemes and the use of the newly developed classification of European Skills/Competences, Qualifications and Occupations (ESCO);

 - d) the Commission will further intensify work on the basis of the EU Skills Panorama for digital jobs in order to accelerate progress on pan-European competences frameworks for digital skills.

12. In all three areas - investments, Digital Single Market and improving skills - a strong commitment is vital if the objective of enhancing growth, competitiveness and jobs is to be achieved. The European Council calls on the Council and the Commission to take forward this agenda and will return to the matter in the course of 2014.

Innovation

13. Investment in research and innovation fuels productivity and growth and is key for job creation. Member States that have continued to invest in research and innovation have fared better in the current crisis than those that have not.
14. In February 2011, the European Council called for a strategic and integrated approach to boost innovation and take full advantage of Europe's intellectual capital. It set out specific steps to achieve this. Two years on, a significant number of them are on track. Joint programming in research and innovation is developing. Annual monitoring of progress on innovation is taking place in the framework of the Europe 2020 strategy. The establishment of a Research and Innovation Observatory by the Commission is under way. A number of programmes providing funding to research and innovation are being finalised. As requested, the Commission recently proposed a single Indicator of Innovation Output which should allow for better monitoring.
15. The Union's intellectual and scientific potential does not always translate into new products and services that can be sold on markets. The main reasons for this commercialisation gap are: difficulties in accessing finance, market barriers and excessive red tape. The grouping of research institutes and industry ("clusters") can provide the ground for fruitful interaction between them and for the emergence of new products, services and industries.

16. Europe needs a better-coordinated use of tools such as grants, pre-commercial public procurement and venture capital, and an integrated approach from research and innovation to market deployment. Special attention should be paid to the role of the public sector in enabling systemic innovations, especially in the cleantech and biotech sectors. The 2010 Innovation Union flagship initiative provides a number of valuable instruments which, combined with financing programmes, such as Competitiveness of Enterprises and SMEs (COSME) and Horizon 2020, including the Risk-Sharing Finance Facility, can support innovation and its impact on the market. The proposals for Joint Technology Initiatives in pharmaceuticals, new energy technologies, aeronautics, the bio-based economy and electronics should be adopted as soon as possible. Efforts should also continue at national level.

17. In order to obtain a full European Research Area by the end of 2014, it is important to accelerate structural reforms of national systems and to strengthen progress monitoring based on robust data provided by Member States. The progress report submitted by the Commission identifies some areas which require more efforts. In particular, we must improve the mobility and career prospects of researchers through adequate pensions solutions, transnational access to research infrastructures and open access to publicly funded research results and knowledge transfer as part of innovation strategies at national and European levels.

18. The European Council invites the Commission and the Member States to continue their efforts in the area of innovation and research. It will take stock of progress at its meeting in February 2014.

Services

19. Services are a fundamental part of the Single Market. To reap the full economic benefits, Member States urgently need to improve implementation of the Services Directive and thus speed up the opening of services markets. All opportunities should be seized in this respect; unjustified or disproportionate barriers should be removed in order to ensure a level playing-field on the services market.

20. The European Council welcomes the peer review of the Services Directive presented by the Commission. It agrees that all Member States should ensure systematic, thorough and robust proportionality assessments of their regulatory requirements. The European Council invites the Commission to continue to assist Member States on the concept of proportionality and invites Member States to take full account of best practices.

21. The European Council stresses the importance of the mutual evaluation of regulated professions launched by the Commission and calls for swift progress. This exercise should identify the remaining barriers to access to professions in the Member States, assess the cumulative effect of all restrictions imposed on the same profession, and suggest appropriate action.

II. ECONOMIC AND SOCIAL POLICY

Combating youth unemployment

22. The fight against youth unemployment remains a key objective of the EU strategy to foster growth, competitiveness and jobs. The European Council recalls the need for the Youth Employment Initiative to be fully operational by January 2014, which will allow the first disbursements to beneficiaries to be made. It calls on the Member States to mobilise all efforts necessary to this end.
23. The European Council also calls for rapid implementation by the Member States of the Youth Guarantee and the Council declaration on the European Alliance for Apprenticeships. It points out that Member States benefiting from the Youth Employment Initiative need to adopt a Youth Guarantee implementation plan before the end of 2013 in order to benefit rapidly from the initiative. In this context, the European Council welcomes the upcoming Paris Conference.

Financing of the economy

24. All efforts should continue to restore normal lending to the economy and facilitate financing of investment, particularly with respect to small and medium-sized enterprises (SMEs).

25. The programming negotiations of the European Structural and Investment Funds (ESIF) should be used to double the overall EU support from these funds to leverage-based financial instruments for SMEs in 2014-2020, with significant increases in countries where conditions remain tight. These instruments should be designed in a way which limits market fragmentation, ensures high leverage effects and quick uptake by the SMEs. This will help concentrate the funds adequately and expand the volume of new loans to SMEs.

26. The European Council takes note of the reports by the Commission and the EIB on the implementation of measures aimed at financing the economy and invites Member States to make good use of the opportunities provided. It reiterates its call to expand joint risk-sharing financial instruments between the Commission and the European Investment Bank (EIB) to leverage private sector and capital market investments in SMEs, with the aim of expanding the volume of new loans to SMEs across the EU. Work should be finalized to amend the Common Provisions Regulation to enable the use of guarantees and securitisation for new and existing loans. The new instruments should achieve high leverage effects and be attractive for private sector and capital markets investment. The EIB should start implementing them while work should continue on further developing tools for the future. While contributions to the SME initiative should remain voluntary, the European Council calls for the greatest possible participation by Member States to reach critical mass. Member States will inform the Commission and the EIB about their contributions by the end of the year. The new instruments should begin operating in January 2014 to accompany recovery, fight unemployment and reduce fragmentation in the initial years of the financial framework.

27. The role of the Union's budget in providing opportunities to SMEs is crucial. In this context, the European Council welcomes the agreement on the COSME and Horizon 2020 programmes and points out that their implementation is a matter of priority. It also encourages the legislator to work swiftly on the proposed legislation on long-term investment funds with a view to its adoption before the end of the legislative period.

Regulatory fitness

28. Regulation at Union level is necessary in order to ensure that EU policy goals, including the proper functioning of the Single Market, are attained. This should be achieved with a maximum of transparency and simplicity and a minimum of costs while always taking account of the need for a proper protection of consumers, health, the environment and employees.
29. The European Council welcomes the recent Commission Communication on regulatory fitness (REFIT), which acknowledges work already undertaken in recent years to alleviate the burden of legislation, in particular for SMEs, and proposes ambitious further steps to make the EU regulatory framework lighter.
30. The European Council urges the Commission and the legislator to rapidly implement the REFIT programme, *inter alia* through simplification of existing EU law, by withdrawing proposals that are no longer needed and by repealing legislation that is out of date.
31. To this end, the European Council underlines the need to monitor progress by means of a comprehensive scoreboard to track progress at the European and national level and facilitate dialogue on regulatory fitness. It welcomes the steps taken by the Member States and the EU aimed at better identification of excessively burdensome regulation. Substantial efforts are required in this respect, both at EU and national levels.

III. ECONOMIC AND MONETARY UNION

32. Following the December 2012 and June 2013 European Council meetings, the European Council has focused its discussion on banking and economic union but will return to all issues in December 2013. This process builds on the EU's institutional framework, in full respect of the integrity of the single market, while ensuring a level playing-field between EU Member States, including via a fair balance between home and host Member States. It will be open and transparent towards Member States not using the single currency.

Strengthened economic policy coordination

33. Strengthening economic governance is an ongoing process in which significant progress has been achieved in recent years. The European Semester brings the elements together in an integrated process leading to the formulation of policy recommendations.
34. To promote strong, sustainable and inclusive economic growth in the Euro area, the coordination of economic policies needs to be further strengthened, notably by increasing the level of commitment, ownership and implementation of economic policies and reforms in Euro area Member States, underpinned by strong democratic legitimacy and accountability at the level at which decisions are taken and implemented.

35. The European Council underlines that closer coordination of economic policies should be focused on policy areas where positive effects on competitiveness, employment and the functioning of the EMU are most prominent.

As a first step, the European Council will make a shared analysis of the economic situation in the Member States and in the Euro area as such. To this end, it will already hold a discussion in December following the publication of the Commission's Annual Growth Survey and the Alert Mechanism Report with the aim to agree, on the basis of the relevant indicators, on the main areas for coordination of economic policies and reforms.

This shared analysis will be based on an assessment of growth and job-enhancing policies and measures, including the performance of labour and product markets, the efficiency of the public sector, as well as research and innovation, education and vocational training, employment and social inclusion in the Euro area.

The Commission will also provide a first overview of the implementation of country-specific recommendations that will be a basis for the further monitoring of their implementation.

Work will be carried forward to strengthen economic policy coordination, with the objective of taking decisions in December on the main features of contractual arrangements and of associated solidarity mechanisms. This would engage all Euro area Member States but non-Euro area Member States may also choose to enter into similar arrangements. Any such measures must be fully compatible with the Single market in all aspects.

Social dimension

36. The European Council welcomes the European Commission's Communication on the social dimension of the EMU as a positive step and restates the importance of employment and social developments within the European Semester. The use of an employment and social scoreboard in the Joint Employment Report and of employment and social indicators along the lines proposed by the Commission should be pursued, following appropriate work in the relevant Committees, for decision by the Council in December with the objective of using these new instruments as early as the 2014 European Semester. This wider range of indicators has the purpose of allowing a broader understanding on social developments.
37. The coordination of economic, employment and social policies will be further enhanced in line with existing procedures while fully respecting national competences. This requires more work to strengthen cooperation between the various Council configurations in order to ensure consistency of those policies in line with our common objectives.
38. The strengthened economic policy coordination and further measures to enhance the social dimension in the Euro area are voluntary for those outside the single currency and will be fully compatible with the Single Market in all aspects.
39. Finally, the European Council underscores the importance of enhancing the social dialogue involving the social partners both at Member State and European level, in particular in the context of the European Semester, with the objective of enhancing the ownership of its conclusions and recommendations across the Union.

Banking Union

40. The European Council has been actively steering the process of establishing the Banking Union. It welcomes the final adoption by the Council of the Single Supervisory Mechanism and the European Banking Authority (EBA) Amending Regulations. This represents a decisive step towards the Banking Union. The European Council reiterates the principle of non-discrimination of Member States regarding banking supervision and resolution as stated by the European Council in October 2012 and reconfirms the agreed new voting arrangements in the EBA regulation for these matters, which is reflecting an appropriate balance between the participating and non-participating Member States. The European Council also reconfirms its agreement that the review on the operation of the voting arrangements will take place from the date on which the number of non-participating Member States reaches four.

41. The Single Supervisory Mechanism is the first step towards the Banking Union. In November, the European Central Bank will launch a comprehensive assessment of the credit institutions of the Member States participating in the Single Supervisory Mechanism in line with the Regulation conferring specific tasks on the European Central Bank. This will be followed by a stress test of banks across the EU. The European Council considers that this exercise is key to reinforce confidence in the EU banking sector and to restore normal lending conditions to firms and households. The European Council expects full support and cooperation by the national authorities to ensure complete transparency and a rigorous approach, which is key for the credibility of the exercise.

42. In this context, the European Council recalls the urgency, for the Member States taking part in the Single Supervisory Mechanism, of establishing a coordinated European approach in preparation for the comprehensive assessment of credit institutions by the European Central Bank. Member States should make all appropriate arrangements, including national backstops, applying state aid rules. European instruments are available according to their agreed rules. The European Council asks the Council to develop this approach as a matter of urgency and to communicate it by the end of November, in line with the goal that the European Central Bank completes the comprehensive assessment of credit institutions in a timely manner.

It also calls on the Eurogroup to finalise guidelines for European Stability Mechanism direct recapitalisation so that the European Stability Mechanism can have the possibility to recapitalise banks directly, following the establishment of the Single Supervisory Mechanism.

43. Completing the Banking Union is urgent and requires not only a Single Supervisory Mechanism but also a Single Resolution Mechanism. The European Council calls on the legislators to adopt the Bank Recovery and Resolution Directive and the Deposit Guarantee Directive by the end of the year. The European Council underlines the need to align the Single Resolution Mechanism and the Bank Recovery and Resolution Directive as finally adopted. It also underlines the commitment to reach a general approach by the Council on the Commission's proposal for a Single Resolution Mechanism by the end of the year in order to allow for its adoption before the end of the current legislative period.

IV. EASTERN PARTNERSHIP

44. The European Council looks forward to the Eastern Partnership Summit in Vilnius on 28 and 29 November 2013. It underlines the importance of the Eastern Partnership for building a common area of democracy, prosperity and stability across the European continent. The European Council reiterates the European Union's willingness to sign the Association Agreement, including the Deep and Comprehensive Free Trade Area, with Ukraine at the Vilnius Summit, provided there is determined action and tangible progress in line with the Council Conclusions of 10 December 2012, and to launch its provisional application. It confirms the European Union's readiness to initial similar agreements with the Republic of Moldova and Georgia at the Vilnius Summit, with the aim of signing them by Autumn 2014.

V. MIGRATION FLOWS

45. The European Council expresses its deep sadness at the recent and dramatic death of hundreds of people in the Mediterranean which shocked all Europeans. Based on the imperative of prevention and protection and guided by the principle of solidarity and fair sharing of responsibility, determined action should be taken in order to prevent the loss of lives at sea and to avoid that such human tragedies happen again.

46. The European Council underlines the importance of addressing root causes of migration flows by enhancing cooperation with the countries of origin and transit, including through appropriate EU development support and an effective return policy. It also calls for closer cooperation with the relevant international organisations, in particular UNHCR and the International Organisation of Migration in the third countries concerned. Not only in the territory of the EU Member States but also in the countries of origin and transit, the fight against trafficking and smuggling of human beings should be stepped up. Furthermore, the European Council calls for the reinforcement of Frontex activities in the Mediterranean. Swift implementation by Member States of the new European Border Surveillance System (EUROSUR) will be crucial to help detecting vessels in order to protect and save lives at the EU's external borders.
47. The European Council invites the newly established Task Force for the Mediterranean, led by the European Commission and involving Member States, EU agencies and the EEAS, to identify -based on the principles of prevention, protection and solidarity- priority actions for a more efficient use of European policies and tools. The Commission will report to the Council at its meeting of 5-6 December 2013 on the work of the Task Force. The Presidency will report to the European Council in December.
48. The European Council will return to asylum and migration issues in a broader and longer term policy perspective in June 2014, when strategic guidelines for further legislative and operational planning in the area of freedom, security and justice will be defined.

STATEMENT OF HEADS OF STATE OR GOVERNMENT

The Heads of State or Government discussed recent developments concerning possible intelligence issues and the deep concerns that these events have raised among European citizens.

They underlined the close relationship between Europe and the USA and the value of that partnership. They expressed their conviction that the partnership must be based on respect and trust, including as concerns the work and cooperation of secret services.

They stressed that intelligence gathering is a vital element in the fight against terrorism. This applies to relations between European countries as well as to relations with the USA. A lack of trust could prejudice the necessary cooperation in the field of intelligence gathering.

The Heads of State or Government took note of the intention of France and Germany to seek bilateral talks with the USA with the aim of finding before the end of the year an understanding on mutual relations in that field. They noted that other EU countries are welcome to join this initiative.

They also pointed to the existing Working Group between the EU and the USA on the related issue of data protection and called for rapid and constructive progress in that respect.

Dokument 2014/0067392

Von: GII2_
Gesendet: Freitag, 25. Oktober 2013 16:26
An: GIII1_; GI1_; GII2_; GII3_; GII4_; GII5_; GIII4_; OESI2_; OESI3AG_; OESII2_; OESIII3_; PGNSA; MI1_; MI3_; MI4_; VII4_; IT5_; Hübner, Christoph, Dr.; Wolf, Katharina; Popp, Michael; Gitter, Rotraud, Dr.; Schlender, Katharina; Bratanova, Elena; Köpke, Jörg; AA Konther, Michael
Cc: PStSchröder_; PStBergner_; StFritsche_; StRogall-Grothe_; LS_; MB_; ALG_; UALGII_; GIII5_; OESI4_; MI5_; B4_; PGDBOS_; PGDS_; VI4_; IT1_; IT3_; O1_; O2_; O4_; O5_
Betreff: *offizielle Endfassung* (engl.) der Schlussfolgerungen des Europäischen Rates am 24./25.10.2013
Anlagen: st00169.en13.doc

Liebe Kolleginnen und Kollegen,

anbei übermittle ich die offizielle Endfassung (engl. Sprachfassung) der Schlussfolgerungen des Europäischen Rates am 24./25.10.2013.

Die deutsche Sprachfassung liegt hier noch nicht vor, kann jedoch nach ihrer Veröffentlichung im Laufe des heutigen Tages auf folgender offizieller ER-Website (Internet) eingesehen bzw. heruntergeladen werden:

<http://www.consilium.europa.eu/press/press-releases/latest-press-releases/newsroomrelated?bid=76&grp=23903&lang=de>

Gegenüberstellung Abschnitt „MIGRATION FLOWS“ (nunmehr Ziff. 46. bis 49. ER-SF):

Auszug <u>4.</u> Entw. ER-SF	Auszug aus <u>offizieller Endfassung</u> ER-SF
<p>V. <u>MIGRATION FLOWS</u></p> <p>45. The European Council expresses its deep sadness at the recent and dramatic death of hundreds of people in the Mediterranean which shocked all Europeans. Based on the imperative of prevention and protection and guided by the principle of solidarity and fair sharing of responsibility, determined action should be taken in order to prevent the loss of lives at sea and to avoid that such human tragedies happen again.</p>	<p>V. <u>MIGRATION FLOWS</u></p> <p>46. The European Council expresses its deep sadness at the recent and dramatic death of hundreds of people in the Mediterranean which shocked all Europeans. Based on the imperative of prevention and protection and guided by the principle of solidarity and fair sharing of responsibility, determined action should be taken in order to prevent the loss of lives at sea and to avoid that such human tragedies happen again.</p>

46. The European Council underlines the importance of addressing root causes of migration flows by enhancing cooperation with the countries of origin and transit, including through appropriate EU development support and an effective return policy. It also calls for closer cooperation with the relevant international organisations, in particular UNHCR and the International Organisation of Migration in the third countries concerned. Not only in the territory of the EU Member States but also in the countries of origin and transit, the fight against trafficking and smuggling of human beings should be stepped up. Furthermore, the European Council calls for the reinforcement of Frontex activities in the Mediterranean. Swift implementation by Member States of the new European Border Surveillance System (EUROSUR) will be crucial to help detecting vessels in order to protect and save lives at the EU's external borders.

47. The European Council invites the newly established Task Force for the Mediterranean, led by the European Commission and involving Member States, EU agencies and the EEAS, to identify -based on the principles of prevention, protection and solidarity- priority actions for a more efficient use of European policies and tools. The Commission will report to the Council at its meeting of 5-6 December 2013 on the work of the Task Force. The Presidency will report to the European Council in December.

48. The European Council will return to asylum and migration issues in a broader and longer term policy perspective in

47. The European Council underlines the importance of addressing root causes of migration flows by enhancing cooperation with the countries of origin and transit, including through appropriate EU development support and an effective return policy. It also calls for closer cooperation with the relevant international organisations, in particular UNHCR and the International Organisation of Migration in the third countries concerned. Not only in the territory of the EU Member States but also in the countries of origin and transit, the fight against trafficking and smuggling of human beings should be stepped up. Furthermore, the European Council calls for the reinforcement of Frontex activities in the Mediterranean and along the Southeastern borders of the EU. Swift implementation by Member States of the new European Border Surveillance System (EUROSUR) will be crucial to help detecting vessels and illegal entries, contributing to protecting and saving lives at the EU's external borders.

48. The European Council invites the newly established Task Force for the Mediterranean, led by the European Commission and involving Member States, EU agencies and the EEAS, to identify -based on the principles of prevention, protection and solidarity - priority actions for a more efficient short term use of European policies and tools. The Commission will report to the Council at its meeting of 5-6 December 2013 on the work of the Task Force with a view of taking operational decisions. The Presidency will report to the European Council in December.

49. The European Council will return to asylum and migration issues in a broader

June 2014, when strategic guidelines for further legislative and operational planning in the area of freedom, security and justice will be defined.

and longer term policy perspective in June 2014, when strategic guidelines for further legislative and operational planning in the area of freedom, security and justice will be defined.

Beste Grüße
i.A.
Roland Arhelger

BMI-Referat G II 2
EU-Grundsatzfragen einschließlich
Schengenangelegenheiten;
Beziehungen zum Europäischen Parlament;
Europabeauftragte
Bundesministerium des Innern
Alt-Moabit 101 D,
10559 Berlin
Tel. +49 (0)30 18 681 - 2370
Fax +49 (0)30 18 681 - 52370
e-mail: roland.arhelger@bmi.bund.de

Von: E01-3 Kluck, Jan [mailto:e01-3@auswaertiges-amt.de]

Gesendet: Freitag, 25. Oktober 2013 15:07

An: BK Felsheim, Georg; BK Meyer, Anke; BK Dopheide, Jan Hendrik; ref503@bk.bund.de; Ludwig.Blaurock@bk.bund.de; BK Uslar-Gleichen, Freiin von, Tania; ref501@bk.bund.de; BK Ruge, Undine; BK Konow, Christian; BKM-EUBeauftragter; GII2_; Arhelger, Roland; MI5_; VI4_; Bender, Ulrike; Wolf, Katharina; BMJ Meyer-Cabri, Klaus Jörg; euro@bmj.bund.de; BMJ Laitenberger, Angelika; BMJ Teichman und Logischen, Bettina von; BMF Ahrens, Susanne; BMF Pohnert, Jürgen; BMF Müller, Ralph; BMF Wiechoczek, Oliver; BMF Göttlinger, Elisabeth; BMWI Lepers, Rudolf; BMWI BUERO-EA1; BMWI Zoll, Ingrid; klauspeter.leier@bmwi.bund.de; BMWI Grzondziel, Julia; BMWI Kunhenn, Dieter; BMAS Referat VI a 1; BMAS Klitscher, Stephan; BMAS Winkler, Holger; BMAS Jobelius, Sebastian; BMAS Hess, Regula; BMELV Referat 612; BMELV Burbach, Rolf; BMVG BMVg Pol I 4; BMFSFJ Freitag, Heinz; BMFSFJ Elping, Nicole; 317@bmfsfj.bund.de; BMG Z32; BMG Langbein, Birte; BMVBS John-Ruff, Gudrun; BMVBS ref-ui20; EIII2@bmu.bund.de; BMU Kracht, Eva; BMU Werner, Julia; BMU Ernstberger, Christian; BMU Münchhausen, Marie-Louise von; 221@bmbf.bund.de; dokumente.413@bmz.bund.de; BMZ Gruschinski, Bernd; BMZ Kreipe, Nils; BPA 301; BPA Köhn, Ulrich

Cc: AA Dittmann, Axel; AA Jokisch, Jens

Betreff: Schlussfolgerungen des Europäischen Rats

Liebe Kolleginnen und Kollegen,
anbei die endgültige Fassung der ER-Schlussfolgerungen (englischsprachige Version).
Viele Grüße,
Jan Kluck



EUROPEAN COUNCIL

Brussels, 25 October 2013

EUCO 169/13

**CO EUR 13
CONCL 7**

COVER NOTE

from : General Secretariat of the Council
to : Delegations
Subject : **EUROPEAN COUNCIL
24/25 OCTOBER 2013**

CONCLUSIONS

Delegations will find attached the conclusions of the European Council (24/25 October 2013).

Signs of economic recovery are visible but the EU needs to pursue its efforts to increase growth potential, enhance job creation and boost European competitiveness. Today the European Council focused on the digital economy, innovation and services. These areas have a particular potential for growth and jobs which must be rapidly mobilized. The European Council provided concrete guidance so as to take full advantage of the existing potential.

The European Council also looked at different economic and social policy areas. It took stock of the implementation of the initiatives taken in June in the fight against youth unemployment and the financing of the economy, in particular of small and medium-sized enterprises, and agreed on additional measures. It gave a new impetus to better regulation.

The European Council held an in-depth discussion on completing the Economic and Monetary Union. It focused in particular on enhanced economic policy coordination, strengthening the social dimension of the Economic and Monetary Union and completing the Banking Union. As decided in June, the European Council will return to all these elements in December with a view to taking decisions.

The European Council looked ahead to the Eastern Partnership Summit which will be held in Vilnius on 28 and 29 November 2013.

The European Council expressed its deep sadness at the recent tragic events in the Mediterranean in which hundreds of people lost their lives and decided to step up the Union's action so as to prevent such tragedies from happening again.

I. DIGITAL ECONOMY, INNOVATION AND SERVICES

1. A strong digital economy is vital for growth and European competitiveness in a globalised world. To this end, all efforts must be made for Europe's industry to regain momentum in digital products and services. There is an urgent need for an integrated single digital and telecoms market, benefiting consumers and companies. As part of its growth strategy, Europe must boost digital, data-driven innovation across all sectors of the economy. Special consideration should be given to supporting the reduction of the digital gap among Member States.

Investing in the digital economy

2. To tap the full potential of the digital economy, to boost productivity and create new economic activity and skilled jobs, Europe needs investment and the right regulatory framework. New investments should be promoted to accelerate the roll-out of infrastructure capable of achieving the broadband speed targets of the Digital Agenda for Europe, and to accelerate the deployment of new technologies, such as 4G, while maintaining technology neutrality. Legislative measures to reduce the cost of broadband roll-out should be adopted rapidly.

3. Several strategic technologies such as Big Data and Cloud computing are important enablers for productivity and better services. Cloud computing should improve access to data and simplify their sharing. Big Data aims to process, collect, store and analyse large amounts of data. EU action should provide the right framework conditions for a single market for Big Data and Cloud computing, in particular by promoting high standards for secure, high-quality and reliable cloud services. The European Commission and the Member States, with the support of the "European Cloud Partnership", should continue to make every effort to put Europe at the forefront of cloud adoption. The European Council calls for the establishment of a strong network of national digital coordinators which could play a strategic role in Cloud, Big Data and Open Data development.

4. The ongoing work to tackle tax evasion, tax fraud, aggressive tax planning, tax-base erosion and profit shifting is also important for the digital economy. Member States should further coordinate their positions where appropriate in order to achieve the best possible solution for Member States and the EU in the OECD/BEPS (Base Erosion and Profit Shifting) framework. In its ongoing VAT review, the Commission will also address issues which are specific to the digital economy, such as differentiated tax rates for digital and physical products. The European Council welcomes the Commission's initiative to set up an expert group on taxation of the digital economy. The European Council will return to taxation-related issues at its December 2013 meeting.

Promoting a consumer and business-friendly Digital Single Market

5. Overcoming fragmentation, promoting effective competition and attracting private investment through an improved, predictable and stable EU-wide legal framework is crucial, while ensuring a high level of consumer protection and allowing Member States a degree of flexibility to take additional consumer protection measures. In this context, the European Council welcomes the presentation by the Commission of the "Connected Continent" package and encourages the legislator to carry out an intensive examination with a view to its timely adoption. It underlines the importance of better coordinating the timing and conditions of spectrum assignment, while respecting national competences in this area.
6. The commitment to complete the Digital Single Market by 2015 has to be delivered on: today's market fragmentation hampers the release of the digital economy's full potential. This requires a comprehensive approach fostering innovation and competition in digital services.

7. No efforts should be spared to accelerate work on the pending legislative proposals, in particular the proposals on e-identification and trust services and on e-invoicing and payment services, so that they can be adopted by the end of the legislative period. There is also a need to address the bottlenecks in accessing one's "digital life" from different platforms which persist due to a lack of interoperability or lack of portability of content and data. This hampers the use of digital services and competition. An open and non-discriminatory framework must therefore be put in place to ensure such interoperability and portability without hindering development of the fast moving digital sphere and avoiding unnecessary administrative burden, especially for SME's. Providing digital services and content across the single market requires the establishment of a copyright regime for the digital age. The Commission will therefore complete its ongoing review of the EU copyright framework in Spring 2014. It is important to modernise Europe's copyright regime and facilitate licensing, while ensuring a high level of protection of intellectual property rights and taking into account cultural diversity.
8. It is important to foster the trust of citizens and businesses in the digital economy. The timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015.
9. The modernisation of public administrations should continue through the swift implementation of services such as e-government, e-health, e-invoicing and e-procurement. This will lead to more and better digital services for citizens and enterprises across Europe, and to cost savings in the public sector. Open data is an untapped resource with a huge potential for building stronger, more interconnected societies that better meet the needs of the citizens and allow innovation and prosperity to flourish. Interoperability and the re-use of public sector information shall be promoted actively. EU legislation should be designed to facilitate digital interaction between citizens and businesses and the public authorities. Efforts should be made to apply the principle that information is collected from citizens only once, in due respect of data protection rules.

Improving skills

10. Users must have the necessary digital skills. Many European citizens and enterprises currently do not use IT sufficiently. This results in a growing difficulty in filling digital jobs. In 2011, the European Union was faced with 300 000 unfilled vacancies in the ICT sector; if this trend is not checked, there could be as many as 900 000 unfilled vacancies by 2015. This skills mismatch is detrimental to our economic and social policy objectives.

11. Concrete steps should be taken in order to redress this situation:
 - a) part of the European Structural and Investment Funds (2014-2020) should be used for ICT education, support for retraining, and vocational education and training in ICT, including through digital tools and content, in the context of the Youth Employment Initiative;

 - b) a higher degree of integration of digital skills in education, from the earliest stages of school to higher education, vocational education and training and lifelong learning should be ensured;

 - c) the Grand Coalition for Digital Jobs should be strengthened to address skills mismatches by supporting targeted labour mobility schemes and the use of the newly developed classification of European Skills/Competences, Qualifications and Occupations (ESCO);

 - d) the Commission will further intensify work on the basis of the EU Skills Panorama for digital jobs in order to accelerate progress on pan-European competences frameworks for digital skills.

12. In all three areas - investments, Digital Single Market and improving skills - a strong commitment is vital if the objective of enhancing growth, competitiveness and jobs is to be achieved. The European Council calls on the Council and the Commission to take forward this agenda and will return to the matter in the course of 2014.

Innovation

13. Investment in research and innovation fuels productivity and growth and is key for job creation. Member States that have continued to invest in research and innovation have fared better in the current crisis than those that have not.
14. In February 2011, the European Council called for a strategic and integrated approach to boost innovation and take full advantage of Europe's intellectual capital. It set out specific steps to achieve this. Two years on, a significant number of them are on track. Joint programming in research and innovation is developing. Annual monitoring of progress on innovation is taking place in the framework of the Europe 2020 strategy. The establishment of a Research and Innovation Observatory by the Commission is under way. A number of programmes providing funding to research and innovation are being finalised. As requested, the Commission recently proposed a single Indicator of Innovation Output which should allow for better monitoring.
15. The Union's intellectual and scientific potential does not always translate into new products and services that can be sold on markets. The main reasons for this commercialisation gap are: difficulties in accessing finance, market barriers and excessive red tape. The grouping of research institutes and industry ("clusters") can provide the ground for fruitful interaction between them and for the emergence of new products, services and industries.

16. Europe needs a better-coordinated use of tools such as grants, pre-commercial public procurement and venture capital, and an integrated approach from research and innovation to market deployment. Special attention should be paid to the role of the public sector in enabling systemic innovations, especially in the cleantech and biotech sectors. The 2010 Innovation Union flagship initiative provides a number of valuable instruments which, combined with financing programmes, such as Competitiveness of Enterprises and SMEs (COSME) and Horizon 2020, including the Risk-Sharing Finance Facility, can support innovation and its impact on the market. The proposals for Joint Technology Initiatives in pharmaceuticals, new energy technologies, aeronautics, the bio-based economy and electronics should be adopted as soon as possible. Efforts should also continue at national level.

17. In order to obtain a full European Research Area by the end of 2014, it is important to accelerate structural reforms of national systems and to strengthen progress monitoring based on robust data provided by Member States. The progress report submitted by the Commission identifies some areas which require more efforts. In particular, we must improve the mobility and career prospects of researchers through adequate pensions solutions, transnational access to research infrastructures and open access to publicly funded research results and knowledge transfer as part of innovation strategies at national and European levels.

18. The European Council invites the Commission and the Member States to continue their efforts in the area of innovation and research. It will take stock of progress at its meeting in February 2014.

Services and Trade

19. Services are a fundamental part of the Single Market. To reap the full economic benefits, Member States urgently need to improve implementation of the Services Directive and thus speed up the opening of services markets. All opportunities should be seized in this respect; unjustified or disproportionate barriers should be removed in order to ensure a level playing-field on the services market. The European Council invites the Commission and the Council to provide yearly progress reports on national reforms on services, including in individual sectors, and invites the Commission to make proposals by March 2014.
20. The European Council welcomes the peer review of the Services Directive presented by the Commission. It agrees that all Member States should ensure systematic, thorough and robust proportionality assessments of their regulatory requirements. In particular, Member States should address disproportionate barriers. The European Council invites the Commission to provide additional guidance to Member States on the concept of proportionality and invites Member States to take full account of best practices.
21. The European Council stresses the importance of the mutual evaluation of regulated professions launched by the Commission and calls for swift progress. This exercise should identify the remaining barriers to access to professions in the Member States, assess the cumulative effect of all restrictions imposed on the same profession, and suggest appropriate action.
22. The European Council reiterates the importance of trade as an engine for growth and job creation, in line with its conclusions of February 2013. It welcomes the political agreement on the key elements of a Comprehensive Economic and Trade Agreement with Canada and looks forward to the swift examination by the European Parliament and the Council. This agreement will provide significant new opportunities for companies in the EU and in Canada and will give an important impetus to enhanced trade relations between both sides of the Atlantic.

II. ECONOMIC AND SOCIAL POLICY

Combating youth unemployment

23. The fight against youth unemployment remains a key objective of the EU strategy to foster growth, competitiveness and jobs. The European Council recalls the need for the Youth Employment Initiative to be fully operational by January 2014, which will allow the first disbursements to beneficiaries to be made. It calls on the Member States to mobilise all efforts necessary to this end.
24. The European Council also calls for rapid implementation by the Member States of the Youth Guarantee and the Council declaration on the European Alliance for Apprenticeships. It points out that Member States benefiting from the Youth Employment Initiative need to adopt plans to tackle youth unemployment, including through the implementation of the "Youth Guarantee", before the end of 2013 in order to benefit rapidly from the initiative. In this context, the European Council welcomes the upcoming Paris Conference.

Financing of the economy

25. All efforts should continue to restore normal lending to the economy and facilitate financing of investment, particularly with respect to small and medium-sized enterprises (SMEs).

26. The programming negotiations of the European Structural and Investment Funds (ESIF) should be used to significantly increase the overall EU support from these funds to leverage-based financial instruments for SMEs in 2014-2020, while at least doubling support in countries where conditions remain tight. These instruments should be designed in a way which limits market fragmentation, ensures high leverage effects and quick uptake by the SMEs. This will help concentrate the funds adequately and expand the volume of new loans to SMEs.

27. The European Council takes note of the reports by the Commission and the EIB on the implementation of measures aimed at financing the economy and invites Member States to make good use of the opportunities provided. It reiterates its call to expand joint risk-sharing financial instruments between the Commission and the European Investment Bank (EIB) to leverage private sector and capital market investments in SMEs, with the aim of expanding the volume of new loans to SMEs across the EU. Work should be finalized to amend the Common Provisions Regulation to enable the use of guarantees. The new instruments should achieve high leverage effects and be attractive for private sector and capital markets investment. The EIB should start implementing them while work should start immediately on further developing tools for the future, especially on securitisation. While contributions to the SME initiative should remain voluntary, the European Council calls for the greatest possible participation by Member States. Participating Member States will inform the Commission and the EIB about their contributions by the end of the year. The new instruments should begin operating in January 2014 to accompany recovery, fight unemployment and reduce fragmentation in the initial years of the financial framework.

28. The role of the Union's budget in providing opportunities to SMEs is crucial. In this context, the European Council welcomes the agreement on the COSME and Horizon 2020 programmes and points out that their implementation is a matter of priority. It also encourages the legislator to work swiftly on the proposed legislation on long-term investment funds with a view to its adoption before the end of the legislative period.

Regulatory fitness

29. Regulation at Union level is necessary in order to ensure that EU policy goals, including the proper functioning of the Single Market, are attained. This should be achieved with a maximum of transparency and simplicity and a minimum of costs while always taking account of the need for a proper protection of consumers, health, the environment and employees.
30. The European Council welcomes the recent Commission Communication on regulatory fitness (REFIT), which acknowledges work already undertaken in recent years to alleviate the burden of legislation, in particular for SMEs, and proposes ambitious further steps to make the EU regulatory framework lighter. The European Council calls on the Commission to make further substantial proposals in this field.
31. The European Council urges the Commission and the legislator to rapidly implement the REFIT programme, *inter alia* through simplification of existing EU law, by withdrawing proposals that are no longer needed and by repealing legislation that is out of date.

32. To this end, the European Council underlines the need to monitor progress by means of a comprehensive scoreboard to track progress at the European and national level and facilitate dialogue on regulatory fitness. It welcomes the steps taken by the Member States and the EU aimed at better identification of excessively burdensome regulation, noting in this respect the subsidiarity and proportionality principles. Substantial efforts are required in this respect, both at EU and national levels. The European Council looks forward to agreeing further steps in this direction at its June meeting and will return to the issue annually as part of the European Semester.

III. ECONOMIC AND MONETARY UNION

33. Following the December 2012 and June 2013 European Council meetings, the European Council has focused its discussion on banking and economic union but will return to all issues in December 2013. This process builds on the EU's institutional framework, in full respect of the integrity of the single market, while ensuring a level playing-field between EU Member States, including via a fair balance between home and host Member States. It will be open and transparent towards Member States not using the single currency.

Strengthened economic policy coordination

34. Strengthening economic governance is an ongoing process in which significant progress has been achieved in recent years. The European Semester brings the elements together in an integrated process leading to the formulation of policy recommendations.
35. To promote strong, sustainable and inclusive economic growth in the Euro area, the coordination of economic policies needs to be further strengthened, notably by increasing the level of commitment, ownership and implementation of economic policies and reforms in Euro area Member States, underpinned by strong democratic legitimacy and accountability at the level at which decisions are taken and implemented.

36. The European Council underlines that closer coordination of economic policies should be focused on policy areas where positive effects on competitiveness, employment and the functioning of the EMU are most prominent.

As a first step, the European Council will make a shared analysis of the economic situation in the Member States and in the Euro area as such. To this end, it will already hold a discussion in December following the publication of the Commission's Annual Growth Survey and the Alert Mechanism Report with the aim to agree, on the basis of the relevant indicators, on the main areas for coordination of economic policies and reforms.

This shared analysis will be based on an assessment of growth and job-enhancing policies and measures, including the performance of labour and product markets, the efficiency of the public sector, as well as research and innovation, education and vocational training, employment and social inclusion in the Euro area.

The Commission will also provide a first overview of the implementation of country-specific recommendations that will be a basis for the further monitoring of their implementation.

Work will be carried forward to strengthen economic policy coordination, with the objective of taking decisions in December on the main features of contractual arrangements and of associated solidarity mechanisms. This would engage all Euro area Member States but non-Euro area Member States may also choose to enter into similar arrangements. Any such measures must be fully compatible with the Single market in all aspects.

Social dimension

37. The European Council welcomes the European Commission's Communication on the social dimension of the EMU as a positive step and restates the importance of employment and social developments within the European Semester. The use of an employment and social scoreboard in the Joint Employment Report and of employment and social indicators along the lines proposed by the Commission should be pursued, following appropriate work in the relevant Committees, for decision by the Council in December, confirmed by the European Council with the objective of using these new instruments as early as the 2014 European Semester. This wider range of indicators has the purpose of allowing a broader understanding on social developments.
38. The coordination of economic, employment and social policies will be further enhanced in line with existing procedures while fully respecting national competences. This requires more work to strengthen cooperation between the various Council configurations in order to ensure consistency of those policies in line with our common objectives.
39. The strengthened economic policy coordination and further measures to enhance the social dimension in the Euro area are voluntary for those outside the single currency and will be fully compatible with the Single Market in all aspects.
40. Finally, the European Council underscores the importance of enhancing the social dialogue involving the social partners both at Member State and European level, in particular in the context of the European Semester, with the objective of enhancing the ownership of its conclusions and recommendations across the Union.

Banking Union

41. The European Council has been actively steering the process of establishing the Banking Union. It welcomes the final adoption by the Council of the Single Supervisory Mechanism and the European Banking Authority (EBA) Amending Regulations. This represents a decisive step towards the Banking Union. The European Council reiterates the principle of non-discrimination of Member States regarding banking supervision and resolution as stated by the European Council in October 2012 and reconfirms the agreed new voting arrangements in the EBA regulation for these matters, which is reflecting an appropriate balance between the participating and non-participating Member States. The European Council also reconfirms its agreement that the review on the operation of the voting arrangements will take place from the date on which the number of non-participating Member States reaches four.

42. The Single Supervisory Mechanism is the first step towards the Banking Union. In November, the European Central Bank will launch a comprehensive assessment of the credit institutions of the Member States participating in the Single Supervisory Mechanism in line with the Regulation conferring specific tasks on the European Central Bank. This will be followed by a stress test of banks across the EU. The European Council considers that this exercise is key to reinforce confidence in the EU banking sector and to restore normal lending conditions to firms and households. The European Council expects full support and cooperation by the national authorities to ensure complete transparency and a rigorous approach, which is key for the credibility of the exercise.

43. In this context, the European Council recalls the urgency, for the Member States taking part in the Single Supervisory Mechanism, of establishing a coordinated European approach in preparation for the comprehensive assessment of credit institutions by the European Central Bank. Member States should make all appropriate arrangements, including national backstops, applying state aid rules. European instruments are available according to their agreed rules. The European Council asks the Council to develop this approach as a matter of urgency and to communicate it by the end of November, in line with the goal that the European Central Bank completes the comprehensive assessment of credit institutions in a timely manner.

It also calls on the Eurogroup to finalise guidelines for European Stability Mechanism direct recapitalisation so that the European Stability Mechanism can have the possibility to recapitalise banks directly, following the establishment of the Single Supervisory Mechanism.

44. Completing the Banking Union is urgent and requires not only a Single Supervisory Mechanism but also a Single Resolution Mechanism. The European Council calls on the legislators to adopt the Bank Recovery and Resolution Directive and the Deposit Guarantee Directive by the end of the year. The European Council underlines the need to align the Single Resolution Mechanism and the Bank Recovery and Resolution Directive as finally adopted. It also underlines the commitment to reach a general approach by the Council on the Commission's proposal for a Single Resolution Mechanism by the end of the year in order to allow for its adoption before the end of the current legislative period.

IV. EASTERN PARTNERSHIP

45. The European Council looks forward to the Eastern Partnership Summit in Vilnius on 28 and 29 November 2013. It underlines the importance of the Eastern Partnership for building a common area of democracy, prosperity and stability across the European continent. The European Council reiterates the European Union's willingness to sign the Association Agreement, including the Deep and Comprehensive Free Trade Area, with Ukraine at the Vilnius Summit, provided there is determined action and tangible progress in line with the Council Conclusions of 10 December 2012, and to launch its provisional application. It confirms the European Union's readiness to initial similar agreements with the Republic of Moldova and Georgia at the Vilnius Summit, with the aim of signing them by Autumn 2014.

V. MIGRATION FLOWS

46. The European Council expresses its deep sadness at the recent and dramatic death of hundreds of people in the Mediterranean which shocked all Europeans. Based on the imperative of prevention and protection and guided by the principle of solidarity and fair sharing of responsibility, determined action should be taken in order to prevent the loss of lives at sea and to avoid that such human tragedies happen again.

47. The European Council underlines the importance of addressing root causes of migration flows by enhancing cooperation with the countries of origin and transit, including through appropriate EU development support and an effective return policy. It also calls for closer cooperation with the relevant international organisations, in particular UNHCR and the International Organisation of Migration in the third countries concerned. Not only in the territory of the EU Member States but also in the countries of origin and transit, the fight against trafficking and smuggling of human beings should be stepped up. Furthermore, the European Council calls for the reinforcement of Frontex activities in the Mediterranean and along the Southeastern borders of the EU. Swift implementation by Member States of the new European Border Surveillance System (EUROSUR) will be crucial to help detecting vessels and illegal entries, contributing to protecting and saving lives at the EU's external borders.

48. The European Council invites the newly established Task Force for the Mediterranean, led by the European Commission and involving Member States, EU agencies and the EEAS, to identify -based on the principles of prevention, protection and solidarity - priority actions for a more efficient short term use of European policies and tools. The Commission will report to the Council at its meeting of 5-6 December 2013 on the work of the Task Force with a view of taking operational decisions. The Presidency will report to the European Council in December.

49. The European Council will return to asylum and migration issues in a broader and longer term policy perspective in June 2014, when strategic guidelines for further legislative and operational planning in the area of freedom, security and justice will be defined.

STATEMENT OF HEADS OF STATE OR GOVERNMENT

The Heads of State or Government discussed recent developments concerning possible intelligence issues and the deep concerns that these events have raised among European citizens.

They underlined the close relationship between Europe and the USA and the value of that partnership. They expressed their conviction that the partnership must be based on respect and trust, including as concerns the work and cooperation of secret services.

They stressed that intelligence gathering is a vital element in the fight against terrorism. This applies to relations between European countries as well as to relations with the USA. A lack of trust could prejudice the necessary cooperation in the field of intelligence gathering.

The Heads of State or Government took note of the intention of France and Germany to seek bilateral talks with the USA with the aim of finding before the end of the year an understanding on mutual relations in that field. They noted that other EU countries are welcome to join this initiative.

They also pointed to the existing Working Group between the EU and the USA on the related issue of data protection and called for rapid and constructive progress in that respect.



Dokument 2014/0067395

Von: Weinbrenner, Ulrich
Gesendet: Freitag, 8. November 2013 18:38
An: PGNSA
Betreff: WG: EP Studie zur nationalen Überwachungsinstrumenten/
programmen
Anlagen: 20131021_LIBE_Study - ET(2013)493032_EN.pdf

zKts.

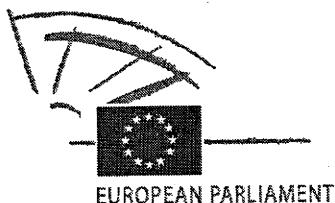
Mit freundlichem Gruß

Ulrich Weinbrenner

Bundesministerium des Innern
Leiter der Arbeitsgruppe ÖS I 3
Polizeiliches Informationswesen, BKA-Gesetz,
Datenschutz im Sicherheitsbereich
Tel.: + 49 30 3981 1301
Fax.: + 49 30 3981 1438
PC-Fax.: 01888 681 51301
Ulrich.Weinbrenner@bmi.bund.de

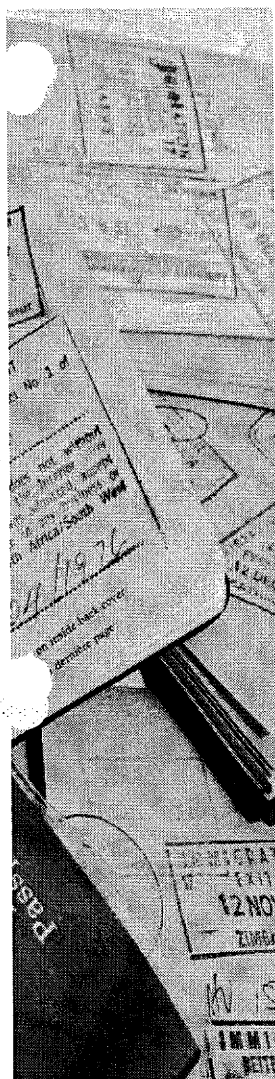
Von: .BRUEEU POL-IN2-2-EU Eickelpasch, Joerg [mailto:pol-in2-2-eu@brue.auswaertiges-amt.de]
Gesendet: Montag, 28. Oktober 2013 08:31
An: Weinbrenner, Ulrich; Jergl, Johann
Cc: t.pohl@diplo.de
Betreff: EP Studie zur nationalen Überwachungsinstrumenten/ programmen

Beigefügte Studie zur Info. Sie wird – wie angekündigt -- Gegenstand einer der LIBE-Sitzungen im November sein.
Viele Grüße,
Jörg Eickelpasch



DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT **C**
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS



Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law

STUDY





DIRECTORATE GENERAL FOR INTERNAL POLICIES
POLICY DEPARTMENT C:
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

**NATIONAL PROGRAMMES FOR MASS
SURVEILLANCE OF PERSONAL DATA
IN EU MEMBER STATES AND THEIR
COMPATIBILITY WITH EU LAW**

STUDY

Abstract

In the wake of the disclosures surrounding PRISM and other US surveillance programmes, this study makes an assessment of the large-scale surveillance practices by a selection of EU member states: the UK, Sweden, France, Germany and the Netherlands. Given the large-scale nature of surveillance practices at stake, which represent a reconfiguration of traditional intelligence gathering, the study contends that an analysis of European surveillance programmes cannot be reduced to a question of balance between data protection versus national security, but has to be framed in terms of collective freedoms and democracy. It finds that four of the five EU member states selected for in-depth examination are engaging in some form of large-scale interception and surveillance of communication data, and identifies parallels and discrepancies between these programmes and the NSA-run operations. The study argues that these surveillance programmes do not stand outside the realm of EU intervention but can be engaged from an EU law perspective via (i) an understanding of national security in a democratic rule of law framework where fundamental human rights standards and judicial oversight constitute key standards; (ii) the risks presented to the internal security of the Union as a whole as well as the privacy of EU citizens as data owners, and (iii) the potential spillover into the activities and responsibilities of EU agencies. The study then presents a set of policy recommendations to the European Parliament.

This document was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs.

AUTHORS

Prof. Didier Bigo, Director of the Centre d'Etudes sur les Conflits, Liberté et Sécurité (CCLS) and Professor at Sciences-Po Paris and King's College London

Dr. Sergio Carrera, Senior Research Fellow and Head of the Justice and Home Affairs Section, Centre for European Policy Studies, CEPS

Mr. Nicholas Hernanz, Research Assistant, Justice and Home Affairs Section, CEPS

Dr. Julien Jeandesboz, Assistant Professor at the University of Amsterdam and Associate Researcher at CCLS

Ms. Joanna Parkin, Researcher, Justice and Home Affairs Section, CEPS

Dr. Francesco Ragazzi, Assistant Professor in International Relations, Leiden University

Dr. Amandine Scherrer, European Studies Coordinator and Associate Researcher at CCLS.

The authors would like to thank the following experts who have contributed to the research of this briefing note: Axel Arnbak, cybersecurity and information law researcher at the Institute for Information Law, University of Amsterdam; Jelle van Buuren, Leiden University, Center for Terrorism and Counter-terrorism; Ot van Daalen, Bits of Freedom; and Mark Klamberg, Senior Lecturer at the Department of Law of Uppsala University.

RESPONSIBLE ADMINISTRATOR

Mr Alessandro DAVOLI

Policy Department Citizens' Rights and Constitutional Affairs

European Parliament

B-1047 Brussels

E-mail: alessandro.davoli@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

To contact the Policy Department or to subscribe to its monthly newsletter please write to: poldep-citizens@europarl.europa.eu

Manuscript completed in October 2013.

Source: European Parliament, © European Union, 2013

This document is available on the Internet at:

<http://www.europarl.europa.eu/studies>

DISCLAIMER

The opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the publisher is given prior notice and sent a copy.

CONTENT

EXECUTIVE SUMMARY	5
INTRODUCTION	7
1. Controversy between the actors about the scale of the problem	11
1.1. Large scale electronic surveillance in democracies: compatibility or not?	12
1.2. Political and ethical controversies regarding the use of these technologies by intelligence services: the question of legitimacy	16
2. The EU member states practices in the context of the revelations of NSA large scale operations	19
2.1. Technical features	20
2.2. Scale	21
2.3. Data types and data targets	22
2.4. Processing and analysis of data	23
2.5. Cooperation between national and international security actors	24
2.6. Legal regimes and oversight	25
3. Legal Modalities of Action at EU level and Compatibility with EU Law	27
3.1. National Security and Democratic Rule of Law	28
3.2. Whose Security? Sincere Cooperation and Citizens' Liberties Compromised	34
3.3. Home Affairs Agencies	36
4. Conclusions and Recommendations: Implications of Large Scale Surveillance for Freedom, Fundamental Rights, Democracy and Sovereignty in the EU	39
4.1. General conclusions	39
4.2. Policy Recommendations	42
List of academic references	48
ANNEX 1 - The EU member states practices in the context of the revelations of NSA large scale operations	50

EXECUTIVE SUMMARY

Surveillance of population groups is not a new phenomenon in liberal regimes and the series of scandals surrounding the surveillance programmes of the US' NSA and UK's GCHQ only reminds us of the recurrence of transgressions and illegal practices carried out by intelligence services. However, the scale of surveillance revealed by Edward Snowden should not be simply understood as a routine practice of intelligence services. Several aspects emerged from this series of revelations that directly affect EU citizens' rights and EU institutions' credibility in safeguarding those rights.

First, these revelations uncover **a reconfiguration of surveillance that enables access to a much larger scale of data** than telecommunication surveillance of the past. Progress in technologies allows a much larger scope for surveillance, and platforms for data extraction have multiplied.

Second, the distinction between targeted surveillance for criminal investigations purposes, which can be legitimate if framed according to the rule of law, and large-scale surveillance with unclear objectives is increasingly blurred. **It is the purpose and the scale of surveillance that are precisely at the core of what differentiates democratic regimes and police states.**

Third, the intelligence services have not yet provided acceptable answers to the recent accusations raised towards them. This raises the **issue of accountability of intelligence services and their private sector partners** and reinforces the need for a strengthened oversight.

In light of these elements, the briefing paper starts by suggesting that an **analysis of European surveillance programmes cannot be reduced to the question of a balance between data protection versus national security**, but has to be framed in terms of collective freedoms and democracy (Section 1). This section underlines the fact that it is the scale of surveillance that is at the heart of the current controversy.

The second section of the briefing paper outlines the main characteristics of large-scale telecommunications surveillance activities/capacities of five EU member states: UK, Sweden, France, Germany and the Netherlands (Section 2). This section reveals in particular the following:

- Practices of so-called 'upstreaming' (tapping directly into the communications infrastructure as a means to intercept data) characterise the surveillance programmes all the selected EU member states, with the exception of the Netherlands for whom there is, to date, no concrete evidence of engagement in large-scale surveillance.
- The capacities of Sweden, France and Germany (in terms of budget and human resources) are low compared to the magnitude of the operations launched by GCHQ and the NSA and cannot be considered on the same scale.
- There is a multiplicity of intelligence/security actors involved in processing and exploiting data, including several, overlapping transnational intelligence networks dominated by the US.
- Legal regulation of communications surveillance differs across the member states examined, however in general legal frameworks are characterised by ambiguity or loopholes as regards large-scale communications surveillance, while national oversight bodies lack the capacities to effectively monitor the lawfulness of intelligence services' large scale interception of data.

This empirical analysis furthermore underlines **the two key issues remaining unclear given the lack of information and the secretive attitude of the services involved in these surveillance programmes**: what/who are the ultimate targets of this surveillance exercise, and how are data collected, processed, filtered and analysed?

The paper then presents modalities of action at the disposal of EU institutions to counter unlawful large-scale surveillance (Section 3). This section underlines that even if intelligence activities are said to remain within the scope of member states exclusive competences in the EU legal system, **this does not necessarily means that member states' surveillance programmes are entirely outside the remits of the EU's intervention.** The ECHR, as well as the EU Charter of Fundamental Rights, could here play a significant role, especially given the fact that, from a legal point of view, EU surveillance programmes are incompatible with minimum democratic rule of law standards and compromise the security and fundamental human rights of citizens and residents in the EU. The forthcoming revision of Europol's legal mandate also appears to be a timely occasion to address the issue of EU competence and liability in sharing and exploiting data generated by national large-scale surveillance operations and to ensure greater accountability and oversight of this agency's actions.

The briefing paper concludes that **a lack of actions of the European Parliament would profoundly undermine the trust and confidence that EU citizens have in the European institutions.** A set of recommendations is finally outlined, suggesting further steps to be drawn from the LIBE committee's inquiry.

INTRODUCTION

Stating the scope of the problem

As already stated by the European Parliament in July 2013, following the revelations of Edward Snowden published by the Guardian and the Washington Post on 6 June 2013 concerning the NSA activities and the European services working with them, it appears that:

- First, the US authorities are accessing and processing personal data of EU citizens on a large scale via, among others, the National Security Agency's (NSA) warrantless wiretapping of cable-bound internet traffic (UPSTREAM)¹ and direct access to the personal data stored in the servers of US-based private companies such as Microsoft, Yahoo, Google, Apple, Facebook or Skype² (PRISM). This allows the US authorities to access both stored communications as well as perform real-time collection on targeted users, through cross-database search programmes such as X-KEYSCORE.³ UPSTREAM, PRISM and X-KEYSCORE are only three of the most publicised programmes, and represent the tip of the iceberg of the NSA's surveillance.⁴
- Second, the UK intelligence agency Government Communications Headquarters (GCHQ) has cooperated with the NSA and has initiated actions of interception under a programme code-named TEMPORA.⁵ Further reports have emerged implicating a handful of other EU member states that may be running (Sweden, France, Germany) or developing (potentially the Netherlands) their own large-scale internet interception programmes, and collaborating with the NSA in the exchange of data.
- Third, EU institutions and EU Member State embassies and representations have been subjected to US-UK surveillance and spying activities. The LIBE Committee recently received testimonies about how the UK GCHQ infiltrated Belgacom systems in what was codenamed 'Operation Socialist' to gain access to the data of the European Institutions.⁶ A letter from Sir Jon Cunliffe, the UK ambassador to the EU stated that the GCHQ chief would not appear (at the hearing) since 'the activities of intelligence services are... the sole responsibility of EU member states'.⁷

The questions opened by these NSA activities and the European services working with

¹ The UPSTREAM programme was revealed when it was discovered that the NSA was tapping cable-bound internet traffic in the very building of the SBC Communications in San Francisco, in 2006. See « AT&T Whistle-Blower's Evidence », *Wired*, 05/17/2006. Available at <http://bit.ly/17oUqIG>

² Through the NSA's programme Planning Tool for Resource Integration, Synchronisation, and Management (PRISM).

³ *The Guardian*, Friday 7 June 2013 and Saturday 8 June 2013.

⁴ Other high-profile NSA's electronic surveillance programmes include: Boundless Informant, BULLRUN, Fairview, Main Core, NSA Call Database, STELLARWIND.

⁵ This note supplements the previous research of Caspar Bowden by looking at the connection between the European programmes and the US surveillance programme. Caspar Bowden: *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights*, PE 474.405, Sept. 2013

⁶ Spiegel journalists who had access to Snowden documents have stated in a post published on September 20, 2013: "According to the slides in the GCHQ presentation, the attack was directed at several Belgacom employees and involved the planting of a highly developed attack technology referred to as a "Quantum Insert" ("QI"). It appears to be a method with which the person being targeted, without their knowledge, is redirected to websites that then plant malware on their computers that can then manipulate them." See www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

⁷ Letter from John Cunliffe to Juan Lopez Aguilar, available at: www.europarl.europa.eu/document/activities/cont/201310/20131003ATT72276/20131003ATT72276EN.pdf

them are therefore directly affecting the European Union institutions and they necessitate a specific inquiry by the European parliament, given quite clearly that these matters do indeed affect EU affairs and interact with EU competence.

Beyond the specific case of the attacks against the EU institutions, **these secret operations impact, first, the daily life of all the populations living inside the European Union** (their citizens and their permanent residents) when they use internet services (such as email, web browsing, cloud computing, social networks or Skype communications – via personal computers or mobile devices), by transforming them into potential suspects. Second, **these operations may also influence the fairness of the competition between European companies and US companies**, as they have been carried out in secret and imply economic intelligence; third, **some governments of the EU were kept unaware of these activities** while their citizens were subject to these operations. An inquiry is therefore central and needs to be prolonged by further in-depth studies, in particular in the context of the EU developments of Rule of Law.

In addition to the fact that these operations have been kept secret from the public, from companies and branches of governments affected by them (with the possible exception of the intelligence community of some European countries), the second **characteristic of these operations** that has to be highlighted is their **"large scale" dimension**, which changes their very nature, as they go largely beyond what was called before targeted surveillance or a non-centralised and heterogeneous assemblage of forms of surveillance⁸. These operations now seem to plug in intelligence capacities on these different forms of surveillance via different platforms and may lead to data mining and mass surveillance. The different appreciations of what is large scale surveillance are discussed in details below.

A large part of the world's electronic communications transiting through cables or satellites, including increasingly information stored or processed within cloud computing services (such as Google Drive, or Dropbox for consumers; Salesforce, Amazon, Microsoft or Oracle for businesses) i.e. petabytes of data and metadata, may become the object of interception via technologies put in place by a transnational network of intelligence agencies specialised in data collection and whose leader seems to be the NSA which pertains simultaneously to different networks. The NSA carries out surveillance through various programmes and strategic partnerships⁹. While the largest percentage of the internet traffic is believed to be collected directly at the root of the communications infrastructure, by tapping into the backbones of the telecommunications networks distributed around the world, the recent exposure of the PRISM programme has revealed that the remaining traffic is tapped through secret data collection and data extraction of nine US-based companies: Microsoft, Google, Yahoo, Facebook, Paltalk, Youtube, Skype, AOL, Apple.¹⁰ The surveillance programmes therefore imply not only governments and a network of intelligence services, but they work through the "forced" participation of internet providers as a hybrid system, as part of a Public-Private-Partnership (PPP) whose consent is limited.

On the basis of the provisions of the US FISA Act, the NSA, with an annual "certification" of the FISA court, can target any non-US citizen or non-US legal resident located outside the territory of the US for surveillance¹¹. **These data, once intercepted, are filtered and the suspicious ones are retained for further purposes** by the NSA and GCHQ.

⁸ K. Haggerty and R. Ericson, (2000), *The Surveillant Assemblage*, *British Journal of Sociology*, 51(4): p. 605-622. See also Bigo, D. (2006), *Intelligence Services, Police and Democratic Control: The European and Transatlantic Collaboration*, in Bigo D., Tsoukala A., *Controlling Security*, Paris. L'harmattan.

⁹ The NSA functions in particular as the center of the network codenamed "Five Eyes" (US, UK, Canada, Australia, New Zealand. See Glenn Greenwald, Laura Poitras and Ewen MacAskill "NSA shares raw intelligence including Americans' data with Israel", *The Guardian*, 11/11/2013. <http://bit.ly/1qEJI84> Accessed 14/10/2013

¹⁰ See Bill Binney, "Democracy and Surveillance Technology", *Congress on Privacy & Surveillance*, 30/09/2013, <http://slideshot.epfl.ch/events/cops> Accessed 14/10/2013

¹¹ See section 702 of the FISA Act See <http://bit.ly/1qEIXf5> Accessed 14/10/2013

The stored data can then be aggregated with other data, and be searched via specifically designed programmes such as X-KEYSCORE.

Furthermore, **internet access providers** in the US (but also in Europe) are under the **obligation** to keep their data for a certain period, in order to give law enforcement agencies the possibility to connect an IP address with a specific person under investigation. The legal obligations concerning access to data and privacy law derogations vary for the internet providers and the intelligence services, depending on the nationality of the persons under suspicion according to the nationality of the person concerned.

For the European citizen using cloud computing or any internet service which transits through the US cable communications systems (possibly all internet traffic) this has very important consequences, on various levels:

- At present, the scope of the US debate around PRISM has centred around the rights of US citizen to be protected from illegitimate purposes of data collection by the NSA and their other intelligence agencies, with a focus on the US Patriot act and FISA reforms, but it has been discussed only for their citizens in the context of their institutions and constitutional frameworks. The implications for EU citizens need to be addressed too.
- As explained in a previous note by Caspar Bowden, it is quite clear that European citizens whose data are processed by US intelligence services are not protected in the same way as US persons under the US Constitution in terms of guarantees concerning their privacy.¹² Consequently the data of European data subjects are 'transferred' or 'extracted' without their authorisation and knowledge, and a legal framework offering legal remedies does not currently exist.

Under European law, the individual has the ownership of his data. This principle is central and protected by the EU Charter and the Treaty. This aspect raises important legal issues that will be tackled in the section 3 of this study: can we consider unauthorised access to data as a "theft" (of correspondance)? Currently, channels permitting lawful search do exist, such as the EU-US Mutual Legal Assistance Agreement (MLAA) that cover criminal investigations, and counter terrorism activities. However, in light of recent revelations, have the US services and their European Member States partners followed the rules of this agreement? Moreover, and contrary to the US legislation, the EU Charter of fundamental rights requires data protection and applies to everyone, not just EU citizens. The ECHR also guarantees the right to privacy for everyone not just nationals of contracting parties. Thus the overall framework of the right to privacy and data protection in the EU cannot be limited to EU citizens alone. However, protections arising from national constitutions could be also limited.

To solve this profound inequality of treatment, it would require either a change of US laws offering the same privacy rights to any data subject intercepted by their systems, independently of their nationality, or to sign an international treaty like the EU-US agreements specifying a **digital bill of rights** concerning all data subjects, whatever their nationality.

The structure of the study

The study starts by shedding light on the Snowden's revelations and highlights to what extent we are witnessing a reconfiguration of surveillance that enables access to a much larger scale of data than telecommunication surveillance of the past. "Large scale" surveillance is at the heart of both a scientific controversy about what the different

¹² C. Bowden (2013), The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights, Study for the European Parliament, PE 474.405, September 2013. See the developments concerning the fact that under FISAA section 702, non-US citizens are excluded from the scope of the 4th Amendment.

technologies of interception of digital messages can do when they are organised into platforms and planning tools in terms of integration of data, and a political and ethical controversy about the use of these technologies by the intelligence services; the two controversies being interwoven by the different actors in order to compete over the legitimacy of such practices.

These preliminary remarks are critical for the second part of the study that deals with a comparative approach to European Programmes of surveillance. Since the publication of the first revelations on the US PRISM programme, disclosures and allegations relating to large-scale surveillance activities by EU member states have emerged as a result of both the Snowden leaks and wider investigative journalism. Section 2 draws on a country-by-country overview of large-scale telecommunications surveillance activities/capacities of five EU member states: UK, Sweden, France, Germany and the Netherlands (set out in Annex 1 of this study). The section draws a set of observations concerning the technical features, modalities and targets pursued by the intelligence services of these EU member states in harvesting large scale data, as well as examining the national and international actors involved in this process and the cooperation between them. It highlights the commonalities, divergences and cross-cutting features which emerge from the available evidence and highlights gaps in current knowledge which require further investigation.

These empirical examples are followed by an investigation of modalities of actions at the disposal of EU institutions concerning large scale surveillance (Section 3). This section tackles the EU competences concerning NSA surveillance programmes and general oversight over EU Member State programmes of surveillance. It assesses the relationship between surveillance programmes and EU competence, employing three legal modalities of action to critically examine EU surveillance programmes from an EU law viewpoint.

The study concludes with a set of recommendations targeted at the European Parliament and aiming to feed into the overall conclusions and next steps to be drawn from the LIBE committee's inquiry.

Methodological note

The exercise of piecing together the extent of large scale surveillance programmes currently conducted by selected EU member states is hampered by a lack of official information and restricted access to primary source material. The empirical evidence gathered for the purpose of this study and presented in Annex 1 therefore relies on three broad forms of evidence:

1. **The reports and testimonies of investigative journalists.** Much of the publicly available evidence covering EU member states' engagement in mass surveillance-like activities stems from revelations of investigative journalists, and their contacts with whistleblowers – current or former operatives of intelligence agencies. Press reports are in some cases very concrete in their sources (e.g. quoting from specific internal documents), while others are more ambiguous. Where possible we provide as much information concerning the journalistic sources where used in this study, however, a cautious approach must be taken to material that researchers have not viewed first hand.
2. **The consultation and input of experts** via semi-structured interviews and questionnaires. Experts consulted for this study include leading academic specialists whose research focuses on the surveillance activities of intelligence agencies in their respective member states and its compatibility with national and European legal regimes.
3. **Official documents and statements.** Where possible, the study makes reference to official reports or statements by intelligence officials and government representatives which corroborate/counter allegations concerning large-scale surveillance by intelligence services of EU member states.

1. Controversy between the actors about the scale of the problem

KEY FINDINGS

- The PRISM scandal in the US and disclosures by Edward Snowden only serve to recall the recurrence of transgressions and illegal practices carried out by intelligence services.
- Surveillance of population groups is not a new phenomenon in liberal regimes. It is the purpose and the scale of surveillance that are precisely at the core of what differentiates democratic regimes and police states.
- Intelligence services have adopted several strategies in order to avoid the accusations of privileging security over liberty.
- There is a growing consensus that the attitude of the NSA and GCHQ, but also other secret services in Europe, are no longer acceptable in a democratic society.
- Therefore, the analysis of Europe surveillance programmes cannot be reduced to the question of a balance between data protection versus national security, but has to be framed in terms of collective freedoms and democracy

A scientific controversy, which has central implications in terms of politics and ethics in democracy, revolves around the idea that large-scaling surveillance has to be contained. It implies a discussion about the role of the technological developments historically and a discussion about the use of these technologies when they are at the service of intelligence services. These questions tackle the legitimacy of such operations, their impact in terms of data protection, privacy and discrimination between individuals. They also affect the question of the structure of democracy and collective freedoms. Therefore **the key question is the one of the nature, the scale, and the depth of surveillance that can be tolerated in and between democracies.**

The objective of this note is not to take side and to arbitrate who is telling the truth in these controversies, as it is with the time constraint impossible to have a clear view of what is knowledge and what are allegations.¹³

This is why it is important to take into account the methodological note set out in the introduction outlining the limits of the knowledge accumulated and to acknowledge the speculative part of the argument. Nevertheless, these limits, once accepted, do not hamper the possibility for the note to propose as a main objective to find solutions that can be accepted despite the discrepancy between these strongly opposing appreciations.

The note suggests that the controversy over large scale harvesting of data has to be understood along a continuum of intelligence services activities: 1) counter terrorism activities that follow a criminal justice logic, 2) counter terrorism activities that try to monitor the future by profiling suspects, 3) cyber spying activities that target specific groups in a military strategic approach, and 4) electronic mass surveillance activities carried out without clear objectives.

The note thus proposes a « red line » approach that would be accepted by all the actors involved. The actors would agree not to cross this line in the future, to fully

¹³ D. Omand (2008), Can we have the Pleasure of the Grin without Seeing the Cat? Must the Effectiveness of Secret Agencies Inevitably Fade on Exposure to the Light? Intelligence and National Security, Volume 23, Issue 5, pages 593-607, 2008.

respect democratic rules, while pursuing their mission of protection against crime and terrorism.

1.1. Large scale electronic surveillance in democracies: compatibility or not?

The characteristics of large scale electronic surveillance differ in many ways from traditional intelligence activities. This section aims at highlighting how the possibilities opened up by the ever-increasing digitalisation of human activity redefine the scale of surveillance, its rationale and its underlying logics.

1.1.1. Surveillance, Intelligence services and democracy

Surveillance of groups of population is not a new phenomenon in liberal regimes. Specific groups of individuals have often been targeted by intelligence services, because they were suspected of conducting criminal activities (including political violence). If democratic regimes have not gone as far as authoritarian ones, whose intelligence bodies were spying quite systematically on their own populations in order to detect dissent in political opinions in the name of a doctrine based on the idea of enemies within (such as the STASI in the Former Democratic Republic of Germany, the *Securitate* in Romania, or the UDBA in former Yugoslavia), they still have a history of large-scale surveillance.

The purposes and the scale of surveillance are precisely at the core of what differentiates democratic regimes and police states. Even if there has been transgressions in the past, intelligence services in democratic regimes in principle do not collect data in mass, on large groups of population, and if surveillance is undertaken on specific individuals, it is on the ground that collection of data is deemed necessary to detect and prevent violent actions in the making, not to gather information on life styles or political opinions. At least this has worked as a kind of 'agreement', a shared understanding between the State and the citizens, which is well captured in this quote:

Our government in its very nature, and our open society in all its instinct, under the Constitution and the Bill of Rights automatically outlaws intelligence organizations of the kind that have developed in police states.¹⁴

Nevertheless, when ramparts against full surveillance are not checked regularly, they may stop operating. In the name of the development of high technologies and their use by 'enemies', intelligence services have crossed these boundaries in the pursuit of their missions. This goes along a frequent redefinition of who is the enemy (or the suspect), and how far s/he is already infiltrated into the territory, that has overstretched the notion of national security. **In a democracy, however, separation of power exists, and the excess of intelligence services have been regularly denounced** when their unlawful activities, often concealed under a veil of secrecy that characterises intelligence-led policing, have been uncovered.

The PRISM scandal in the US and the recent Snowden's revelation only reminds us the recurrence of wrongdoings and illegal practices in 'targeted surveillance' carried out by intelligence services as well as the resistance of the political authorities to recognise that the services went too far. **In the past and prior to PRISM and al.¹⁵, US authorities have been condemned in numerous occasions for the surveillance and infiltration of large groups of individuals by law enforcement authorities.** The civil rights movements and the communists were the targets of the 1950s, the anti-war

¹⁴ A. Dulles (1963), *The Craft of Intelligence*, New York: Harper&Row, p.257.

¹⁵ Even if we acknowledge that PRISM is only a small programme within the broader NSA programmes of surveillance, and that other meaningful programmes have been revealed – such as XKeyscore, we will keep the reference to PRISM and al. as generic to designate NSA programmes to ensure clarity.

movements in the 1960s and the 1970s. Secret programmes were in place with an extensive use of informants, intercepted mail and phone calls, engineered break-ins¹⁶. COINTELPRO in the late 1950s, CHAOS and MINARET in the 1960s and the 1970s were all recognised as unlawful surveillance programmes and specific rules have been elaborated to protect US persons from this political surveillance.

The Foreign Intelligence Surveillance Act (FISA) court was specifically designed in 1978 to counterbalance the intelligence powers and to give the judiciary the power to oversee claimed "foreign intelligence" activities, especially if they were affecting fundamental rights of US citizen. As detailed elsewhere, this court has constantly seen its powers undermined, even more so after 9/11 and the launch of the war on terror¹⁷. The court's scope is also limited to the protection of US citizen, and does not include non-US persons even though the latter are also the victims of unlawful surveillance. The current PRISM and other NSA activities and their relations to other intelligence services and private companies in the US further illustrates the limitations of powers of the judiciary over intelligence activities, as well as the difficulty to implement a parliamentary oversight over such activities, including the participation of private actors having a global reach in surveillance.

In Europe, a series of scandals emerged when practices of undercover policing and surveillance of political parties were endangering civil liberties, but they were more connected with infiltrations and undercover operations than mass surveillance. In Spain the creation of the GAL (Grupos Antiterroristas de Liberación) to fight ETA ended up, after many years of procedure, with the condemnation of the former Minister of Interior and its imprisonment in 1996. In France, the *Renseignements Généraux* were threatened to be shut down after a series of illegal activities involving illegal phone-taps and the presumed assassination of a gay activist in the 1990s, the Pasteur Doucé. More recently, in June 2013, Luxembourg's Prime Minister Juncker officially announced he would resign following a spying scandal, involving illegally bugging politicians.

The need for an oversight of intelligence activities by parliamentary or judicial authorities has progressively been widely accepted by the late 1990s, of course not without difficulties. French intelligence services only recently agreed to an external procedure of control. The *Renseignements Généraux* have partly survived under the DCRI, but their missions have been re-oriented. These services always insisted that they either focused on very specific cases connected with spying or political violence, or that they were *only* undertaking better « opinion polls » than the researchers and private companies providing similar « services ». As detailed hereafter, the specificity of large-scale surveillance considerably challenges these supposedly reassuring statements and raises the question of the connections between the services in charge of antiterrorism and the services in charge of collecting data for large-scale surveillance.

The War on Terror launched after the events of 9/11 somehow shook the fragile consensus according to which democracies do not carry out mass surveillance and have to accept some oversight. In the US, and to a lesser degree in Europe, a series of programmes have been initiated, in secret, using all existing resources of modern information technology. The possibilities of surveillance have increased at the same pace of the increase of data availability. Regular increase in bandwidth has enabled new uses of the Internet, such as mass storage and processing of personal, private and governmental data through cloud computing. The development of mobile computing devices (smartphones, tablets) has similarly provided a new wealth of geo-localised, personal information.

¹⁶ See G. T. Marx (1989), *Undercover: Police Surveillance In America*, University Of California Press.

¹⁷ On FISA loopholes and the court limitations, see the note produced for the LIBE Committee: Caspar Bowden, *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights*, PE 474.405, Sept. 2013

Each time a scandal occurs, as in the Swift and TFTP related scandals and their EU-US repercussions¹⁸, the demand for an oversight of intelligence activities by parliamentary and/or judicial authorities gains more legitimacy. Clearly the modalities of oversight remain challenging, and their implementation highly problematic, because surveillance programmes are often transnational and have a global reach, but also because of the ability of these services to surround their activities with a veil of secrecy (the 'classified information' argument). The alleged difficulty to draw the line between the interests of the State, those of a specific government or of a specific political group (when these are not purely private interests) only adds to the current problem¹⁹. In addition, when the programmes are using a world wide surveillance on citizens of other states, without the knowledge of these citizens, and even sometimes without the knowledge of their governments, the question is not anymore one of data protection and privacy of an individual versus this surveillance, it becomes a question of democracy itself where systematic surveillance of a "mass" of people may undermine the regime, while arguing it is for protection (see section 3).

1.1.2. Large scale surveillance and mass surveillance: what is at stake?

This note insists on the difference that exists between the scale and depth of the programmes that are connected to PRISM and al. and the programmes previously undertaken in counterterrorism and counterspying. What has to be questioned here is the possible transformation of large scale surveillance **into what can be called a 'cyber mass surveillance' that enables access without warrant to a much larger scale of data** than telecommunication surveillance of the past, such as ECHELON.

Ironically, it was the European Parliament's inquiries about NSA's ECHELON programme in 2000 and 2001 that already revealed that surveillance programmes capable of interception and content inspection of telephone calls, fax, e-mail and other data traffic globally through the interception of communication bearers including satellite transmission were in place.²⁰ As reported to the European Parliament by the then whistle-blower Duncan Campbell, ECHELON was one part of a global surveillance systems involving cooperation of satellites stations run by Britain, Canada, Australia and New Zealand,²¹ and concern aroused in particular by the assertion in Campbell's report that ECHELON had moved away from its original purpose of defence against the Eastern Bloc and was being used for purposes of industrial espionage.²²

Other US programmes that were denounced by watchdogs can be mentioned, such as CAPPS I & II (Computer Assisted Passenger Pre-Screening System) and US-Visit related

¹⁸ A. Amicelle (2011), The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and the "SWIFT Affair", Research Question 36, CERI, Sciences-Po.

¹⁹ See P. Gill (2012), 'Intelligence, Threat, Risk and the Challenge of Oversight', *Intelligence and National Security*, 27:2, pp. 206-22; see also A. Wills, M. Vermeulen, H. Born, M. Scheinin, M. Wiebusch, A. Thornton (2011), Parliamentary Oversight of Security and Intelligence Agencies in the EU, Note for the European Parliament, PE 453.207, 15 June 2011.

²⁰ On ECHELON, see European Parliament (2001), *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))*, PE 305.391 A5-0264/2001. See resolutions on the right to privacy and data protection, in particular that of 5 September 2001 on the existence of a global system for the interception of private and commercial communications (Echelon interception system OJ C 72 E, 21.3.2002, p. 221.

²¹ Duncan Campbell, 'Inside Echelon: the history, structure, and function of the global surveillance system known as Echelon', *Telepolis* (2000): www.heise.de/tp/artikel/6/6929/1.html; Duncan Campbell, The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition, Part 2/5, in: STOA (Ed.), *Development of Surveillance Technology and Risk of Abuse of Economic Information* (October 1999), PE 168.184.

²² See Final Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)), PE.305.391

PNR records, which gather personal information from unidentified government databases as well as commercial data sources to set up no fly and terrorist watch lists; NIMD (Novel Intelligence from Massive Data), an initiative of the secretive Intelligence Community Advanced Research and Development Activity (ARDA) which focuses on "massive data"; MATRIX (Multistate Anti-Terrorism Information Exchange), a state-level program supported by the U.S. Department of Justice. MATRIX aims to give state law enforcement agencies across the nation a powerful new tool for analysing the personal records of both criminals and ordinary Americans. According to an article published in the *Washington Post*, the programme "would let authorities (...) instantly find the name and address of every brown-haired owner of a red Ford pickup truck in a 20-mile radius of a suspicious event".²³

This reminder of such surveillance programmes and the intelligence activities they authorised sheds a particular light over the current Snowden's revelation. Two main aspects should be here underlined: **PRISM and ai. should not be considered as a rupture from the past (even though their magnitude is quite unique), nor as an isolated initiative** as many other parts of the world develop similar programmes, as described in Section 2.

A series of programmes have been initiated, using all existing resources of the Internet, both in the US and in Europe, after 2004 with the development of integrated platforms, the breaking of software encryption keys, the development of new software permitting routinely to filter, visualise and correlate unprecedented amounts of data and metadata. **These new resources for surveillance, the widespread use of smart phones and the development of cloud computing have blurred the line between 'targeted surveillance' – justified by the fight against crime – and data mining, which carries the risk of extending the scale, and the purpose, of surveillance.** These programmes have been justified by the will to protect the population from crimes, and were tailored to provide tools for the profiling of categories of people likely to commit such crimes. However, once data are available to search and extraction, other purposes may arise.

One such attempt, the "Total Information Awareness" (TIA) programme, has been precisely rejected by the US Congress on this ground in 2003 and (at least publicly) limited to Terrorism Information Awareness. Yet the idea of warrantless wiretapping has been accepted at that time, as well as blanket data searches. Revealed in 2005 by the *New York Times*, this programme has been strongly denounced. However, this programme did not disappear, and was de facto legalised in 2007 by the *Protect America Act*.

This raises a number of questions: how far do « PRISM » in the US and « Tempora » in the UK follow or not the same logic of TIA? Do they maintain a purpose limited to terrorism and crime or are the data used also for tax evasion, for advantaging some private companies in their contracts, for profiling political opinion of groups considered as marginals, for elaborating scenarios concerning political conflicts and international situations?

Concerns increasingly arise that these programmes are in addition interconnected and that some European Member States services participate to these data extractions of the Internet data for multipurposes "explorations". Snowden indeed claimed that data collected by the Tempora programme is shared with the NSA and that no distinction is made in the gathering of data between private citizens and targeted suspects²⁴. But

²³ "U.S. Backs Florida's New Counterterrorism Database: 'Matrix' Offers Law Agencies Faster Access to Americans' Personal Records" *The Center for Investigative Reporting*, 05/08/2013 <http://bit.ly/1gEOGBR> Accessed 04/10/2013

²⁴ Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball "GCHQ Taps Fibre-Optic Cables For Secret Access To World's Communications" *The Guardian*, 21/06/2013

GCHQ has strongly insisted that they were not using data for indiscriminate searches²⁵, and that this use was restricted for national security, detection and prevention of crime purposes. One may ask: **where is the "red line" that intelligence services in democratic regimes cannot cross when they use cyber surveillance and, if a "red line" is recognised, is it shared by the US and the EU?**

1.2. Political and ethical controversies regarding the use of these technologies by intelligence services: the question of legitimacy

1.2.1. The position of the security services

Intelligence services have adopted several strategies in order to avoid the accusations of privileging security over liberty and threatening the nature of democratic regimes:

- Some security services have insisted that they had followed specific protocols, with the full knowledge of their other European partners. They have argued that surveillance has been strictly limited to counter-terrorism operations, and that surveillance took place on a small scale. When they do accept that they run large scale surveillance programmes, they insist they use data only to confirm information they already have, and that this surveillance only targets small groups of individuals or IP addresses. Therefore, according to them, this can not be assimilated to data mining.
- Other services or other persons in the same services have considered that they were not carrying out counter-terrorism operations, but cyber-security, cyber-defense and that they have the right to do such activities beyond the scope of the MLAA, that they have their own right to define what were the boundaries of their national security, and that they were not constrained by any international agreement²⁶. They have also considered that these activities are not a lack of compliance with the article 4.3 of the Treaty of the EU concerning the loyalty of the MS to the principles of the EU Charter, and that they were fully covered by the article reserving the intelligence activities to the member states only. In their views, impunity does prevail.

Security services and several academics working on intelligence often refer to the fact that open societies also have enemies, including internal enemies, and that the secret services have been set up to act beyond the legal framework, not to be prisoner of it. They consider that only their own government, and often only the president or the prime minister, has the right to know what they do. They also deny the fact that the International or European Courts may have a say on this matter. It is a strong professional habit and a discourse largely shared by different US and European services, especially the ones which are not often in touch with the judiciary. This attitude and the series of beliefs it imply is certainly at the heart of the general problem of the different appreciation in terms of legitimacy of what has been revealed by Snowden on PRISM.

²⁵ Tempora is considered as a "buffer" which keeps the Internet data passing through the cable for a couple of days, in order to give more time to the teams who search suspects to have a "line" of conversation. They extract data from the cable to find IP locations and emails associated, but they do not retain the data in mass or use them for general profiling.

²⁶ General Keith Alexander, director of the NSA and Chief of the Central Security Service (CHCSS) as well as Commander of the United States Cyber Command, has made the link between the new project of cyber defense that he defended on 12 March 2013 at the Congress and the Snowden "leak" which undermines in his view the capacity of answer of the US versus foreign nations attacks on cyber.

1.2.2. The position of the other actors

Clearly, **not all branches of government accept** the attitude of the secret services. The considerations of a government tied by the Rule of Law differ from one country to another one. Some have a more "permissive" legal environment than others. Most, but in practice not all, governments of the EU considered that they have to respect the decisions of the European Courts (ECJ and ECHR) concerning the right to life, torture, or data protection and privacy even when they limit their so-called "freedom of action". The US do not seem ready to accept any constraint of that sort if the principles do not exist in their own constitution.

In the case of the PRISM affair, and previously in the case of TFTP, Commissioner Reding has written a letter to the US Attorney General, Eric Holder, raising European concerns and asking for clarification and explanations regarding PRISM and other such programmes involving data collection and searching, and the laws under which such programmes may be authorised. A detailed answer from the US authorities is still pending months after the events, despite the discussions which took place at the EU-US Justice Ministerial meeting in Dublin on 14 June 2013.

Some lawyers, civil servants, NGOs and journalists have considered that these permanent delays in terms of answers, and the silence of the intelligence services in the matter, further legitimate the need to undertake urgent action against the double standards that the US government imposes on its partners. They consider that the US government maintains the fiction of a global collaboration against crime and terrorism while applying a strategy of full spectrum dominance, which is more and more aggressive and they consider their technological advance as a strategic advantage against their allies. In this case, the image of a community of nations is clearly undermined in favour of a revival of national struggles for dominance and a clash of sovereignties. This reformulation affects the US-EU relations, but also the internal relations between member states in the EU. As we will see in section 3, respect of other's sovereignty is one of the key questions emerging from the PRISM affair and other programmes carried out by European services, inside Europe and in the context of transatlantic collaboration.

In this context, a lack of actions of the European Parliament would profoundly undermines **the trust and confidence** that EU citizens have in the European institutions, and especially in the European Parliament to safeguard and protect the most fundamental freedoms related to their private and family lives.

Actors of civil societies, especially journalists of the most well respected newspapers in the world, and human right NGOs consider that the attitude of the NSA and GCHQ, but also other secret services in Europe, are not any more acceptable. In the case of the GCHQ in the UK, **civil society actors consider that their actions could be labelled as acts of cyber warfare aggression, as form of treason of European member states' services** spying on other EU citizens on the behalf of their US counterparts, and that if it is not a treason per se, it is a breach of trust and confidence in terms of solidarity with the EU, by placing other allegiances with third parties against the EU ones.

Other European secret services have also to be watched. They may not be connected directly with the transnational network of the NSA, but they may try to build their own apparatus. France and Germany have developed at a smaller scale some equivalent capabilities and reportedly access transnational electronic communications without a regular warrant but on the basis of special courts, as well as they share data with other countries. These aspects are further developed in Section 2.

The reaction of a part of the civil society has been stronger than the political reactions that always tend to minimise the possible transatlantic rift. Most of the newspapers (especially in the comments left by readers) and internet blogs have spoken favourably in favour of Snowden and other whistleblowers, and they have developed an anxiety concerning the rise of surveillance which is often mixing facts and fears concerning a totalitarian future, with references to Georges Orwell, Philip K Dick, or an easy reading of Michel Foucault. These reactions are for the moment concentrated on the infosphere of

Internet bloggers, but after the arrestation of David Miranda, the partner of the journalist Glenn Greenwald of the Guardian by GCHQ, a large part of the world's journalists of investigations have started to share the image of a "state of exception" in the making, or of a "surveillance state".²⁷ Journalists and human rights NGOs have joined the more marginal scenes of the infosphere in favour of freedom of the Internet. Many activists consider that the easyness of technologies of surveillance cannot be a justification for their use and some of them regularly use the formula that we are "sleepwalking into a surveillance state". Joined by an increasing number of persons, they refuse to accept such a disproportion between the massive collection of data and metadata, the length of their retention in regards to the so-called objective of preventing terrorism, which has become a blanket excuse for mass data collection used for many other purposes.

For the above mentioned reasons, an analysis of Europe surveillance programmes cannot be reduced only to the question of a **balance between data protection versus national security and to a technical question to be resolved by experts, but has to be framed also in terms of collective freedoms and nature of the democratic regime.**

If derogations to data protection may exist, national security cannot be a justification for a structural transformation of rule of law and democratic expressions of civil societies in an open world of information.

If future inquiries show that most of the actions undertaken by the NSA, GCHQ and other European services – in collaboration or in competition between them but using the same practices – have not only focused on counter terror activities, but on economic espionage, illegal bugging of political leaders and EU institutions, and possibly on data mining for purposes of total information awareness, as well as on manipulation of opinion and strategies to influence life styles and consumption habits, then the responsibility of these services and their governments has to be dealt with from a judicial perspective. Even if future research may show that the different EU member states' intelligence services have restricted their activities to counter-terrorism and not mass surveillance, this does not prevent the need for principles of necessity and proportionality.

In this context, we will try to answer the different key questions in the following sections:

- In the different surveillance programmes in place in Europe, which ones are based on similar logics as the NSA's? Which ones involve forms of cooperation with the NSA?
- How does this affect the idea of a European Union in solidarity in terms of Foreign Affairs but also in terms of shared Fundamental Rights equally available for all its citizens?
- If the question of the use of technologies of surveillance is a political one, then who should address it: the EU Member States, or all the institutions within the EU that are involved in the protection of the open nature of the societies composing the population of Europe?

²⁷ Edwy Plenel, "Contre l'Etat d'exception" *Mediapart*, 10/08/2013 <http://bit.ly/1qETpDB> Accessed 14/10/2013.

2. The EU member states practices in the context of the revelations of NSA large scale operations

KEY FINDINGS

- The overview of publicly available knowledge on large-scale surveillance activities by five EU member states – the UK, Sweden, France, Germany and the Netherlands – reveal evidence of engagement in the large-scale interception and processing of communications data by four of those member states. Further investigation and research is required in order to gain a better understanding of the techniques, capacities and lawfulness of these programmes.
- Practices of so-called 'upstreaming' (tapping directly into the communications infrastructure as a means to intercept data) characterise the surveillance programmes of all the selected EU member states, with the exception of the Netherlands for whom there is no concrete evidence of engagement in large-scale surveillance.
- The capacities of Sweden, France and Germany (in terms of budget and human resources) are low compared to the magnitude of the operations launched by GCHQ and the NSA and cannot be considered on the same scale.
- There is a multiplicity of intelligence/security actors involved in processing and exploiting data, including several, overlapping transnational intelligence networks dominated by the US.
- Legal regulation of communications surveillance differs across the member states examined, however in general legal frameworks are characterised by ambiguity or loopholes as regards large-scale communications surveillance, while national oversight bodies lack the capacities to effectively monitor the lawfulness of intelligence services' large scale interception of data.

The following section draws on the evidence presented in Annex 1 on potential practices of large-scale surveillance being conducted by the intelligence services of EU member states. Annex 1 selects for in-depth assessment five countries where existing evidence (drawn from investigative journalism, academic analysis or official documentation) indicates large-scale electronic surveillance practices which may be classified as mass surveillance: the UK, Sweden, France, Germany and (potentially in the future) the Netherlands.

Disclosures since June 2013 surrounding the activities of the **UK's GCHQ** indicate a range of programmes and projects linked to the mass interception, storage and processing of telecommunications data, at the core of which is the so-called 'Tempora' programme (see Section 1, Annex 1). These revelations were followed in September 2013 by reports focusing on the activities of **Sweden's National Defense Radio Establishment (FRA)**. Operations and programmes for the mass collection of data by the FRA are reportedly elevating this agency to an increasingly important partner of the global intelligence network (Section 2, Annex 1). Evidence has simultaneously emerged concerning similar projects for the large-scale interception of telecommunications data by both **France's General Directorate for External Security (DGSE)** (Section 3, Annex 1) and **Germany's Federal Intelligence Service (BDE)** (Section 4, Annex 1.) There are strong suggestions to indicate that several if not all of these member states are engaging in exchanging this intercepted data with foreign intelligence services, namely the NSA. In addition, other EU member states are currently in the process of expanding

their signals intelligence capabilities, with the **Netherlands'** establishment of a new **Joint Sigint Cyber Unit (JSCU)** (Section 5, Annex 1.) providing a prime example.

Each of these five member states is examined considering the following criteria: the basic technical features of large-scale surveillance programmes; stated purpose of programmes, targets and types of data collected; actors involved in collection and use, including evidence of cooperation with the private sector; cooperation or exchange of data with foreign intelligence services, including the NSA; legal framework and oversight governing the execution of the programme(s). On the basis of these criteria, do surveillance programmes run by EU member states share commonalities with those executed by the NSA? How do they compare in terms of scale, technical features and the degree of accountability and oversight characterising their implementation? The member state by member state overview in Annex 1 reveals the following shared features/points of diversion and cross-cutting issues:

2.1. Technical features

According to the reports and evidence presented in Annex 1 concerning the means of gathering mass telecommunications data, the practice of so-called 'upstreaming' – tapping directly into the communications infrastructure as a means to intercept data – appears to be a relatively widespread feature of surveillance by several EU member states, namely the UK, Sweden, France and Germany. Disclosures by the Guardian in July on GCHQ's so-called 'Tempora' programme allege that the UK intelligence service have placed interceptors on approximately 200 undersea fibreoptic cables which arrive at the South-West coast of Britain.²⁸ These revelations have been followed in September by a renewed focus on the activities of Sweden's FRA, which has seen intermittent reports over the last five years concerning the interception and storage of communications data from fibre-optic cables crossing Swedish borders from the Baltic sea.²⁹ The last three months have also seen reports citing France and Germany as relying on upstreaming methods as a means to gather bulk data.³⁰ This method of interception is believed to be a relatively recent addition to the surveillance arsenal of these member states' intelligence services, with most programmes dating from around the late 2000s (see Annex 1). They therefore are understood to complement the more established satellite interception programmes pursued by US and EU intelligence services (UK, Sweden, France) of which the most extensive is 'FORNSAT', the successor of the ECHELON programme, as the main networked foreign satellite collection system coordinated by Five Eyes (see section 2.5 below).³¹

At the same time, there is little evidence (with the exception of reports concerning Germany)³² that the intelligence services of EU member states are currently engaged in collecting data directly from the servers of private companies, as employed in the NSA's PRISM Programme. For the moment at least, this practice appears to be restricted to the US. However, given the secrecy surrounding intelligence services activities, and the allegations concerning cooperation between Germany's BND and private internet service providers, it would require further in-depth investigation to draw any firm conclusions.

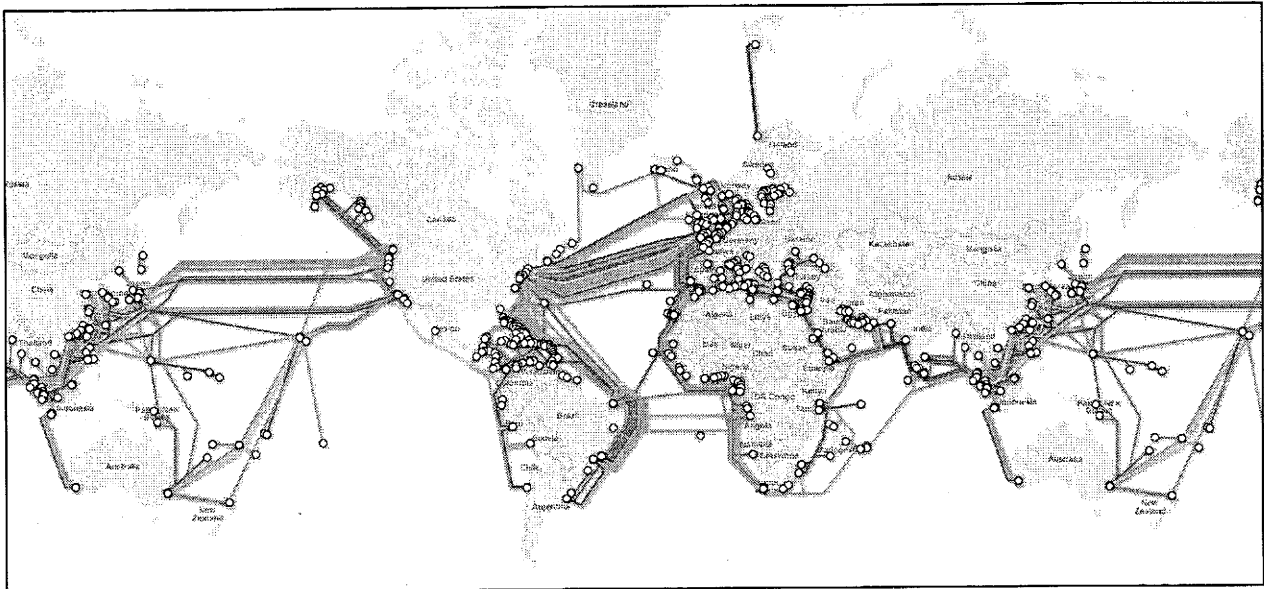
²⁸ E. MacAskill et al. (2013), 'GCHQ taps fibre-optic cables for secret access to world's communications', *The Guardian*, 21 June 2013.

²⁹ N. Nielsen (2013), 'EU asks for answers on UK snooping programme', *EU Observer*, 26 June 2013.

³⁰ J. Follorou and F. Johannes (2013), 'R v lations sur le Big Brother fran ais', *Le Monde*, 4 July 2013; Spiegel Online (2013) '100-Millionen-Programm: BND will Internet- berwachung massiv ausweiten', 16 June 2013.

³¹ Statement by Duncan Campbell at the European Parliament's LIBE Committee Inquiry on Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013.

³² P. Beuth (2013) 'Wie der BND das Netz  berwacht', *Zeit Online*, 18 June 2013.

Figure 1. Map showing concentration of global submarine cables

Source : <http://www.submarinecablemap.com/>

2.2. Scale

Given the scarcity of information concerning the programmes detected, and particularly the programmes by EU member states, it is difficult to draw firm conclusions concerning the relative scale of these practices. Nevertheless, a clear distinction can be made between the US/UK mass interception and data analysis programmes (such as PRISM, Upstream and Tempora) and the surveillance practices by other EU intelligence services. In terms of budgetary allocation, human resources and quantity of data collected and analysed, it appears unlikely that the programmes of EU member states such as Sweden, France and Germany come close to the sheer magnitude of the operations launched by GCHQ and the NSA.

First the capacities of the aforementioned EU member state intelligence services are relatively limited, with annual budgets of around half a billion euro³³ (see Annex 1) as opposed to the 10 billion dollar annual budget of the NSA.³⁴ The PRISM programme is relatively low cost (an estimated 20 million dollars), because much of the financial burden of data collection and processing is on the companies themselves (Apple, Google, Facebook etc.). Nevertheless, there is evidence that the NSA makes a substantial budgetary outlay on electronic large-scale surveillance, for instance spending 250 million dollars a year on programmes to circumvent encryption technologies.³⁵ GCHQ meanwhile is reported to have invested approximately one billion pounds (1.2 billion euro) in its 'Mastering the Internet' project, which allegedly provides the overarching framework for Tempora as well as several other telecommunications surveillance programmes (see Annex 1).³⁶

³³ Both Germany's BND and Sweden's FRA were allocated annual budgets of approximately 500 million euro in 2012. GCHQ's annual budget is reported to be approximately 1 billion euro. See Annex 1.

³⁴ B. Gellman and G. Miller (2013), 'U.S. spy network's successes, failures and objectives detailed in 'black budget' summary', *Washington Post*, 29 August 2013: <http://www.washingtonpost.com/wp-srv/special/national/black-budget/>

³⁵ J. Ball, J. Borger and G. Greenwald (2013), 'Revealed: how US and UK spy agencies defeat internet privacy and security', *The Guardian*, 6 September 2013.

<http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>

³⁶ D. Leppard and C. Williams (2009), 'Jacqui Smith's secret plan to carry on snooping', *The Sunday Times*, 3 May 2009.

We can also infer from the relatively low staffing capacities of the key EU intelligence services under scrutiny (generally in the low thousands as opposed to the NSA's 30,000-40,000 employees³⁷ – see Annex 1) that the surveillance practices undertaken by these member states are relatively modest. The processing and analysis of mass data requires a significant human resources investment, as indicated by reports that the NSA has allocated 850,000 of its operatives and external contractors to process the data captured by surveillance activities (including data intercepted and shared by GCHQ).³⁸ However, this observation raises several further questions, if we consider reports of growing technical capacities of intelligence services of EU member states such as Sweden and France for gathering bulk data (e.g. from upstream interception techniques): without the organisational capacity to process mass data, how is this data handled, is it for purposes of internal processing or exchange with foreign intelligence services?

2.3. Data types and data targets

Commonalities can be traced in the types of data targeted by programmes pursued by both the NSA and EU member states' intelligence services. As in the case of the NSA, the UK and Sweden collect both metadata and content, with the storage and handling of data differentiated depending on whether it consists of metadata or content.³⁹ In France, reports only allude to the collection of metadata while in Germany information pertaining to the type of data collected is unavailable.

In certain EU member states (UK, Sweden, Germany) programmes nominally target so-called 'external communications'.⁴⁰ Hence, the official targets of surveillance programmes are those communications which take place outside the territory of the member state in question (but which are routed through the national communications infrastructure) or that take place between a resident of that member state and a foreign contact. This is a consequence of national legal regimes which limit or place more stringent safeguards on the monitoring of internal communications. As a consequence, parallels can be drawn with the discriminatory approach taken by the NSA under FISA in only targeting those communications by non-US nationals as they pass through communications infrastructure on US territory. However, although the UK, Swedish and German large scale surveillance programmes in principal intend to intercept only external communications, in practice interception is likely to be less discriminate given that internal communications are often routed outside a member states' territory. As a consequence, all users of telecommunications (email, phone, social media etc.) may potentially fall victim to having their communications data intercepted. What is currently not clear is whether the internal communications that are unintentionally intercepted are systematically disregarded or whether they are (illegally) retained and processed by intelligence services.

The lack of information on how data is analysed and processed once collected makes it difficult to shed light on the ultimate targets of this surveillance exercise. A common feature of the surveillance programmes identified in the EU and that of the NSA's programmes is the lack of clearly delineated set of objectives, or grounds justifying the resort to electronic surveillance. There is no evidence across the member states selected for examination that surveillance programmes are restricted to counter-terrorist

³⁷ M. Rosenbach (2013), 'Prism Exposed: Data Surveillance with Global Implications' *Der Spiegel*, 10 June 2013 : <http://www.spiegel.de/international/world/prism-leak-inside-the-controversial-us-data-surveillance-program-a-904761-2.html>; NSA (2012) '60 Years of Defending our Nation': http://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf.

³⁸ E. MacAskill et al. (2013), 'GCHQ taps fibre-optic cables for secret access to world's communications', *The Guardian*, 21 June 2013.

³⁹ See Annex 1 (Sections 1 and 2).

⁴⁰ See Annex 1 (Sections 1, 2 and 4).

operations or countering external (military) threats. Rather, it appears from the available evidence that the ultimate data subjects targeted by these programmes are broad. For instance, the UK's GCHQ identify that the targets of its programmes "boil down to diplomatic/military/commercial targets/terrorists/organised criminals and e-crime/cyber actors."⁴¹

2.4. Processing and analysis of data

The scale of the big data collected from upstream interception requires establishing systematic methods, techniques and infrastructure to filter such large flows of information. Electronic large-scale surveillance implies data extraction, data comparison, data retention and the use of a great variety of databases. Concrete and detailed information shedding light on how data collected via the programmes discussed in Annex 1 are processed, filtered and analysed is currently unavailable, although hints as to the methods used to filter metadata and content are cited in reports and expert statements (see Annex 1).

These include the use of so-called 'Massive Volume Reduction' employed by the UK's GCHQ to reduce bulk data by removing 30% of less intelligence relevant data such as peer-to-peer downloads ('high volume, low value traffic').⁴² Reports with regard to UK and German programmes also cite the use of 'selectors' (e.g. keywords, email addresses, phone numbers of targeted individuals) to search data.⁴³ These 'selectors', allegedly allow intelligence services to access the content of an individual's communications, gather information about anyone that individual communicates with, and track locations online and offline, in turn permitting intelligence services to create sophisticated graphs of targets' social networks, associates, locations and movements.⁴⁴

However, the lack of further detail leaves an important gap in our understanding of the practices intelligence services are engaging to exploit the bulk data collected. These details would be critical to determine operational legitimacy and interaction with national legal frameworks regulating surveillance (see 2.6 below). For instance, must operatives first register an authorised initial target before launching a search or do they have a wide margin of manoeuvre when searching data? Do intelligence services engage in statistical analysis of the data gathered, and if so, based on which criteria? Are private companies engaged to collaborate in the engineering and design of algorithms and specific software that enable to compile and classify specific trends, patterns and profiles? More information as regards these questions would be essential to establish to what degree the exploitation of bulk data manifests characteristics of data profiling and data mining, which has so far been vigorously denied by intelligence service officials.⁴⁵

⁴¹ E. MacAskill et al. (2013), 'Mastering the internet: how GCHQ set out to spy on the world wide web,' *The Guardian*, 21 June 2013. <http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet>

⁴² E. MacAskill et al. (2013), 'GCHQ taps fibre-optic cables for secret access to world's communications,' *The Guardian*, 21 June 2013. <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>.

⁴³ E. MacAskill et al. (2013), 'GCHQ taps fibre-optic cables for secret access to world's communications,' *The Guardian*, 21 June 2013. <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>; Spiegel Online (2013) '100-Millionen-Programm: BND will Internet-Überwachung massiv ausweiten', 16 June 2013, available at www.spiegel.de/politik/deutschland/internet-ueberwachung-bnd-will-100-millionen-investieren-a-905938.html

⁴⁴ J. Risen and L. Poitras (2013), 'N.S.A. Gathers Data on Social Connections of U.S. Citizens,' *New York Times*, 28 September 2013: <http://mobile.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html>.

⁴⁵ For instance, US Director of National Intelligence, Washington DC, June 8, 2013: Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act.

What is clear however is that data appears to serve 'multi-purpose' ends. This can be inferred from the multiplicity of actors engaged in using data from European surveillance programmes once processed and filtered (see below).

2.5. Cooperation between national and international security actors

A cross-cutting feature of the surveillance programmes examined is the multiplicity of intelligence/security actors involved in processing and exploiting data. For instance, in Germany and France, the evidence indicates that large scale surveillance programmes constitute intelligence platforms that feed multi-level exchange of data between national law enforcement and security bodies.⁴⁶ Intelligence reports drawn from Sweden's surveillance programme also feed at least eight different 'customer' organisations ranging from defence agencies to law enforcement and customs bodies.⁴⁷ The wide spread of organisations with access to metadata or as recipients of intelligence drawn from this data again reflects the indication that data is being used for a wide range of security purposes far beyond the narrow focus of counter-terrorism and defence which has traditionally formed the primary focus of national intelligence activities.

Cooperation with foreign intelligence services also appears to be a common feature of the member states programmes outlined in Annex 1. In certain cases there are reports/allegations of large scale data exchange with the NSA (UK, Sweden and Germany): Cooperation with the US also appears to extend to collaboration/sharing of research to advance the technological means of mass surveillance. This may provide a partial explanation for why several of these mass surveillance programmes appear to date from around the same time period (mid-late 2000s).

Disentangling cooperative relationships between different EU and US intelligence services indicates a complex web of multiple, overlapping networks. First among these networks is the above-mentioned Five Eyes (composed of the US, UK, Canada, Australia and New Zealand) that originated from a 1946 multilateral agreement for cooperation in signals intelligence,⁴⁸ and which has extended over time in terms of activities (Echelon, and now Fornsats) and in terms of privileged partners. Sweden is one of these new partners which, according to Duncan Campbell, now permits Five Eyes to gain access to fibre optic cables from the Baltic states and Russia.⁴⁹ In addition, the US also engages in cooperative relationships with 'second' and 'third tier' partners such as France and Germany.⁵⁰ With these partners they engage in more ad hoc collaborations, but also offensive espionage, as reflected in the recent disclosures from the NSA whistleblower Edward Snowden published in *Le Monde* which suggests that the NSA had been intercepting French phone traffic "a massive scale".⁵¹ The latter revelation provides an illustrative example of dual networks between intelligence services, one collaborative, one aggressive, and raises the question over whether the EU member state government concerned (in this case France) has full oversight and awareness of what the various transnational intelligence networks in which its services participate are doing. Overall, the picture emerges of a US which

⁴⁶ See Annex 1 (Sections 3 and 4).

⁴⁷ See Annex 1 (Sections 2).

⁴⁸ This agreement, known as the UKUSA Agreement, was declassified in 2010 and is now publicly available on the NSA's website: www.nsa.gov/public_info/declass/ukusa.shtml

⁴⁹ Statement by Duncan Campbell at the European Parliament's LIBE Committee Inquiry on Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013.

⁵⁰ Ibid.

⁵¹ *Le Monde* reported that more than 70 million French phone calls had been recorded in one 30-day period in late 2012. See J. Follorou and G. Greenwald (2013), 'France in the NSA's crosshair : phone networks under surveillance,' *Le Monde*, 21 October 2013.

effectively dominates the diplomacy of surveillance, in ways that disrupt the cohesion of the EU in the security field.

2.6. Legal regimes and oversight

The legal regulation of communications surveillance differs across the five EU member states examined, and there is significant variation as regards the strength of oversight intelligence agencies are subject to when intercepting telecommunications data.

Some legal regimes operate on the basis of orders issued by special courts (Sweden), others on the basis of warrants issued by the government (UK, Netherlands) or by an authorising role accorded to specially appointed oversight bodies (Germany, France, Netherlands). However, as in the US where the loopholes of the existing regulations were denounced prior to the PRISM scandal, there is often a lack of legal clarity in member states' legislative frameworks where collection of mass internet data is concerned. Thus for instance, the UK Parliament's Intelligence and Security Committee concluded following an investigation into GCHQ activities under the PRISM programme that while "GCHQ has not circumvented or attempted to circumvent UK law, it is proper to consider further whether the current statutory framework governing access to private communications remains adequate". In particular the Committee underlines that "in some areas the legislation is expressed in general terms".⁵²

The implementation of programmes for interception via 'up-streaming' by EU member states indicate that law-making has not kept pace with the technological developments seen in surveillance practices in recent years, often designed for traditional intelligence techniques such as wiretapping, rather than the mass 'dragnet' approach that appears to be increasingly adopted by US and EU intelligence agencies. Thus in France, a senior representative of the intelligence services is reported to claim that the collection of meta-data by the DGSE is not illegal but a-legal, conducted outside the law.⁵³ Further, the lower levels of legal protection accorded to the collection of metadata in certain member states (e.g. UK, Sweden) does not take into account that this information can nevertheless be extremely revealing about individuals' lives. The exception here is the Netherlands where the current legislative framework does not permit the Dutch intelligence services to wiretap "cable bound communications" under any circumstances.⁵⁴ However, a modification to the law is expected in order to allow the establishment and activities of the JSCU.⁵⁵

As discussed above, the legislative frameworks of the UK, Sweden and Germany restrict warrantless collection of data where it concerns internal communications between residents of those member states, echoing the US restrictions on intercepting data between US citizens under FISA. However, evidence revealing data exchange between Western intelligence services raises a number of questions as to whether intelligence agencies share data in order to plug the gaps or circumvent the legal frameworks/safeguards intended to protect the rights of individuals in their national jurisdictions. This would point to a potential scenario of privacy shopping by services to exploit regimes with the weakest protection/oversight or with the greatest legal loopholes. Such a scenario is to some extent reflected in reports indicating that GCHQ

⁵² Intelligence and Security Committee of Parliament, Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme, 17 July 2013, available at: http://isc.independent.gov.uk/files/20130717_ISC_statement_GCHQ.pdf

⁵³ Statement by Jacques Follorou at the European Parliament's LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013.

⁵⁴ See Annex 1, Section 5.

⁵⁵ See Annex 1, Section 5.

marketed itself to the NSA on the basis of the UK's weak regulatory and oversight regime.⁵⁶

As regards oversight, in several member states oversight bodies are faced with constraints which hamper their ability to apply sufficient scrutiny to intelligence agencies' surveillance practices. In Sweden, the two main oversight institutions, the intelligence court (UNDOM) and the Inspection for Defence Intelligence Operations (SIUN) are deemed to be insufficiently independent.⁵⁷ In France the main oversight body, the CNCIS, is deemed to be substantially constrained in its reach due to its limited administrative capacity.⁵⁸ There are gaps also in the UK's intelligence oversight regime, as evidenced by the statement released in July by the ISC on GCHQ's Alleged Interception of Communications under the PRISM Programme. The committee, chaired by former foreign secretary Sir Malcolm Rifkind, took detailed evidence from GCHQ for its investigation, including a list of counter-terrorist operations for which the UK was able to obtain intelligence from the US, and found that GCHQ had acted within the law. The statement⁵⁹ however remains quite vague on what information it gained access to. Moreover, it indicates that the members of the committee had no prior knowledge of GCHQ's activities in the PRISM programme.

Finally, in terms of oversight it is worth considering the oversight mechanisms potentially built in to systems and databases used to process and search data collected. The only indication in this regard concerns the GCHQ's Tempora Programme which requires that in order to target an individual's data via a "selector" -- the operative will have to type into a box on his or her computer screen a Miranda number, to show that the process is taking place in response to a specific request for information, and will also need to select a justification under the Human Rights Act from a drop-down menu.⁶⁰ However, without further information (e.g. how detailed these justifications are), it is difficult to judge to what degree these mechanisms represent an administrative 'tick-box exercise' or whether they operate as a genuine safeguard. In any case they cannot substitute a strong institutional oversight framework which currently appears lacking in the member states examined here.

⁵⁶ N. Hopkins and S. Ackermann (2013), 'Flexible laws and weak oversight give GCHQ room for manoeuvre,' *The Guardian*, 2 August 2013.

⁵⁷ See Annex 1, Section 2.

⁵⁸ See Annex 1, Section 3.

⁵⁹ Intelligence and Security Committee of Parliament, Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme, op. cit.

⁶⁰ J. Lancaster (2013), 'The Snowden files: why the British public should be worried about GCHQ,' *The Guardian*, 3 October 2013.

3. Legal Modalities of Action at EU level and Compatibility with EU Law

KEY FINDINGS

- Surveillance programmes in EU member states are incompatible with minimum democratic rule of law standards which nurture from the EU Charter of Fundamental Rights and the European Convention of Human Rights, and are in turn constitutive components of their national constitutional traditions.
- European fundamental rights commitments, enshrined and developed in the case-law of the ECtHR and the CJEU, constitute key standards of the concept of national security in EU law and are to be used at times of reviewing evolving secretive surveillance practices.
- The member states' surveillance programmes equally jeopardise the EU principle of sincere cooperation, enshrined in Article 4.3 of the Treaty on European Union, as they compromise; first, the compliance with existing EU level mutual assistance and cooperation legal regimes and lawful searches between EU Member States and with the USA; second, the coherency in EU's external relations with the USA and other third countries; and third, the internal security of the Union as a whole. They also jeopardise the privacy of EU nationals as data owners and data citizens.
- Large-scale electronic surveillance blurs the lines between national sovereignty and matters relating to EU competence as it potentially spills over into the security activities of the EU institutions and its agencies. More precisely, EU liability may be invoked where EU agencies become implicated in sharing and exploiting data generated by national surveillance operations.
- The boundaries between domestic and foreign interception is blurred by data exchange between intelligence services. At the same time, those member states' domestic legal regimes which distinguish between the legal guarantees applied to national citizens over other EU citizens may raise questions of discrimination.

Under European law, the individual has the ownership of his data, (unlike the US where it is the company or service that has assembled the data). This principle is central and protected by the EU Charter and the Treaty. Therefore, it can be contended that transnational programmes linking the NSA with a series of European intelligence services and facilitating data exchange, could potentially be considered as a 'theft' (of correspondance) on top of the potentially illegal access, collection and processing and data if this has been done without the authorisation and/or knowledge of the national authorities, which are in charge of the management of these electronic data, and which are the only ones that may authorise derogations in terms of national security under the respect of the bilateral, European and international agreements previously signed.

A legal framework of the EU-US **Mutual Legal Assistance Agreement (MLAA)**, has been ratified by the Union and the US Congress, to permit collaboration that cover criminal investigations, and counter terrorism activities in search of evidence for law enforcement purposes. It stipulates the modalities for gathering and exchanging information, and for requesting and providing assistance in obtaining evidence located in one country to assist in criminal investigations or proceedings in another.⁶¹ **The**

⁶¹ Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 181/34, 19.07.2003.

channels permitting lawful search are therefore organised (and, it should be noted, critiqued by NGOs and journalists as accepting too readily the logic of the global counter terrorism initiated by the USA and its limitations to privacy). But it is not clear from the revelations of the activities conducted by the NSA, that the **US services and their European Member State partners have even followed the rules of this agreement, rather evidence indicates they have bypassed or ignored these channels in favour of covert cooperation** allowing to go beyond counter-terrorism collaboration and serving a multitude of other purposes. John Lanchester, who has been one of the rare persons to read the GCHQ files whose UK copy the Guardian was forced to destroy, expresses clearly what is at stake. Certainly democratic states need intelligence services, open societies have enemies, and tools of electronic surveillance are useful against them. It is for this reason that the right to privacy needs to be qualified in the interest of security, but the question arises when the technologies give the possibility of **mass capture of data** and that they are used for **strategic surveillance**, as in that case **security without limits may put democracy at risk**.⁶²

The relationship between communications surveillance programmes and EU competences remains a contested one. Intelligence activities are said to remain within the scope of Member States exclusive competences in the EU legal system.⁶³ Yet, **are Member States large scale surveillance programmes outside the remits of EU's intervention?** This Section develops three main legal modalities of action to assess and critically examine EU mass surveillance programmes from an EU law viewpoint: First, the concept of national security in a democratic rule of law framework (Section 3.1); Second, the insecurity of the Union and its citizens (Section 3.2); Third, home affairs agencies activities (Section 3.3).

3.1. National Security and Democratic Rule of Law

Large scale surveillance programmes implemented by some EU Member States stand in a difficult relationship with EU founding commitments, principles and legal obligations as outlined in Article 2 TEU. This provision identifies a set of principles which are deemed to be common to all EU Member States and which include, amongst others, the respect of democracy, rule of law and human rights. It is argued that EU surveillance programmes are incompatible with **minimum democratic rule of law standards which are in turn constitutive components of their national constitutional traditions**. This is premised on an understanding of rule of law as the legally based rule of a democratic state, which delivers fundamental rights. O'Donnell has argued that the rule of law should not only be understood as a generic characteristic of the legal system and the performance of the courts, but also as the legally based rule of a democratic state, which delivers fundamental rights (and limits the use of discretion or 'exceptionalism') by state authorities.⁶⁴ According to the 'democratic rule of law' the legal system needs to be in itself democratic and there must be mechanisms of accountability and supervision by an independent judiciary at the heart of the system.

The notion of 'national security' as framed and understood by some intelligence communities and certain national governments in PRISM-like EU programmes does not correspond with **the democratic understanding of national security as foreseen in**

⁶² John Lanchester "The Snowden files: why the British public should be worried about GCHQ", The Guardian, 03/01/2013 accessed 14/10/2013. Available at <http://bit.ly/17oYoB8>

⁶³ This is founded in Article 4.2 Treaty on European Union (TEU) which emphasises that "*The Union shall respect...their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order, and safeguarding national security. In particular, national security remains the sole responsibility of each Member State*". In the same vein, Article 72 of the Treaty on the Functioning of the European Union (TFEU) stipulates that "*This Title shall not affect the exercise of the responsibilities incumbent upon Member States within regard to the maintenance of law and order and the safeguarding of internal security*".

⁶⁴ G. O'Donnell (2004), The Quality of Democracy: Why the Rule of Law Matters? *Journal of Democracy*, Vol. 15, No. 4, October.

Member States' constitutional systems, where a key element of constitutionality remains in the effective judicial control and supervision of executive or governmental actions, including those circumscribed under the boundaries of State's national security.⁶⁵

National constitutional traditions not only formally foresee the democratic and rule of law foundations of the state, where 'the arbitrary' is carefully limited (so there exists an adequate level of protection against abuse of power) and must be read from the perspective of the separation of powers principle. Government and law enforcement are in this way under scrutiny of the judiciary and open justice. Member States constitutions now also feature European fundamental human rights commitments and standards emerging from **the European Convention of Human Rights and the EU Charter of Fundamental Rights**. These bring the jurisprudence and transnational supervision from the Strasbourg Court (Section 3.1.1) and the Court of Justice of the European Union (Section 3.1.2) at the core of the evolving national practices and concepts of 'national security'.

3.1.1. National Security and the ECHR

There is a significant body of jurisprudence by the European Court of Human Rights (ECtHR) on what constitutes interference "*prescribed by law*" in the context of secret surveillance and information gathering. The judge-made requirements of "*in accordance to the law*" and "*necessary in a democratic society*" have consolidated themselves as key testing standards at times of determining the lawfulness and proportionality of government's interferences with fundamental human rights such as those foreseen in Article 8 of the European Convention of Human Rights (ECHR), which lays down the right to respect for family and private life.

A key issue of contestation before Strasbourg has been the extent to which national governments justifications to interfere with ECHR rights have been 'in accordance with the law' or 'prescribed by the law', pursue a legitimate aim and are necessary in a democratic society. In its landmark judgment *Weber and Saravia v. Germany* of 2006,⁶⁶ the Court examined the legality of the extension of the powers of the German Federal Intelligence Service with regard to the recording of telecommunications in the course of so-called 'strategic monitoring',⁶⁷ as well as the use of personal data obtained and its transmission to other authorities. The Court dismissed the applicants' complaints under

⁶⁵ Refer for instance the Case *Binyam Mohamed v. The Secretary of State for Foreign and Commonwealth Affairs*, 10.2.2010, where the England and Wales Court of Appeal ruled that (Paragraphs 132 and 133):

the ultimate decision whether to include the redacted paragraphs into the open version of the first judgment is a matter for judicial, not executive, determination (...) It is ultimately for a judge, not a minister to decide whether a document must be disclosed, and whether it can be referred to, in open court. That decision is for a judge, not a minister, not least because it concerns what goes on in court, and because a judge is better able to carry out the balancing exercise (...) Furthermore, practically any decision of the executive is subject to judicial review, and it would seem to follow that a minister's opinion that a document should not be disclosed in the national interest is, in principle, reviewable by a court. (...) What is included in, or excluded from, a judgment is self-evidently a matter for a judge, not a minister. *It is another aspect of the separation of powers that the executive cannot determine whether certain material is included in, or excluded from, the open material in a judgment.* That must be a decision for the judge giving the judgment in issue, subject of course to the supervisory jurisdiction of any competent appellate court. (Emphasis added).

See also German Federal Constitutional Court, Press Release no. 31/2013, 24 April 2013, Counter-Terrorism Database in its Fundamental structures compatible with the Basic Law, but nor regarding specific aspects of its design.

⁶⁶ *Weber and Saravia v. Germany*, no. 54934/00, 29 June 2006, § 80. See also Association for European Integration and Human Rights and Ekimzhiev, cited above, §§ 75-77.

⁶⁷ "Strategic monitoring is aimed at collecting information by intercepting telecommunications in order to identify and avert serious dangers facing the Federal Republic of Germany, such as an armed attack on its territory or the commission of international terrorist attacks and certain other serious offences." See § 4 and paragraphs 18 et seq. of the judgement.

Article 8 ECHR on the basis that the German legislation⁶⁸ provided adequate and effective guarantees against abuses of State's strategic monitoring powers, and the interferences with the secrecy of telecommunications were necessary in a democratic society in the interests of national security and for the prevention of crime.

However, the Court established in the *Weber* case a set of criteria for determining the lawfulness of secret surveillance and interference of communications and to avoid 'abuse of powers' and arbitrariness. The Court underlined that the risks of arbitrariness are particularly evident in those cases where a power vested in the executive is exercised in secret, and therefore held that

It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated... The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures...⁶⁹

In particular, the following **minimum safeguards** were highlighted, which should be set out in statute law in order to avoid abuses of power: First, the nature of the offences which may give rise to an interception order; Second, a definition of the categories of people liable to have their telephones tapped; Third, a limit on the duration of telephone tapping; Fourth, the procedure to be followed for examining, using and storing the data obtained; Fifth, the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.⁷⁰ The ECtHR added in this respect that

... it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.⁷¹ (Emphasis added)

The ECtHR found the UK's secret interception of communications to be in violation with Article 8 of the ECHR in the case *Liberty v. UK*.⁷² In contrast with the situation addressed in *Weber*, the Court considered that UK domestic law did not provide sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. It therefore found the UK to be in violation of Article 8 and that the interference with the applicants' rights was not being "in accordance with the law".

The ECtHR paid especial attention to **the requirement of foreseeability**, i.e. the extent to which UK domestic law that was adequately accessible and formulated with sufficient precision as to be foreseeable. The authorities' conduct was not "in accordance with the law" because it was unsupported by any predictable legal basis satisfying the accessibility principle.⁷³ The ECtHR stated that "*The expression "in accordance with the law" under Article 8 § 2 requires, first, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be compatible with the rule of law and accessible to the person concerned, who must, moreover, be able to foresee its consequences for him*"⁷⁴ The ECtHR noted the

⁶⁸ Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses), also called "the G 10 Act", as modified by the Fight against Crime Act of 28 October 1994 (*Verbrechensbekämpfungsgesetz*).

⁶⁹ *Weber and Saravia v. Germany*, op. cit. §93.

⁷⁰ § 95.

⁷¹ § 94.

⁷² *Liberty and Others v. the United Kingdom*, no. 58243/00, 1/10/2008.

⁷³ § 56 of *Liberty v. UK*.

⁷⁴ The Court recalled its findings in previous cases (see *Weber and Saravia v. Germany* (dec.), no. 54934/00, 29 June 2006, § 78) "that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the

Government's concern that "the publication of information regarding the arrangements made by the Secretary of State for the examination, use, storage, communication and destruction of intercepted material during the period in question might have damaged the efficacy of the intelligence-gathering system or given rise to a security risk". However, it stated that

...the German authorities considered it safe to include in the G10 Act, as examined in Weber ..., express provisions about the treatment of material derived from strategic interception as applied to non-German telephone connections. In particular, the G10 Act stated that the Federal Intelligence Service was authorised to carry out monitoring of communications *only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order and which search terms had to be listed in the monitoring order*. Moreover, the rules on storing and destroying data obtained through strategic monitoring were set out in detail in section 3(6) and (7) and section 7(4) of the amended G10 Act. ... The G10 Act further set out detailed provisions governing the transmission, retention and use of data obtained through the interception of external communications.⁷⁵ (Emphasis added).

In *Kennedy v. UK*⁷⁶ the ECtHR further examined the extent to which the secret interception of communications by the UK security services was in accordance to the law and necessary in a democratic society. The Court acknowledged that the Contracting States enjoy a *certain margin of appreciation* in assessing the existence and extent of such necessity, but stressed that **this margin is nonetheless subject to European supervision**. It also pointed out that "the values of a democratic society must be followed as faithfully as possible in the supervisory procedures, if the bounds of necessity are not to be exceeded".⁷⁷ It also stated that in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, **it was in principle desirable to entrust supervisory control to a judge**,⁷⁸ and that **sufficient detail should be provided of the nature of the offences in question**.⁷⁹

In contrast to the *Liberty and Others* case which concerned the legislation on interception of communications between the United Kingdom and any other country (external communications), *Kennedy* concerned 'internal communications' which comprise communications within the UK. The Court recalled that under UK law "*Indiscriminate capturing of vast amounts of communications is not permitted under the internal communications provisions of RIPA*".⁸⁰ The ECtHR restated the **three criteria according to which an interference with a ECHR right may be justified and legitimate**: First, the impugned measure must have some basis in domestic law. Second, the domestic law must be compatible with the rule of law and accessible to the person concerned. Third, the person affected must be able to foresee the consequences of the domestic law for him.⁸¹ The ECtHR also insisted that powers to instruct secret surveillance of citizens are only tolerated under Article 8 "**to the extent that they are strictly necessary for safeguarding democratic institutions**", which in practice means that

telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them", § 59. See, among other authorities, *Kruslin v. France*, judgment of 24 April 1990, Series A no. 176-A, § 27; *Huvig v. France*, judgment of 24 April 1990, Series A no. 176-B, § 26; *Lambert v. France*, judgment of 24 August 1998, Reports of Judgments and Decisions 1998-V, § 23; *Perry v. the United Kingdom*, no. 63737/00, § 45, ECHR 2003-IX; *Dumitru Popescu v. Romania* (No. 2), no. 71525/01, § 61, 26 April 2007.

⁷⁵ § 68 of *Liberty v. UK*.

⁷⁶ *Kennedy v. the United Kingdom*, no. 26839/05, 18.8.2010.

⁷⁷ § 154. See also *Kvasnica v. Slovakia*, no. 72094/01, § 80, 9 June 2009.

⁷⁸ § 167. See *Klass and Others*, § 56.

⁷⁹ § 159.

⁸⁰ *Liberty and Others*, § 64.

⁸¹ See for instance *Rotaru v. Romania*, § 52; *Liberty and Others*, § 59; and *Iordachi and Others*, § 37.

... there must be *adequate and effective guarantees against abuse*. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.⁸² (Emphasis added).

The Court has repeatedly stressed in its case law the importance of giving a narrow interpretation to exceptions to basic fundamental human rights envisaged in the ECHR, in particular to protect the individual against any abuse of power and in what concerns human rights where no exceptions are allowed (absolute in nature). Cases related to the so-called 'extraordinary renditions and secret detentions' have been illustrative in this regard and have developed **democratic rule of law standards which establish the boundaries of lawfulness of secret intelligence activities in a democratic society**. As a way of illustration, the Court ruled in *El-Masri v. Macedonia* that an essential object of Article 8 ECHR "is to protect the individual against arbitrary interference by the public authorities" and that the interference must be "in accordance with the law".⁸³ In respect of the violation of Article 5 ECHR (right to liberty and security), the Court held that

Although the investigation of terrorist offences undoubtedly presents the authorities with special problems, that *does not mean that the authorities have carte blanche* under Article 5 to arrest suspects and detain them in police custody, free from effective control by the domestic courts and, in the final instance, by the Convention's supervisory institutions, whenever they consider that there has been a terrorist offence.⁸⁴ (Emphasis added).

In *Nada v. Switzerland* of 2012,⁸⁵ the ECtHR dealt with the review of the sanctions regime established by Security Council Resolution 1267 (1999) to freeze the funds and other financial resources of the individuals and entities identified by the Security Council's Sanctions Committee as being associated with Osama bin Laden, al-Qaeda or the Taliban, and the human rights consequences of the inability of the listed persons to challenge effectively the decision to list them. The Court held that an interference with ECHR rights could be considered "*necessary in a democratic society*" for a legitimate aim "*if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are "relevant and sufficient"*".⁸⁶ It added that for a measure to be regarded as proportionate and as necessary in a democratic society, the possibility of recourse to an alternative measure that would cause less damage to the fundamental right at issue whilst fulfilling the same aim. Moreover, the ECtHR reiterated that in any event **the final evaluation of whether the interference is necessary remains subject to review by the Court for conformity with the requirements of the Convention**.⁸⁷

⁸² See § 153. *Klass and Others*, cited above, §§ 49 to 50; and *Weber and Saravia*, cited above, § 106.

⁸³ *El-Masri v. Macedonia*, No. 39630/09, 13 December 2012.

⁸⁴ *El-Masri v. Macedonia*, op. cit., § 232.

⁸⁵ *Nada v. Switzerland*, No. 10593/08, 12 September 2012.

⁸⁶ § 180. See also *S. and Marper*, cited above, § 101, and *Coster v. the United Kingdom* [GC], no. 24876/94, § 104, 18 January 2001).

⁸⁷ § 184. However,

"A margin of appreciation must be left to the competent national authorities in this connection. The breadth of this margin varies and depends on a number of factors including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference (see *S. and Marper*, § 102)."

The Court concluded that

the restrictions imposed on the applicant's freedom of movement for a considerable period of time did not strike a fair balance between his right to the protection of his private and family life, on the one hand, and the legitimate aims of the prevention of crime and the protection of Switzerland's national security and public safety, on the other. Consequently, the interference with his right to respect for private and family life was not proportionate and therefore not necessary in a democratic society. § 198.

3.1.2. National Security and the EU Charter of Fundamental Rights

A second legal modality of action when assessing EU large-scale surveillance programmes in a selection of EU Member States is their relationship with the EU Charter of Fundamental Rights. The EU Charter has been recognised the same legal value as the Treaties since the entry into force of the Lisbon Treaty. The EU Charter comes along a set of EU general principles some of which find their origins in national constitutional traditions and others have been further developed by the CJEU jurisprudence. The national constitutional traditions of EU Member States are illustrating **a progressive 'process of constitutionalisation' of the EU Charter in their domestic legal systems**. This has been confirmed by the European Commission's 2012 Annual Report on the Application of the EU Charter,⁸⁸ which covered an assessment of the Member States' frameworks of judicial reviews of 'constitutionality', and which concluded that

The analysis of court rulings referring to the Charter further suggests that national judges *use the Charter to support their reasoning, including when there is not necessarily a link with EU law*. There is also some evidence of an incorporation of the Charter *in the national systems of fundamental rights protection*.⁸⁹ (Emphasis added)

The CJEU pointed out in *Fransson*⁹⁰ that 'outside the scope of EU law' national authorities and courts remain free to apply national standards of protection of fundamental rights, **provided that the level of protection offered for by the Charter, as interpreted by the Court, and the primacy, unity and effectiveness of European law are not compromised**. The CJEU has in this way held that the EU Charter is becoming a constitutive component of 'the national constitutional traditions' of EU Member States. As Vice-President of the European Commission, Viviane Reding has stated,⁹¹

The concept of national security does not mean that "*anything goes*": States do not enjoy an unlimited right of secret surveillance. In Europe, also in cases involving national security, every individual – irrespective of their nationality – can go to a Court, national or European, if they believe that their right to data protection has been infringed. *Effective judicial redress is available for Europeans and non-Europeans alike. This is a basic principle of European law*. (Emphasis added).

In the same vein, Reding reiterated the relevance of the EU Charter presentation on 19 June 2013 at the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament.⁹² During the questions and answers, and following questions from MEPs referring to the lack of EU competence in what concerns intelligence services activities, Reding stated that

... "intelligence" of course is not in our remit, but ... *even in questions of intelligence the fundamental rights which are inscribed in our basic text are not eliminated but they are also to be considered*. So the position of the European Commission and the defence of the fundamental rights of the citizens is without any doubt in that respect. (Emphasis added).

⁸⁸ European Commission, 2012 Annual Report on the Application of the EU Charter of Fundamental Rights, 2013, European Commission, DG for Justice, retrievable from http://ec.europa.eu/justice/fundamental-rights/files/charter_report_2012_en.pdf

⁸⁹ Ibid, page 15. Reference was in particular made to the Austrian Constitutional Court, Cases U 466/11 and U 1836/11, 14.3.2012, where according to the European Commission the Constitutional Court

... recognised the very special role of the Charter within the EU legal system, and its different nature compared to the body of rights and principles which the Court of Justice of the EU has been developing throughout the years. It took the view that the Charter is enforceable in the proceedings brought before it for the judicial review of national legislation, and therefore individuals can rely upon the rights and the principles recognised in the Charter when challenging the lawfulness of domestic legislation. The Austrian Constitutional Court identified strong similarities between the role played by the Charter in the EU legal system and that played by the ECHR under the Austrian Constitution, according to which the ECHR has force of constitutional law.

⁹⁰ Case C-617/10, *Fransson*, 26 February 2013.

⁹¹ V. Reding, PRISM scandal: The data protection rights of EU citizens are non-negotiable, Press Conference, EU-U.S. Justice and Home Affairs Ministerial /Dublin, 14 June 2013.

⁹² Refer to www.europarl.europa.eu/news/en/news-room/content/20130617IPR12352/html/PRISM-EU-citizens'-data-must-be-properly-protected-against-US-surveillance

The relevance of effective and open justice was underlined by CJEU in the case *ZZ v. Secretary of the State of Home Department* C-300/11, of 4 June 2013, which confirmed that the provision of effective judicial review is a central component even within the scope of Member States measures adopted on the basis of 'State security'.⁹³ The CJEU was of the opinion that "*although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision concerns State security cannot result in European Union law being inapplicable*".⁹⁴ It added that in those circumstances where a national authority opposes precise and full disclosure to the person concerned of the grounds constituting a decision refusing entry in a Member State for reasons of State security,⁹⁵ Member States are required to

... first, to provide for effective judicial review both of the existence and validity of the reasons invoked by the national authority with regard to State security and of the legality of the decision taken under Article 27 of Directive 2004/38 and, second, to prescribe techniques and rules relating to that review, as referred to in the preceding paragraph of the present judgment.⁹⁶

The CJEC concluded that the contested regulations, which did not provide for any remedy in respect of the freezing of assets, were in breach of fundamental rights and were to be annulled. Here also, the relevance of effective judicial review and scrutiny was identified as a central component of an EU understanding of rule of law. The Luxembourg Court held that such review should be seen as a "**constitutional guarantee**" forming part of the very foundations of the Community and that

... the Community is based on the rule of law, inasmuch as neither its Member States nor its institutions can avoid review of the conformity of their acts with the basic constitutional charter, the EC Treaty, which established a complete system of legal remedies and procedures designed to enable the Court of Justice to review the legality of acts of the institutions.⁹⁷ (Emphasis added).

3.2. Whose Security? Sincere Cooperation and Citizens' Liberties Compromised

The legal tensions between large-scale surveillance and democratic rule of law with fundamental rights endanger as a consequence the security of the Union and that of its citizens, and unleash insecurity for the Union as a whole. The intelligence communities' understandings and practices of national security and Member States' surveillance programmes equally jeopardise the EU principle of sincere cooperation, as they make more difficult carrying out the tasks flowing from the Treaties and put at risk the attainment of the Union's objectives, including those in external relations and the common foreign and security policy.⁹⁸

⁹³ See also the Kadi Judgement on judicial supervision <http://curia.europa.eu/juris/document/document.jsf?text=&docid=139745&pageIndex=0&doclang=FN&mode=lst&dir=&occ=first&part=1&cid=205883>, Paragraphs 326 and 327.

⁹⁴ See Case C-387/05 *Commission v Italy* [2009] ECR I-11831, paragraph 45.

⁹⁵ 57 states that "However, if, in exceptional cases, a national authority opposes precise and full disclosure to the person concerned of the grounds which constitute the basis of a decision taken under Article 27 of Directive 2004/38, by invoking reasons of State security, the court with jurisdiction in the Member State concerned must have at its disposal and apply techniques and rules of procedural law which accommodate, on the one hand, legitimate State security considerations regarding the nature and sources of the information taken into account in the adoption of such a decision and, on the other hand, the need to ensure sufficient compliance with the person's procedural rights, such as the right to be heard and the adversarial principle".

⁹⁶ Paragraph 58. See also paragraphs 65 and 66.

⁹⁷ Paragraph 281. Case 294/83 *Les Verts v Parliament* [1986] ECR 1339, paragraph 23.

⁹⁸ Refer to Article 4.3 TEU which states that "*Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties. The Member States shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions*

The violations of democratic rule of law and fundamental rights inherent to large-scale surveillance, and their supranational nature and fundamentals, affect the security of the Union as a whole. They also jeopardize the use of legally established channels at EU level, some of which have been concluded with the USA. As Reding said in the above mentioned intervention in the EP LIBE Committee in June 2013, "*if you don't go through the MLA and directly to companies asking data of EU citizens that is a violation of international law (Recital 90 of Regulation)*".

In a Council of the EU Discussion Paper on COSI and terrorism it was stated that

Regardless of this [i.e. Article 4.2 TEU], the transnational nature of terrorism and its perpetrators makes it a clear threat also *to the common internal security of the Union*. It is therefore important that the work against terrorism, at least *when it affects the EU as a whole*, is coordinated so that it can be conducted efficiently and focused on common identified and prioritised threats.⁹⁹ (Emphasis added).

A similar argument could be used in light of the nature of some of the EU large-scale surveillance programmes existing in a number of Member States. Just as 'acts of political violence' are said to be increasingly supranational, so the process of 'intelligence gathering' are supranational as well, coming from a variety of sources abroad or 'at home'. Their supranational nature and implications make the national security as framed and understood by certain actors in the 'intelligence communities' not only in tension with the security of that state as democratic rule of law, but also that of the other Member States and the of the Union as a whole.

EU large-scale surveillance programmes also compromise the security and fundamental human rights of citizens and residents in the Union, in particular those related to privacy and effective legal protection. The involvement of certain EU Member States in NSA programmes deprive EU citizens of their ownership of their personal and private data, and subject them to discriminatory treatments, i.e. nationals of other EU Member States are subject to a larger disproportionate impact of large scale surveillance programmes, as they are unjustifiably less favorably treated than nationals as privacy holders in interceptions of 'internal communications'. For example, Privacy International has argued that the UK Tempora programme involves unjustified discrimination against non-UK nationals and EU citizens. In its submission, Privacy International highlighted that

Further, the operation is in breach of Article 12(1) TFEU. The Tempora operation has a disparate adverse impact on EU citizens who are not nationals of the United Kingdom. This is because a certification under section 8(4) of RIPA 2000 can only be granted in respect of the interception of external communications, which are more likely to be made by non-UK citizens. Union citizens who are not UK citizens are far more likely to have their communications intercepted, searched and retained. Both UK citizens and non-UK citizens pose risks to national security. Accordingly, such differences in

of the Union. The Member States shall facilitate the achievement of the Union's tasks and refrain from any measure which could jeopardise the attainment of the Union's objectives." See also Article 24.3 TFEU which stipulates that "*The Member States shall support the Union's external and security policy actively and unreservedly in a spirit of loyalty and mutual solidarity and shall comply with the Union's action in this area. The Member States shall work together to enhance and develop their mutual political solidarity. They shall refrain from any action which is contrary to the interests of the Union or likely to impair its effectiveness as a cohesive force in international relations."*

⁹⁹ Council of the EU (2013), Discussion Paper on COSI and Terrorism, 10162/13, Brussels, 3 June 2013, p. 3. See also Council of the EU, Standing Committee on Operational Cooperation on Internal Security (COSI), Summary of Discussions, 11265/13, Brussels, 24 June 2013, page 5, where it was said that

The Swedish discussion paper on the COSI competences and tasks with regard to terrorism (doc. 10612/12) was welcomed by various delegations. Several delegations suggested having a wider debate at some stage on whether COSI is fulfilling its mandate and where it could provide added value, including in the context of the Council's JHA structures (CATS, SCIFA). Delegations felt that COSI could address the topic of terrorism but with due respect to the provisions of the Treaty and Member States' competences. Delegations also highlighted that duplication of efforts with other working parties such as the Terrorism Working Party and COTER should be avoided.

treatment are not justifiable or lawful. A systematic scheme of processing of personal data primarily directed at non-UK nationals cannot be justified under EU law.¹⁰⁰

There is also a fundamental gap in current EU legal framework which increases the vulnerability of citizens privacy-related rights and liberties. As additionally alleged by Privacy International in its complaint before the Strasbourg Court of July 2013.¹⁰¹ They highlight in particular that those differences between foreign and domestic interception and information gathering regimes lead to an absence of legal protection when information is shared between countries.

PRISM-like surveillance programmes challenge this premise (a central distinction has been made between foreign and domestic interception and information gathering secret regimes), and reveal a gap in protection and accountability in the EU. **Are the distinctions between internal and external communications any longer relevant in what concerns warrant schemes for interceptions in Member States legal systems?**¹⁰²

3.3. Home Affairs Agencies

Another means by which large scale surveillance practices blur the lines between national sovereignty and matters relating to EU competence is their potential spillover into the security activities of the EU institutions and its agencies. More precisely, EU liability may be invoked where the EU's institutions and its agencies become implicated in sharing and exploiting data generated by national large scale surveillance operations.

This is particularly relevant as regards the activities of EU Home Affairs agencies which play a central role in putting into practice the "comprehensive model for information exchange" which sits at the heart of the EU's Internal Security Strategy.¹⁰³ Europol and INTCEN (and to a lesser extent Eurojust, Frontex and OLAF) are key actors at the forefront of gathering, exchanging and processing information often based on consolidated versions of reporting and contributions from Member States' national security and intelligence agencies.

¹⁰⁰ Privacy International submission to the Investigatory Powers Tribunal, 'Statement of Grounds', 8 July 2013, paragraph 57, available at: www.privacyinternational.org. Reference was here made to the Case C-524/06 *Huber v Germany* [2008] ECR I-9705 at [69-81].

¹⁰¹ "With communication being increasingly global, and vast amounts of personal data being transferred and stored around the world, there is an obvious gap in legal protection to ensure respect for private life. The regimes in both the US and the UK governing the interception, obtaining, and storing of material deal differently with foreign and domestic interception and information gathering (in the UK the difference depends on whether communication is regarded as "internal" or "external" and in the US on whether or not the person targeted is a non-US citizen located outside the US). Those differences between foreign and domestic interception and information gathering regimes lead to an absence of legal protection when information is shared between countries. UK authorities can intercept communications sent or received by individuals located in the US (and which will be regarded as "external" for the purposes of RIPA), which happen to pass through UK fibre cables, and hand them over to US authorities, thus avoiding the US rules governing interception of those located within the country. The NSA can intercept an email under FISA section 1881a which is sent between two individuals in London because it happens to travel through the US as it will be regarded as "foreign intelligence material" as far as the US authorities are concerned, and it can then be handed over to the UK authorities without their having to comply with any of the requirements governing interception set out in RIPA and the Code of Practice. The same is true of private information about UK residents stored by internet companies in the US." *Ibid*, paragraph 45.

¹⁰² *Liberty vs. UK*

14. The IPT found that the difference between the warrant schemes for interception of internal and external communications was justifiable, because it was more necessary for additional care to be taken with regard to interference with privacy by a Government in relation to domestic telecommunications, given the substantial potential control it exercised in this field; and also because its knowledge of, and control over, external communications was likely to be much less extensive. THIS IS NO LONGER THE CASE

¹⁰³ E. Guild and S. Carrera (2011), 'Towards an Internal (In)security Strategy for the EU?' CEPS Liberty and Security Series, January 2011.

Europol for instance relies to a large degree on the input of member states' intelligence services to feed its strategic analysis products, such as the annual EU Terrorism and Situation and Trend Reports (TE-SAT).¹⁰⁴ Similarly the EU Intelligence Analysis Centre (INTCEN) within the EEAS acts as 'a single entry point in the EU for classified information coming from Member States' civilian intelligence and security services' and on this basis produces intelligence analyses, early warnings and situational awareness to the EEAS, EU decision-making bodies and member states.¹⁰⁵

The processes surrounding the exchange of intelligence between the member states and EU home affairs agencies like Europol and INTCEN are notoriously opaque.¹⁰⁶ There is no mechanism to verify the nature of data and information transferred to EU level, nor to ensure that the sources and means by which such data is generated are legitimate and in compliance with the national laws of the member state in question and EU fundamental rights standards. Europol Director Rob Wainwright, during the European Parliament Hearing of 24th September 2013, stressed that the EU's law enforcement agency "has no contacts at all with the NSA or CIA".¹⁰⁷ However, he conceded that data dealt with by Europol agents and received direct from the member states may originate from EU intelligence agencies, and even the NSA. The lack of clarity in this response is somewhat in keeping when one considers the gaps in oversight that characterise the flow of information within the agency: a significant proportion of the data that passes through Europol is understood to be exchanged bi-laterally between national liaison officers stationed in Europol. However, it provides little reassurance as to the trusted nature of Europol's information sources.

There is therefore a strong possibility that tainted information – i.e. data gleaned from unlawful mass surveillance or exchanged without due regard for compliance with fundamental rights, data protection and privacy standards, would enter the AFSJ and be shared and processed at EU level. This possibility should bring a number of concerns for EU lawmakers. It implies a degree (however limited) of complicity by EU agencies in practices which present a number of tensions with fundamental EU legal principles and human rights standards. EU agencies could therefore share in any liability resulting from the mis-use of this data.

The liability incurred by EU agencies raises an important side issue about the data that is handled by these organisational actors and the justification for their access to often sensitive information. As Geyer notes, when considering the risk that EU institutions and agencies have handled intelligence resulting from extraordinary rendition and the torture of terror suspects, information processed at EU level does not serve to avoid 'imminent security threats' but rather serves mid- and long-term policy objectives or – as in the case of Europol and INTCEN – the creation of risk analysis, strategic reports and threat assessments. In this light, the already questionable argumentation brought forward at national level to justify the use of large scale surveillance techniques, i.e. to counter direct threats to national security, is even less applicable to the access and use of such information at EU level.¹⁰⁸

Finally, the sharing of intelligence with EU agencies such as Europol further blurs the question of legal competence. Europol is established under Article 88 of the Lisbon Treaty

¹⁰⁴ See Europol, *TE-SAT 2013 – EU Terrorism Situation and Trend Report*.

¹⁰⁵ EU Intelligence Analysis Centre (EU INTCEN), Factsheet. Available at: www.asktheeu.org/en/request/637/response/2416/attach/5/EU%20INTCEN%20Factsheet%20PUBLIC%20120618%201.pdf

¹⁰⁶ J. Parkin (2012), *EU Home Affairs Agencies and the Construction of EU Internal Security*, CEPS Liberty and Security Series, December 2012; C. Jones (2013), *Secrecy reigns at the EU's Intelligence Analysis Centre*, Statewatch Analysis.

¹⁰⁷ European Parliament, LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, 23 September 2013.

¹⁰⁸ F. Geyer (2007), *Fruit of the Poisonous Tree – Member States' Indirect Use of Extraordinary Rendition and the EU Counter-Terrorism Strategy*, Centre for European Policy Studies, 3 April 2007.

under chapter V, 'Police Cooperation' and its legal mandate establishes the agency as a law enforcement body. However, the sharing of information with Europol by national intelligence services not only potentially compromises the agency's integrity, it also renders indistinguishable the boundaries of what is police cooperation and what is intelligence at EU level. The tendency reflects the merging of police, military and intelligence logics and practices that we've seen at national level in the operation of large scale surveillance programmes (see section two) and creates a legal insecurity and uncertainty in the actions of EU agencies. This could partly be addressed during the forthcoming revision of Europol's legal mandate, in order to ensure greater accountability and oversight of this agency's actions. Despite claims as to the necessity of such intransparency/autonomy as central to EU home affairs agencies functioning, the application of a 'balance approach' is not applicable given that the activities of these agencies hold profound implications for human rights and liberties.

4. Conclusions and Recommendations: Implications of Large Scale Surveillance for Freedom, Fundamental Rights, Democracy and Sovereignty in the EU

4.1. General conclusions

In light of the previous sections, the implications of the different programmes that have engaged into practices of large-scale surveillance have to be underlined, especially from a fundamental rights perspective. These implications are far reaching and go beyond the traditional dilemma between the rights of citizens to data protection and the right of the state to depart from the Rule of law in the name of national security. They raise questions about the nature of our political regimes, and the nature of sovereignty.

As we have explained in section 2, what is at stake is not an opposition between the USA and Europe. **What is at stake is what is done with the data gathered by intelligence services when large-scale surveillance is taking place: is it "targeted" surveillance, or "mass-surveillance"?** Most European services involved in the fight against terrorism and organised crime have used the large-scale collection of metadata as a way to "connect the dots" between the activities of suspects in criminal investigations. They have used surveillance in order to reconstitute networks of possible suspects associated with their main target, drawing both on real-time and stored data. In this case, even if large-scale collection is taking place, it may be considered as "targeted surveillance". Based on warrants and on clear purposes that can be overseen at a later date, it can be justified. This is the kind of surveillance that the legal framework of the EU-US Mutual Legal Assistance Agreement (MLAA) has organised. Even if some lawyers consider that this scope is already a problem for data protection and privacy, this agreement at the very least allows room for negotiation.

However, in the case of European services collaborating with the NSA through the different surveillance programmes, the situation is markedly different. These collaborations have been kept secret and go beyond the legality of the agreements in place. One can presume they may have implied forms of spying activities against European companies in favour of US companies. One can also presume they may have breached the solidarity principle between European countries in favour of other alliances, notably by sending data of other European citizens without the knowledge of their own state to the NSA and its allies of the enlarged Five Eyes network. One can wonder if routine practices that exceed mere targeted surveillance and that de facto emancipate intelligence services from principles of rule of law have taken place. The question remains: how far this surveillance goes? How data obtained by such surveillance are exploited?

Once extracted, data may be used for multi-purposes if they are retained, either by intelligence services, Internet providers or their subcontractors. Some journalists and people interviewed have pointed out that extension of large scale surveillance expands the number of persons put on watch lists around the world, with the tendency to consider that the best platform for watch lists is one with "more people in it", without further considering the quality of the information on which such lists are based. To what extent can these forms of profiling and strategic surveillance be considered as data mining?

It seems that NSA surveillance programmes resemble the TIA: they are multi-purpose, warrantless and may imply forms of data mining. They are not just anti-terrorist programmes set up to detect plotters working against the national interests of the United States – despite the NSA Director' claim that this was the case. We still do not know if it is the case or not, but if data mining and predictive analytics are involved, the analysis of the different programmes involving large scale surveillance cannot be reduced to a question of a balance between security and privacy, nor to a question of asymmetry of sovereignties in diplomatic alliances: it is a question of security measures putting

democracy at risk. **A first challenge for the future is therefore to discuss the legitimacy of such programmes and to prevent the path leading to data mining.**

A second challenge is to assess the efficiency of this type of surveillance. At a very pragmatic level, large-scale surveillance appears to have strong limitations and is certainly not key in crime prevention. Such surveillance creates a double tendency. The first tendency is to collect data extensively and retain them over a long period of time in order to establish series of trends that facilitates big data correlations and hierarchies. The question of data retention is thus significant, and raises considerable legal challenges. The second tendency is to create additional categories that encapsulate series of criteria of profiling, in order to target specific groups of individual that can be managed by human beings. The question of human resources managing these data thus becomes an important one too. These retention and selection process are supposedly in place to ensure the *quality* of the information, whereas *quantity* can generates errors (false negatives and false positives). However, one can easily see that even if algorithms can help to connect a series of elements, this will not necessarily give a meaningful result in terms of prevention. Even if cyber surveillance can help to "connect the dots", most of the time such gathering of information becomes meaningful only *after* a specific event has occurred, not *before*. Stella Remington, former Director General of MI5, recalled this very eloquently when she explained that despite the fact that the intelligence services in Boston had information on the Chechen perpetrators of the Boston bombings in April 2013, they were unable to anticipate the attack and therefore the services in charge could not be held responsible for what happened. She explicitly made the point that, even with computer programmes, it was not possible to put under effective surveillance a group of people with less than five agents on each case. In light of the numerous uncertainties that surround cyber/communications surveillance, she also expressed doubts and concerns about the costs of investments in this kind of surveillance, as, as she pointed out: it is impossible to 'keep tabs on every suspect'.¹⁰⁹ In addition mass surveillance via data mining may be a strategy to retrofitting evidence in a case after having exercised undue surveillance and may disrupt the process of criminal justice instead of accelerating it. Large scale surveillance is in that case not oriented towards evidence findings, but towards an array of presumptions, which are justified ex-post through allegations of contacts between individuals that may be at three levels of association from each other.

A third challenge is to revisit US/EU relationships in the field of surveillance. At a diplomatic level, the US largely dominates the diplomacy of surveillance, in ways that clearly disrupt the cohesion of the EU in the field. The US surveillance agencies have maintained a matrix of reading and cooperation inherited from the cold war with three different layers:

- The Five Eyes (US-UK-Canada-Australia-New Zealand) that originated from a 1946 multilateral agreement for cooperation in signals intelligence, with which the US partly cooperate in collecting information and sharing results; network which has extended over time in terms of tasks with Echelon and in terms of privileged partners, especially Sweden that, accordingly to Mark Klamberg, permit to 5 eyes to gain access to the internet cables of the baltic states and Russia through them, as well as the special relationship of 5 eyes with Israel for all the region of Middle East.
- Some EU countries with whom the US had ad hoc collaborations and sometimes aggressive relationships (France, Germany, Italy, Benelux and Switzerland, Poland); in terms of collaborations, the DGSE in Paris was the node of a different network of 6 countries called Alliance base, different from Five Eyes and regrouping four of the five eyes (New Zealand is not in – may be as a reminder of the rainbow warrior), but adding France and Germany. Alliance base is believed to

¹⁰⁹ R. Alexander (2013), 'Terror Watch Lists: Can You Keep Tabs On Every Suspect?', BBC News, 2 June 2013, available at: www.bbc.co.uk/news/magazine-22718000

have ended in 2009 because of tensions between the French and the US.¹¹⁰ In terms of difficult relationships the US and France have accused reciprocally the other country to have conducted illicit economic espionage.

- The other countries of Europe, Middle East and South America, which they consider as pure targets for their operations and do not want in any collaborative process

It is therefore delusive to consider that the EU Member States as a whole and moreover the EU institutions (Council and Commission) can become a strong stakeholder in negotiations with the US in the field of surveillance, despite the efforts of the EU Counter-Terrorism Coordinator. As an addition, EU Member States also have a different attitude concerning the collaboration with the US in terms of intelligence. This is reflected in their different national laws that explicitly protect the collaboration between their services and the US from investigating judges. Therefore, at a diplomatic level, large scale communications surveillance reveals strong asymmetries at the international level.

A fourth challenge for the future is how to tackle the involvement of private actors in this surveillance game. Private actors have now become a significant part of the large scale surveillance, and play a key mediation role between the state and the citizens' rights. The development of transnational platforms of exchange of information, and the participation at all stages of private actors should receive full attention of the European Parliament. The rights of citizens, but also of consumers are here both at stake. As clearly demonstrated in a previous European Parliament note dedicated to cloud computing¹¹¹, the set of relations currently defining cloud computing technologies and crime prevention encompasses negotiations and tensions between public authorities and private entities. In this set of relationships, data protection and privacy are often objects of negotiations to the detriment of the individuals' rights.

In any case, it appears clear that, at a democratic level, **large scale surveillance restructures the very notion of security and protection of human beings as well as the conceptions we have of freedom and fundamental rights.** The types of profiling large scale surveillance generates is highly discriminatory and disrupts social cohesion. Eminent sociologists have convincingly argued that the use of statistics over specific groups of population not only undermines the idea that diversity is perfectly legitimate and desirable in a free society, but also leads to discrimination and stigmatisation¹¹². The challenges underlined above are paramount for the future of our democracies, and will be with us for some time. Not tackling them would inevitably create room for new scandals and delegitimation of all the actors involved. A lack of actions of the European institutions will not help putting an end to the controversy, while silence could be interpreted as a form of complicity.

The French *Ligue des Droits de l'Homme* has already taken action. As they underlined, these activities are no longer within the scope of antiterrorist and counter-intelligence activities: they are a form of 'fraudulent access and retention in an automated data processing system' with 'illegal collection of personal data', 'violation of intimacy and privacy' and 'violations of the confidentiality of correspondence'.¹¹³ Other NGOs have suggested the link with cyber theft of identities. Could these surveillance activities be

¹¹⁰ Source: D. Servenay (2010), 'Terrorisme: pourquoi Alliance Base a fermé à Paris', Rue89, 24 May 2010, available at: <http://www.rue89.com/2010/05/24/terrorisme-fermeture-dalliance-base-a-paris-152349>

¹¹¹ D. Bigo et al (2012), Fighting cyber crime and protecting privacy in the cloud, Study for the European Parliament, PE 462.509

¹¹² See: H. Becker (1963), *Outsiders: Studies in the Sociology of Deviance*, New York: The Free Press; D. Lyon (2003), *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, London: Routledge; O. H. Gandy, Jr. (2002), "Data Mining and Surveillance in the Post-9.11 Environment", IAMCR Data Mining, 7 November 2002.

¹¹³ See Libération (2013), "Enquête à Paris sur le programme d'espionnage américain Prism", 28/08/2013. <http://bit.ly/1euuQar> Accessed 17/10/2013

considered as forms of cyber crime? Rob Wainwright, Director of Europol, immediately argued that Europol '[has] no mandate to investigate any allegations of unauthorised activities by governments'. This significantly contrasts with Europol's retroactive positions concerning the cyber-attack against Estonia, allegedly carried out by Chinese intelligence services.¹¹⁴

National security is not the sole property of intelligence communities or national governments. National security interests are subject to supra-national democratic rule of law processes and standards, which now include human rights instruments/actors (ECHR) and post-national (fundamental rights) institutions like the European Union and its fundamental rights *acquis*. It could be argued that large scale surveillance practices in EU Member States constitute a systematic and persistent breach of the Union's values as foreseen in Article 7 TEU. Viviane Reding implicitly brought what is occurring in the UK under the remits of Article 7 TEU by stating that:

... you certainly have noted that when a journalist is put under pressure in one of our Eastern Member States, Foreign Ministers from Germany, Britain, France, Sweden and Finland get very excited and ask the Commission to intervene. The European Parliament immediately calls for a plenary debate and tables a motion for a resolution condemning this incident. But we received not a single call from all these Foreign Ministers and all these Parliamentarians when Mr Miranda was arrested at the airport in London three weeks ago. Or when the Guardian had to destroy certain evidence on request of the British government.¹¹⁵

The controversies raised by the recent revelations will not vanish easily, even if legal actions and concrete initiatives may take time. The actions, or the lack of actions, of the European Parliament will be watched carefully. With the European elections approaching, one should not under-estimate the consequences this could have on voters: there is indeed a possible rise of European parties that advocate less power for EU institutions, precisely because the latter are seen as ineffective to protect their citizens and the residents living in the EU. The Commission has already asked the director of the NSA and the UK representative in Brussels to account for what has happened. Letters have been sent and no answers were given. **It is here the credibility of the Commission itself that is at stake, and more generally of the EU institutions.**

4.2. Policy Recommendations

The following recommendations explore possibilities for the EP to fully exercise its role as a safeguard for EU citizens' rights.

Recommendation 1: The European Parliament should use the powers as its disposal to require explanations from the US and to investigate further EU Member States collaborations with the NSA.

It could, for instance, ask for immediate suspensions of some existing agreements, such as the TFTP Agreement. It is also possible to reschedule the agenda concerning the negotiations for the US-EU Transatlantic Free Trade Agreement.¹¹⁶

The EP could also re-introduce proposals that were discarded after intense lobbying from the US administration. The "anti-Fisa clause" (the proposed article 42 of the Data

¹¹⁴ "MEPs raise suspension of EU-US bank data deal", European Parliament, Press release, 24/09/2013. <http://bit.ly/1euwVDh> Accessed 17/10/2013

¹¹⁵ http://europa.eu/rapid/press-release_SPEECH-13-677_en.htm

¹¹⁶ The freezing or termination of the TFTP Agreement with the United States was raised by MEPs during a hearing of the LIBE Committee on 24 September 2013. See www.europarl.europa.eu/news/en/news-room/content/20130923IPR20604/html/MEPs-raise-suspension-of-EU-US-bank-data-deal.

protection regulation draft¹¹⁷), in particular, would have nullified any U.S. request for technology and telecoms companies to hand over data on EU citizens.

The EP could finally launch a specific enquiry on the specific network of intelligence agencies that are working with the NSA in Europe in order to analyse more in detail what is the nature and the scale of their cooperation. A key element would be to assess if the transnational governmental networks that have a transatlantic dimension are engaging in a sort of "privacy shopping" by exchanging targets of surveillance in order to use the loopholes created in many national privacy laws by the existing difference in terms of protection regarding the nationality or/and territory criteria of the surveillance (foreign intelligence justification).

Recommendation 2: A "professional code for the transnational management of data" within the EU should be set up, including guidelines on how this code would apply to EU partners

Such a code could limit the unlawful practices of intelligence services without undermining their efficiency. Sir David Omand, former director of GCHQ between 1996 and 1997, has proposed a series of best practices that could be implemented so that intelligence services act in full respect of democratic rules.¹¹⁸ These elements are central if a red line has to be agreed on, taking into account all the actors involved. These principles raised by David Omand could be used as a "professional" charter, applied to all the services involved in the access to European data:

There must be sufficient sustainable cause. Any tendency for the secret world to encroach into areas unjustified by the scale of potential harm to national interests has to be checked.

There must be integrity of motive. No hidden agendas: the integrity of the whole system throughout the intelligence process must be assured, from collection to analysis and presentation.

The methods used must be proportionate. Their likely impact must be proportionate to the harm that is sought to prevent, for example by using only the minimum intrusion necessary into the private affairs of others.

There must be right and lawful authority. There must be the right level of sign-off on sensitive operations, with accountability up a recognised chain of command to permit effective oversight.

There must be a reasonable prospect of success. All intelligence operations need careful risk management, and before approval is given there has to be consideration of the likelihood of unintended consequences and the impact if the operation were to be exposed or otherwise go wrong

Recourse to secret intelligence must be a last resort. There should be no reasonable alternative way of acquiring the information by non-secret methods.¹¹⁹

An additional principle should be: **one should not mix what constitutes suspicious criminal activities and what constitutes different life styles.** This principle is

¹¹⁷ "Article 42 requires for transfers to third countries, where no adequacy decision has been adopted by the Commission, to adduce appropriate safeguards, in particular standard data protection clauses, binding corporate rules and contractual clauses. The possibility of making use of Commission standard data protection clauses is based on Article 26(4) of Directive 95/46/EC. As a new component, such standard data protection clauses may now also be adopted by a supervisory authority and be declared generally valid by the Commission. Binding corporate rules are now specifically mentioned in the legal text. The option of contractual clauses gives certain flexibility to the controller or processor, but is subject to prior authorisation by supervisory authorities." Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), <http://bit.ly/1hZGREt> Accessed 17/10/2013.

¹¹⁸ David Omand, "NSA leaks: how to make surveillance both ethical and effective", The Guardian, 11/06/2013. <http://bit.ly/1hZI4vy> Accessed 17/10/2013

¹¹⁹ Ibid.

central, not only because the fairness of criminal systems in our democracies is too often destabilised by such mixing, but also because a police state can easily emerge from this¹²⁰. Freedom of thought, of opinion and expression are here at stake. Bans on some specific modalities of data mining have to be explored, along similar lines than what were examined by the US Congress in 2003: the *Data Mining Moratorium Act* (S. 188) proposed by Senator Russ Feingold's (D-WI) and the *Citizens' Protection in Federal Databases Act* (S. 1484) proposed by Senator Ron Wyden's (D-OR). This has been reactivated recently with the *Amash amendment*, narrowly defeated, which would have required the NSA to limit its telephone data collection only to individuals "under investigation".¹²¹

Recommendation 3: the EP should submit a Proposal on limitation of actions of private contractors while keeping in mind the free circulation of the Internet and the possibility of a European Privacy Cloud (EPC).

As it has recently been recognised by the European Commission in the memo entitled "What does the Commission mean by secure Cloud computing services in Europe?",¹²² the EU needs to develop its own capacities in terms of cloud computing, in order to guarantee what we could define as a European Privacy Cloud (EPC). It is clear that the modalities of the **U.S.-E.U. safe harbour agreement**, presented by the USA as a guarantee in terms of privacy have been gravely **violated**. All companies involved in the PRISM scandal (Apple, Google, Yahoo, Facebook, etc.) were members of the safe harbour agreement. The data protection directive regarding the access of private providers who are routing to the US European data via cloud computing **has to be revised**.

A Canadian proposal may be here explored. This proposal elaborates a **"route tracking device"** that proposes to the internet client to choose fast or "secure" routes for sending emails or other communications¹²³. Such a proposal would oblige the companies to propose the option for all European countries internet users to keep their internal communications and data storages in Europe. If the US companies do not propose this option, they would be obliged to warn the visitors on their websites. European companies may be required to do the same and to sign a code of privacy agreement respectful of the European Charter of Human Rights. To ask to the Open sources to find way to organise the equivalent of what is offered by the big 9 companies today is also a possibility.

All users, whatever their nationality, should be equally protected. Internet users should have equal right over the secrecy of their correspondence. Such a right is not contrary to legitimate claims of the different services for their missions concerning crime and national security.

Recommendation 4: The European Parliament should ensure that certain key provisions in the Data Protection draft Regulation be maintained during negotiations with Council

The recent vote in the LIBE Committee of the European Parliament on the General Data Protection Regulation on 21 October 2013 has unveiled some key proposals as regards data transfers to non-EU countries that still need to be confirmed during the negotiations with member states before becoming law. Current Article 43a states that, if a third

¹²⁰ B. Hudson, S. Ugelvik (2012), « Justice and Security in the 21st Century: Risks, Rights and the Rule of Law ». Routledge. 256p.

¹²¹ Read more: <http://www.digitaltrends.com/mobile/why-the-nsa-collects-everyones-phone-records/#ixzz2i3coVI9Y>

¹²² European Commission - MEMO/13/898, 15 October 2013

¹²³ J. Obar and A. Clement (2013), 'Internet surveillance and boomerang routine,' Working Paper, July 2013, University of Toronto.

country asks a firm or organisation to disclose personal data processed in the EU, the firm or organisation needs to get permission from the national data protection authority and inform the person concerned before transferring any data. Failing to comply with this safeguard implies sanctions (current Article 79 of the Regulation): for organisations, written warnings may be issued for less serious breaches, or the organisation might be subjected to a data protection audit; for companies the sanctions might take the form of a fine of up to €100 million or 5% of annual worldwide turnover, whichever is greater. When imposing these penalties, the data protection authorities would have to take into account aggravating factors such as the duration of the breach, its negligent or repetitive character, willingness to cooperate and the amount of damage done. It is crucial that the European Parliament consider such provisions as 'red lines' during the inter-institutional negotiations on the final text of the Regulation.

Recommendation 5: The European Parliament should propose the establishment of a policy infrastructure at EU level capable of ensuring effective follow-up of intelligence revelations

There is a need for the European Parliament to reflect critically about the EU's institutional capacity to deal with recurrent breaches by EU and foreign intelligence agencies which clearly impinge on the rights and freedoms of European citizens. Lessons should be learned from the Echelon affair to ensure that a more systematic and sustainable policy infrastructure is put into place that can ensure genuine follow-up in the wake of intelligence scandals.

Consideration should be given to the possibility of establishing a common model of European cooperation on intelligence exchange and sharing between EU Member States and with third countries, which would be particularly concerned with refusing to cooperate in cases where the information was obtained through unlawful treatment of the individual. The model should also foresee more legal certainty concerning the kind of information that is exchanged, and the parameters for it to be considered as 'intelligence', as well as a common legal definition of 'law enforcement authorities' that would clearly differentiate the roles of intelligence services and other law enforcement (police) authorities. This common model should be closely, carefully and democratically monitored at both the national and European levels. As previous research has proposed,¹²⁴ a 'yellow card, red card system' could be adopted, in which transmission of tainted information in breach of the common accord would first be signalled by a warning (a 'yellow card') and if repeated, by exclusion (a 'red card') from the information-sharing network.

A committee at the European level led by the European Counter Terrorist Coordinator could be set up to address possibilities for applying EU principles in the field of data protection, privacy and collective freedoms and to propose the base for a transatlantic digital bill of rights concerning all data subjects, whatever their nationality. In order to be credible it should gather not only policymakers but also internet providers as well as researchers and civil society representatives.

The participation of national parliaments should be also foreseen, in light of the Brussels Declaration that emphasised the need to create a "European Intelligence Review Agencies Knowledge Network" (EIRAN), with the main goal of improving democratic accountability of the intelligence and security services in Europe. The European Parliament could use the EP's inter-parliamentary arrangement with national parliaments

¹²⁴ F. Geyer (2007), *Fruit of the Poisonous Tree*, op. cit.; S. Carrera et al (2012), *The results of inquiries into the CIA's programme of extraordinary rendition and secret prisons in European states in light of the new legal framework following the Lisbon Treaty*, Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), June 2012.

for sharing information on 'good' and 'bad' practices in the scrutiny of law enforcement authorities and intelligence services and the state of affairs in domestic inquiries.¹²⁵

Recommendation 6: The European Parliament should exercise its powers to promote minimum standards set by ECtHR

The EU and the Council of Europe are not excluded from intervening in matters of national security where they affect the human rights and fundamental freedoms of European citizens and all those affected by their government's security practices.

The European Court of Human Rights has developed a substantial body of jurisprudence on what constitutes interference prescribed by the law in the context of secret surveillance and information gathering which effectively establishes a set of criteria for determining the lawfulness of secret surveillance and interference of communications. The European Parliament should examine these minimum safeguards and reflect on how further value could be given to those standards within the EU legal system in order to ensure that they become an integral part in defining the "red line" that intelligence services in democratic regimes cannot cross when they use large-scale surveillance.

A new study should be conducted to explore in detail the legal implications of ECtHR jurisprudence on intelligence-related activities over the EU's Internal Security Strategy and EU Home Affairs activities. Closer cooperation between the European Parliament and the Council of Europe (and its Parliamentary Assembly, PACE) would be here also welcomed.

Recommendation 7: Ensure more effective scrutiny and monitoring of EU Home Affairs Agencies in the field of security and information exchange

There are no mechanisms in place to ensure that EU home affairs agencies such as Europol (and Intsen in so far as it can be classified an EU 'agency') have not received, processed or used information or intelligence that was illegally obtained by national authorities or third countries.

The forthcoming revision of Europol's mandate should be taken as an opportunity to address the accountability issues raised above. An independent evaluation could also be conducted about the extent to which any EU agencies may have known or received any sort of information relating to large-scale surveillance programmes by the EU member states. To understand the risks of EU Home Affairs agency (indirect) involvement in programmes of communications surveillance, a mapping could be undertaken of the points of intersection of national (intelligence) and law enforcement agencies which may have been involved in large-scale surveillance and the EU intelligence or information exchange architecture. These points of intersection should be subjected to sensitive, democratic, legal and judicial controls.

As a means to ensure democratic accountability and oversight, the EP could establish a special (permanent) inter-parliamentary committee on EU regulatory agencies, with special focus on EU Home Affairs agencies working in the field of security and information exchange for law enforcement purposes. This committee could be run by the European

¹²⁵ See also S. Carrera et al (2012), *The results of inquiries into the CIA's programme of extraordinary rendition and secret prisons in European states in light of the new legal framework following the Lisbon Treaty*, Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), June 2012.

Parliament's LIBE, with the participation of other relevant committees and representatives from corresponding committees of national parliaments. Its mandate include the possibility of setting up 'confidential working groups' that would have access to and could assess the secret/non-publicly disclosed information. It should have the power, resources and expertise to initiate and conduct its own investigations and inquiries, as well as full and unhindered access to the information, officials and installations necessary to fulfil its mandate.

Recommendation 8: EP to explore the potential for an EU level protection for whistle-blowers

It should be considered whether systematic protection for whistle-blowers could be introduced in the EU level legal framework, potentially including strong guarantees of immunity and asylum.

Recommendation 9: Further research should be commissioned by the European Parliament on large-scale surveillance practices by EU member states

The evidence presented in this briefing paper opens a set of new and pressing questions on the activities of European intelligence services and their compatibility with EU law, demonstrating that further research is needed on this area. The European Parliament should commission an in-depth research study to examine the specific features and techniques of large-scale surveillance by EU member states, and their lawfulness under current domestic legal regimes as well as their compatibility with EU legal principles and standards.

List of academic references

- A. Amicelle (2011), *The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and the "SWIFT Affair"*, Research Question 36, CERJ, Sciences-Po.
- H. Becker (1963), *Outsiders: Studies in the Sociology of Deviance*, New York: The Free Press;
- D. Bigo (2006), *Intelligence Services, Police and Democratic Control: The European and Transatlantic Collaboration*, in Bigo D., Tsoukala A., *Controlling Security*, Paris: L'harmattan.
- D. Bigo et al. (2011), *Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament*, Study for the European Parliament's LIBE Committee, November 2011.
- D. Bigo et al (2012), *Fighting cyber crime and protecting privacy in the cloud*, Study for the European Parliament, PE 462.509.
- C. Bowden (2013), *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights*, Study for the European Parliament, PE 474.405, September 2013
- D. Campbell (1999), *The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition*, Part 2/5, in: STOA (Ed.), *Development of Surveillance Technology and Risk of Abuse of Economic Information* (October 1999), PE 168.184.
- S. Carrera et al (2012), *The results of inquiries into the CIA's programme of extraordinary rendition and secret prisons in European states in light of the new legal framework following the Lisbon Treaty*, Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), June 2012.
- A. Dulles (1963), *The Craft of Intelligence*, New York: Harper&Row.
- O. H. Gandy, Jr. (2002), *"Data Mining and Surveillance in the Post-9.11 Environment"*, IAMCR Data Mining, 7 November 2002.
- F. Geyer (2007), *'Fruit of the Poisonous Tree Member States' Indirect Use of Extraordinary Rendition and the EU Counter-Terrorism Strategy*, CEPS Working Document No. 263/April 2007.
- P. Gill (2012), *'Intelligence, Threat, Risk and the Challenge of Oversight'*, *Intelligence and National Security*, 27:2, pp. 206-22.
- E. Guild and S. Carrera (2011), *'Towards an Internal (In)security Strategy for the EU?'* CEPS Liberty and Security Series, January 2011.
- K. Haggerty and R. Ericson, (2000), *The Surveillant Assemblage*, *British Journal of Sociology*, 51(4): p. 605-622.
- S. Heumann, B. Scott (2013), *"Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany"*, Stiftung Neue Verantwortung / Open Technology Institute publication, September 2013.
- B. Hudson, S. Ugelvik (2012), *« Justice and Security in the 21st Century: Risks, Rights and the Rule of Law »*. Routledge. 256p.
- C. Jones (2013), *Secrecy reigns at the EU's Intelligence Analysis Centre*, Statewatch Analysis.
- M. Klamberg, (2010), *'FRA and the European Convention on Human Rights'*, Nordic Yearbook of Law and Information Technology, Bergen 2010, pp. 96-134.

D. Lyon (2003), *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, London: Routledge.

G. T. Marx (1989), *Undercover: Police Surveillance In America*, University Of California Press.

J. Obar and A. Clement (2013), 'Internet surveillance and boomerang routine,' Working Paper, July 2013, University of Toronto.

G. O'Donnell (2004), The Quality of Democracy: Why the Rule of Law Matters? *Journal of Democracy*, Vol. 15, No. 4, October.

D. Omand (2008), Can we have the Pleasure of the Grin without Seeing the Cat? Must the Effectiveness of Secret Agencies Inevitably Fade on Exposure to the Light? *Intelligence and National Security*, Volume 23, Issue 5, pages 593-607, 2008.

J. Parkin (2012), *EU Home Affairs Agencies and the Construction of EU Internal Security*, CEPS Liberty and Security Series, December 2012.

A. Wills, M. Vermeulen, H. Born, M. Scheinin, M. Wiebusch, A. Thornton (2011), *Parliamentary Oversight of Security and Intelligence Agencies in the EU*, Note for the European Parliament, PE 453.207, 15 June 2011.

D. Weller, B. Woodcock (2013) 'Internet Traffic Exchange: Market Developments and Policy Challenges', *OECD Digital Economy Papers*, 207.

ANNEX 1 - The EU member states practices in the context of the revelations of NSA large scale operations

The following Annex draws together the available evidence to shed light on potential programmes of large-scale surveillance being conducted by the intelligence services of EU member states. It seeks to establish whether PRISM-like surveillance programmes exist in the EU: do surveillance programmes run by EU member states share commonalities with those executed by the NSA? How do they compare in terms of scale, technical features and the degree of accountability and oversight characterising their implementation?

The section does not attempt to make a new, comprehensive assessment of the surveillance practices of every EU member state but rather selects for in-depth assessment five countries where existing evidence (via investigative journalism, academic analysis or official documentation) indicates electronic surveillance practices which go beyond traditional, targeted surveillance for intelligence purposes. These are the UK, Sweden, France, Germany and the Netherlands. Each member state is examined with the following criteria in mind: the basic technical features of large-scale surveillance programmes; stated purpose of programmes, targets and types of data collected; actors involved in collection and use, including evidence of cooperation with the private sector; cooperation or exchange of data with foreign intelligence services, including the NSA; legal framework and oversight governing the execution of the programme(s).

1. UK¹²⁶

Of the five member states examined, evidence indicates that the UK government is engaged in by far the most extensive large-scale surveillance activities in the EU.

Internet surveillance in the UK is primarily carried out by the agency known as the Government Communications Headquarters (GCHQ), which produces signals intelligence (SIGINT) for the UK government. GCHQ is mandated to work "in the interests of national security, with particular reference to the defense and foreign policies of Her Majesty's government; in the interests of the economic wellbeing of the United Kingdom; and in support of the prevention and the detection of serious crime".¹²⁷ In budgetary terms GCHQ receives the greatest investment of all the UK's intelligence services (approximately 1 billion pounds annually) and its human resources are twice the size of the workforce of MI5 and MI6 combined (6000 staff).¹²⁸

The disclosures by former Booz Allen Hamilton employee Edward Snowden and revelations in the US and European press, particularly the Guardian newspaper, have provided a much broader understanding of the depth and range of GCHQ's activities than experts previously had access to. These reports describe a range of programmes and projects linked to the large-scale access, processing and storage of data which fall within the overarching framework of a GCHQ project named by the agency 'Mastering the Internet' (MTI).¹²⁹ Reports indicate a budget of over £1 bn devoted to the MTI project

¹²⁶ Data presented here is primarily based on revelations published in press reports, testimonies to the European Parliament Inquiry on electronic surveillance of EU citizens and the expert witness statement of Dr. Ian Brown, Associate Director of Oxford University's Cyber Security Centre.

¹²⁷ Intelligence Services Act (ISA) 1994.

¹²⁸ Source: N. Hopkins, J. Borger and L. Harding (2013), 'GCHQ: inside the top secret world of Britain's biggest spy agency,' *The Guardian*, 2 August 2013. <http://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden>.

¹²⁹ Source: E. MacAskill et al. (2013), 'Mastering the internet: how GCHQ set out to spy on the world wide web,' *The Guardian*, 21 June 2013. <http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet>.

over a three year period,¹³⁰ creating capacities for the intercept, storage and processing of data on a par with, and potentially even exceeding that of, the NSA with whom it engages in close cooperation.

1.1. Programme(s) for large-scale surveillance

Potentially the most far-reaching of the programmes run by GCHQ within the MTI project is the so-called **Tempora Programme**. According to disclosures by the Guardian newspaper, the UK is engaged in the routine interception of undersea cables for the purpose of capturing internet content. Reports allege that GCHQ has placed data interceptors on approximately 200 of the UK-based fibre-optic cables that transmit internet data into and out of the British Isles carrying data to Western Europe from telephone exchanges and internet servers in North America.¹³¹ The Tempora programme is estimated to be around 5 years old, having been first developed and piloted in 2009 and operational since at least early 2012.¹³²

The technique of directly tapping the fibre-optic cables entering and exiting the UK (known as Special Source Exploitation) appears to have given GCHQ access to unprecedented quantities of information. In terms of scale, leaked official documents claim that by 2012 GCHQ was able to process data from at least 46 fibre-optic cables at any one time, giving the agency the possibility to intercept, in principal, more than 21 petabytes of data a day.¹³³ This is estimated to have contributed to a 7000% increase in the amount of personal data available to GCHQ from internet and mobile traffic in the past five years and given the UK the biggest internet access in Five Eyes.¹³⁴ Data is understood to be stored at underground storage centres at GCHQ headquarters in Cheltenham, and potentially other agency sites (GCHQ's sister base in Bude, Cornwall as well as another unnamed base outside of the UK).¹³⁵

The data intercepted and processed consists both of 'content', referring to recordings of phone calls, content of email messages, entries on Facebook, histories of an internet user's access to websites etc, as well as 'metacontent': data recording the means of creation of transmitted data, the time and date of its creation, its creator, location where created.¹³⁶ Content intercepted by Tempora is kept for up to 3 days while metacontent is stored for up to 30 days. Around 300 GCHQ and 250 NSA operative are charged with analysing the data intercepted by Tempora.¹³⁷

¹³⁰ Source: C. Williams (2009), 'Jacqui's secret plan to master the internet,' *The Register*, 3 May 2009. http://www.theregister.co.uk/2009/05/03/gchq_mti/

¹³¹ Source: E. MacAskill et al. (2013), 'GCHQ taps fibre-optic cables for secret access to world's communications', *The Guardian*, 21 June 2013. <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

¹³² Source: Ibid.

¹³³ A petabyte is approximately 1000 terabytes, which is in turn 1000 gigabytes. The comparison made by the Guardian was that this is equivalent to sending all the book in the British Library 192 times every 24 hours.

¹³⁴ Source: P. Beaumont (2013), 'NSA leaks: US and Britain team up on mass surveillance,' *The Observer*, 22 June 2013; N. Hopkins, J. Borger and L. Harding (2013), 'GCHQ: inside the top secret world of Britain's biggest spy agency,' *The Guardian*, 2 August 2013. <http://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden>.

¹³⁵ Source: Statement by Duncan Campbell at the European Parliament's LIBE Committee Inquiry on Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013; N. Hopkins, J. Borger and L. Harding (2013), 'GCHQ: inside the top secret world of Britain's biggest spy agency,' *The Guardian*, 2 August 2013. <http://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden>

¹³⁶ Source: E. MacAskill et al. (2013), 'GCHQ taps fibre-optic cables for secret access to world's communications', *The Guardian*, 21 June 2013. <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>.

¹³⁷ Source: Ibid.

Both content and metacontent are filtered using a technique called Massive Volume Reduction (MVR). Approximately 30% of the data is removed early in the process, classified as 'high volume, low value' traffic (consisting for instance of peer-to-peer music, film and computer programme downloads). The remaining data is searched using so-called 'selectors', which can include keywords, email addresses, and phone numbers of targeted individuals. There are approximately 40,000 such selectors identified by GCHQ.¹³⁸

The objectives underpinning this mass collection of data and the individuals targeted are ambiguous, and as yet not clearly delineated in the documents and reported disclosures. According to an intelligence source quoted by the Guardian, the criteria governing the use of selectors to search and filter the data relate to 'security, terrorism, organised crime and economic well-being'.¹³⁹ An internal GCHQ memo dated October 2011 stated that: "[Our] targets boil down to diplomatic/military/commercial targets/terrorists/organised criminals and e-crime/cyber actors".¹⁴⁰

In principal, the UK legal framework allows Tempora only to target 'external' communications, in other words communications between non-UK residents, or between a UK resident and a non-UK resident. However, in practice, given that a substantial proportion of internal UK communications is routed offshore, all internet users are potential targets of the Tempora programme, both British citizens (and UK residents) as well as non-British citizens and residents. As the UK is an important landing point for the vast majority of transatlantic fibre-optic cables, the monitoring of these cables means that a large proportion of communications from around the world would be intercepted.¹⁴¹

Details concerning the logistical operation of the Tempora programme imply some cooperation with private sector telecommunications companies. On Friday 2 August 2013, the Süddeutsche newspaper published the names of the commercial companies cooperating with GCHQ and providing access to their customer's data within the Tempora programme.¹⁴² The newspaper cited seven companies (BT, Vodafone Cable, Verizon Business, Global Crossing, Level 3, Viatel and Interroute), referred to as 'intercept partners' which together operate a large proportion of the undersea fibre-optic internet cables.¹⁴³ Allegations claim that companies are paid for logistical and technical assistance and are obliged to cooperate under the 1984 Telecommunications Act. Spokespersons of the companies concerned have stated that they are legally obliged to cooperate, and all cooperation is in accordance with European and national laws.¹⁴⁴ Allegations have also

¹³⁸ The NSA has reportedly identified 31,000 selectors. Source: E. MacAskill et al. (2013), 'GCHQ taps fibre-optic cables for secret access to world's communications', *The Guardian*, 21 June 2013. <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>.

¹³⁹ Source: E. MacAskill et al. (2013), 'GCHQ taps fibre-optic cables for secret access to world's communications', *The Guardian*, 21 June 2013. <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

¹⁴⁰ Source: Quoted in E. MacAskill et al. (2013), 'Mastering the internet: how GCHQ set out to spy on the world wide web,' *The Guardian*, 21 June 2013. <http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet>.

¹⁴¹ Expert Witness Statement of Ian Brown for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK Application No: 58170/13 to the European Court of Human Rights.

¹⁴² Source: J. Goetz and F. Obermaier (2013), Snowden enthüllt Namen der spähenden Telekomfirmen, *Süddeutsche Zeitung*, 2 August 2013. The paper's exposé was based on information it had seen on internal GCHQ powerpoint slide from 2009.

¹⁴³ Source: J. Goetz and F. Obermaier (2013), Snowden enthüllt Namen der spähenden Telekomfirmen, *Süddeutsche Zeitung*, 2 August 2013. The paper's exposé was based on information it had seen on internal GCHQ powerpoint slide from 2009.

¹⁴⁴ Source: J. Ball, L. Harding and J. Garside (2013), BT and Vodafone among telecoms companies passing details to GCHQ, *The Guardian*, 2 August 2013.

been made that GCHQ has accessed cables without the consent or knowledge of the companies that own or operate them.¹⁴⁵

The Guardian reports on the Tempora programme have been verified and deemed credible by external experts, such as Ian Brown, member of the UK Information Commissioner's Technology Reference Panel. According to Dr. Brown's witness statement in the application to the European Court of Human Rights *Big Brother Watch and others vs. the United Kingdom*:

The Guardian reports appear to me to be credible. Some of the details have been confirmed by the US government, and by previous leaks (including by statements by former senior NSA officials such as William Binney.) Much of the technology used (such as optical splitter equipment) is commercially available. The budgetary resources required fit within the publicly known budgets of the UK and US intelligence agencies.¹⁴⁶

Another key dimension of GCHQ's large-scale surveillance activity that has emerged from the Guardian's disclosures is the **UK's participation in the PRISM Programme**. Following press revelations concerning the US surveillance activities and programmes operated by the NSA (see Section One of this study), the Guardian reported that the US shares information it obtains via the PRISM programme with the UK authorities. According to reports, GCHQ has had access to the data gathered under the PRISM programme since June 2010 and generated 197 intelligence reports from this data in 2012. It has been subsequently presumed that GCHQ also has access to wider information obtained by NSA surveillance activities under section 1881a, including material that is directly intercepted from so-called 'upstream collection' – the direct interception of communications as they pass through fibre optic cables and electronic infrastructures of telecommunication companies or online service providers in the US (and potentially around the world).¹⁴⁷

Privacy advocacy groups and experts have claimed that through their access to US programmes such as PRISM, the UK is able to obtain information about UK citizens' or residents' internal communications, that would otherwise be out of bounds to UK intelligence agencies without first obtaining a warrant under the Regulation of Investigatory Powers Act 2000 (RIPA). The allegations that this cooperation has effectively allowed the UK authorities to circumvent the UK legal regime have been investigated by the ISC and are further discussed in Section 1.3 below.

Leaked documents have also cited a **decryption programme** named '**Edgehill**'. On 6 September 2013, the Guardian published a report alleging that GCHQ has been cooperating with a 10 year programme by the NSA against encryption technologies.¹⁴⁸ According to documents seen by the Guardian, a GCHQ pilot programme attempted to establish a system which could identify encrypted traffic from its internet cable tapping programmes (e.g. Tempora). Reports indicate that the decryption programme, named 'Edgehill,' was seen as critical in maintaining the strategic advantage that GCHQ has gained with its Tempora Programme, as large internet providers began increasingly to encrypt their communications traffic.

GCHQ documents show that Edgehill's initial aim was to decode the encrypted traffic certified by three major (unnamed) internet companies and 30 types of Virtual Private

¹⁴⁵ Source: Ibid. See also Statement by Duncan Campbell at the European Parliament's LIBE Committee Inquiry on Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013.

¹⁴⁶ Source: Expert Witness Statement of Ian Brown for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK Application No: 58170/13 to the European Court of Human Rights.

¹⁴⁷ Source: Privacy International submission to the Investigatory Powers Tribunal, 'Statement of Grounds', 8 July 2013, available at: www.privacyinternational.org

¹⁴⁸ Source: J. Ball, J. Borger and G. Greenwald (2013), 'Revealed: how US and UK spy agencies defeat internet privacy and security,' *The Guardian*, 6 September 2013.

Network (VPN) – used by businesses to provide secure remote access to their systems. It is reported that by 2015, GCHQ hoped to have cracked the codes used by 15 major internet companies, and 300 VPNs. The Guardian also claims that analysts on the Edgehill project were working on ways into the networks of major webmail providers as part of the decryption project.

Documents leaked by Edward Snowden have also indicated that the UK has engaged in GCHQ-coordinated offensive operations aimed at **diplomatic or economic espionage**. Internal GCHQ powerpoint slides published by the Guardian in June 2013 indicated that GCHQ intercepted the phones and monitored internet use of Foreign politicians and diplomats taking part in two G20 summit meetings in London in 2009.

In September 2013, Der Spiegel published revelations that GCHQ coordinated a project codenamed 'Operation Socialist' which saw a cyber-attack against the Belgian telecoms company Belgacom.¹⁴⁹ During the European Parliament hearing of 3 October, Belgacom vice-President Geert Standaert stated that the 'spyware', discovered in June 2013, had penetrated 124 out of its 26,000 IT systems.¹⁵⁰ Belgacom executives indicated that the scale and sophistication of the attack implied a state actor, but neither conformed nor denied allegations alluding to GCHQ's involvement.¹⁵¹

In addition to the main disclosures relating to GCHQ large-scale surveillance activities discussed above, other programmes about which less is known, have come to light. These include the so-called '**Global Telecoms Exploitation**' programme which is understood to also be conducted through tapping fibre-optic cables and which allows GCHQ to handle 600 million 'telephone events' each day.¹⁵²

Further, documents leaked to the Guardian reveal a "**mobile**" project designed to exploit mobile devices, collecting voice, sms and geo-locations as well as the additional functionalities that come with smartphones, such as emails, internet searches and social media posts. Internal GCHQ documents underscore the importance of this project in order to keep pace with the increase use of smart phones which is likely to see 90% of all internet traffic coming from mobile phones by 2015.

According to the Guardian, it had seen documents which make it clear that "GCHQ was now capable of "attacking" hundreds of apps, and a "mobile capability map" from June last year stated the agency had found ways of looking at the search patterns, emails and conversations on many commonly used phone services."¹⁵³

1.2. Cooperation with foreign intelligence services

Evidence that has come to public attention over the past four months indicates a close working relationship between the NSA and GCHQ on mass cyber surveillance activities.¹⁵⁴

¹⁴⁹ Source: Spiegel online (2013), 'Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm,' Der Spiegel, 20 September 2013.

¹⁵⁰ Source: European Parliament's LIBE Committee Inquiry on Inquiry on Electronic Mass Surveillance of EU Citizens, 3 October 2013.

¹⁵¹ Source: European Parliament's LIBE Committee Inquiry on Inquiry on Electronic Mass Surveillance of EU Citizens, 3 October 2013.

¹⁵² Source: E. MacAskill et al. (2013), 'GCHQ taps fibre-optic cables for secret access to world's communications', *The Guardian*, 21 June 2013. <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>. Also Expert Witness Statement of Ian Brown for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK Application No: 58170/13 to the European Court of Human Rights.

¹⁵³ Source: E. MacAskill et al. (2013), 'Mastering the internet: how GCHQ set out to spy on the world wide web,' *The Guardian*, 21 June 2013. <http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet>.

¹⁵⁴ Source: N. Hopkins and J. Borger (2013), 'Exclusive: NSA pays £100m in secret funding for GCHQ,' *The Guardian*, 1 August 2013. <http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden>.

This concerns both data and intelligence sharing but also in the collaborative development of pilot programmes and technologies. For example, early internal GCHQ documents describing Tempora initially referred to this programme as "a joint GCHQ/NSA research initiative."¹⁵⁵ Reports also allege close cooperation between GCHQ and the NSA in the development of decryption technologies.¹⁵⁶

In terms of data and intelligence sharing, the UK appears to conduct a substantial and routine reciprocal relationship of data exchange with the US authorities. Reflecting the details of the UK's access to PRISM data outlined in Section 2.1.2. above, a UK government paper that set out the views of GCHQ in the wake of the 2010 strategic defence and security review admitted that 60% of the UK's high-value intelligence "is based on either NSA end-product or derived from NSA collection" (end product referring to official reports that are distillations of raw intelligence.)¹⁵⁷

Similarly, the UK is reported to provide access to the data collected through the Tempora and other programmes, available to the NSA, with Guardian reports implying that while the UK had the means to collect huge amounts of data through Tempora and its access to undersea internet cables, the NSA could provide the resources (850,000 operatives) and technologies to process and analyse that data. An internal report explained that "GCHQ and NSA avoid processing the same data twice and proactively seek to converge technical solutions and processing architectures."¹⁵⁸

The degree of cooperation between the two agencies are reflected in revelations exposing the details of the NSA payments to GCHQ in the last years. The Guardian reports that the payments, which are set out in GCHQ's annual "investment portfolios" seen by the newspaper, show that the US government has paid at least £100m to the UK spy agency GCHQ over the last three years. The papers show that the NSA gave GCHQ £22.9m in 2009. The following year the NSA's contribution increased to £39.9m, of which £17.2m was allocated for the agency's Mastering the Internet project. The NSA also paid £15.5m towards redevelopments at GCHQ's sister site in Bude, Cornwall, which intercepts communications from the transatlantic cables that carry internet traffic. In 2011/12 the NSA paid another £34.7m to GCHQ.¹⁵⁹

1.3. Legal framework and oversight

1.3.1. Legal framework

Surveillance of communications in the UK are carried out within the legal framework established by the UK's 2000 Regulation of Investigatory Powers Act (RIPA). The warranting process under RIPA falls under two separate regimes, depending on the types of data accessed. Interception of content is authorised by a warrant signed by the Secretary of State specifying an individual or premises and is valid for 3-6 months.¹⁶⁰ Access to "communications data" is regulated under a separate Chapter of RIPA and

¹⁵⁵ Source: E. MacAskill et al. (2013), 'Mastering the internet: how GCHQ set out to spy on the world wide web,' *The Guardian*, 21 June 2013. <http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet>.

¹⁵⁶ Source: J. Ball, J. Borger and G. Greenwald (2013), 'Revealed: how US and UK spy agencies defeat internet privacy and security,' *The Guardian*, 6 September 2013.

¹⁵⁷ Source: N. Hopkins and J. Borger (2013), 'Exclusive: NSA pays £100m in secret funding for GCHQ,' *The Guardian*, 1 August 2013. <http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden>

¹⁵⁸ Source: Quoted in E. MacAskill et al. (2013), 'Mastering the internet: how GCHQ set out to spy on the world wide web,' *The Guardian*, 21 June 2013. <http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet>.

¹⁵⁹ Source: N. Hopkins and J. Borger (2013), 'Exclusive: NSA pays £100m in secret funding for GCHQ,' *The Guardian*, 1 August 2013. <http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden>.

¹⁶⁰ Part 1, Chapter 1 of RIPA, 2000.

permits some agencies to self-authorise access to some of this data.¹⁶¹ "Communications data" is here defined in relatively vague terms and refers to 'traffic data' that includes identities of individuals and equipment as well as location details, routing information and signaling information.¹⁶²

An interception warrant specifying an individual or premises is not needed where UK authorities intercept communications external to the UK. In this scenario, an authorising certificate from the Secretary of State is required which describes the nature/classification of material to be examined.¹⁶³ It is under the latter legal mechanism by which data exchange with the US, including that implicated in the PRISM programme, as well as Tempora Programme activities are understood to have been authorised.¹⁶⁴

In addition, under the Telecommunication Act 1984 the Secretary of State may give providers of public electronic networks "directions of a general character... in the interests of national security or relations with the government of a country or territory outside the United Kingdom".¹⁶⁵

Although RIPA is stated to be compatible with the ECHR and includes explicit tests of proportionality and necessity before communications content and metadata may be accessed, however, experts have noted that "the standards according to which these tests of proportionality are carried out are mainly secret, and applied by the government's legal advisers and the Secretary of State, with limited oversight."¹⁶⁶

1.3.2. Oversight

The UK's intelligence oversight regime is composed of an Intelligence and Security Committee, an Interception of Communications Commissioner (IoCC) and the Investigatory Powers Tribunal.

On 7 June 2013, the Intelligence and Security Committee (ISC)¹⁶⁷ issued a statement indicating that it had launched an investigation into allegations that the agency circumvented UK law by using the NSA's PRISM programme to access the content of private communications within the UK without proper authorisation. On 17 July 2013 the Chairman of the Intelligence and Security Committee of Parliament, the Rt Hon Sir Malcolm Rifkind MP, issued a follow-up statement regarding the outcome of those investigations.¹⁶⁸ The statement concluded that, after taking detailed evidence from GCHQ, any suggested allegations are 'unfounded' and complied with the legal safeguards

¹⁶¹ Part 1, Chapter 2 of RIPA, 2000. See also Expert Witness Statement of Ian Brown for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK Application No: 58170/13 to the European Court of Human Rights. According to RIPA, communications data can be accessed by a range of government agencies on a broad set of grounds, including in the interests of national security, preventing or detecting crime or disorder, economic wellbeing and so on, and includes any purpose specified in an order made by the Secretary of State. See S.22(2) RIPA.

¹⁶² S. 21 (4) RIPA

¹⁶³ S.8(4) RIPA

¹⁶⁴ Source: Expert Witness Statement of Ian Brown for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK Application No: 58170/13 to the European Court of Human Rights.

¹⁶⁵ S.94 Telecommunication Act.

¹⁶⁶ Source: Expert Witness Statement of Ian Brown for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK Application No: 58170/13 to the European Court of Human Rights.

¹⁶⁷ The Intelligence and Security Committee of Parliament (ISC) is a statutory committee of Parliament that has responsibility for oversight of the UK intelligence community. The Committee was originally established by the Intelligence Services Act 1994. The Committee oversees the intelligence and security activities of the UK, including the policies, expenditure, administration and operations of the Security Service (MI5), the Secret Intelligence Service (MI6) and the Government Communications Headquarters (GCHQ). The Committee consists of nine Members drawn from both Houses of Parliament.

¹⁶⁸ Intelligence and Security Committee of Parliament, Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme, 17 July 2013, available at: <http://isc.independent.gov.uk/news-archive/17july2013>

set out in RIPA. The ISC maintained that "in each case" that it examined, GCHQ had a warrant for interception in accordance with RIPA, although the terms of those warrants have not been published. Experts have concluded from the ISC's public statements, that it was not previously aware of the PRISM Programme. While the ISC concluded that GCHQ has not circumvented the law, it nevertheless acknowledged the need 'to consider further whether the current statutory framework governing access to private communications remains adequate.'

An Investigatory Powers Tribunal, appointed from current or former senior members of the judiciary, also exists to explore complaints covering the eligibility of GCHQ activities under RIPA. Both the UK charity Privacy International and the civil rights group Liberty have submitted claims to the IPT following the revelations of GCHQ's activities in PRISM and Tempora.¹⁶⁹ However, this body has not in the past demonstrated a strong oversight function of GCHQ.¹⁷⁰

¹⁶⁹ Privacy International submission to the Investigatory Powers Tribunal, 'Statement of Grounds', 8 July 2013, available at: www.privacyinternational.org

¹⁷⁰ In 2004 the IPT received dealt with 115 cases in which it found no breach of RIPA or the Human Rights Act 1998. In leaked documents there are implications that GCHQ did not take this oversight mechanism particularly seriously, stating in internal documents leaked to the Guardian newspaper that "so far they have always found in our favour." (Guardian – GCHQ taps fibre optic cables)

2. Sweden¹⁷¹

According to revelations by investigative journalists and experts consulted for the purpose of this study, Sweden is becoming an increasingly important partner of the global intelligence network. Signals intelligence operations in Sweden are the responsibility of the National Defence Radio Establishment (FRA). In recent years, reports have emerged which allege that FRA has engaged in operations and programmes for the mass collection of data, with features that resemble in part those pursued by the US' NSA and the UK's GCHQ.

2.1. Programme(s) for large-scale surveillance

Since five years, there have been reports of FRA accessing data traffic crossing its borders.¹⁷² In 2008 the TV broadcaster SVT reported that the FRA was collecting/receiving data from the Baltic states and forwarding in bulk to the USA, based on the testimony of a FRA whistleblower.¹⁷³ These allegations were recently restated during Duncan Campbell's testimony to the European Parliament Inquiry on Electronic Mass Surveillance of EU Citizens of 5 September 2013, where he alleged that while the Försvarets radioanstalt has been running satellite interception facilities for many years, Sweden's new internet laws passed in 2009 (FRA law) authorised the agency to monitor all cable bound communications traffic into and out of Sweden, including emails, text messages and telephone calls. FRA is now alleged to engage in intercepting and storing communications data from fibre-optic cables crossing Swedish borders from the Baltic sea.¹⁷⁴

The evidence indicates that FRA has been running operations for the 'upstream' collection of private data - collecting both the content of messages as well as metadata of communications crossing Swedish borders. The metadata is retained in bulk and stored in a database known as 'Titan' for a period of 18 months.¹⁷⁵

It is understood that interception of these fibre-optic cables involves a legal obligation on communications service providers to transfer all cable communication crossing Swedish borders to specific "interaction points", where the communications service providers surrender the data to the state.¹⁷⁶

¹⁷¹ The information gathered on the large-scale surveillance practices of Sweden is based primarily on the expert input of Dr. Mark Klamberg, Uppsala University as well as press articles, and official documentation.

¹⁷² Source: N. Nielsen (2013), 'EU asks for answers on UK snooping programme', *EU Observer*, 26 June 2013.

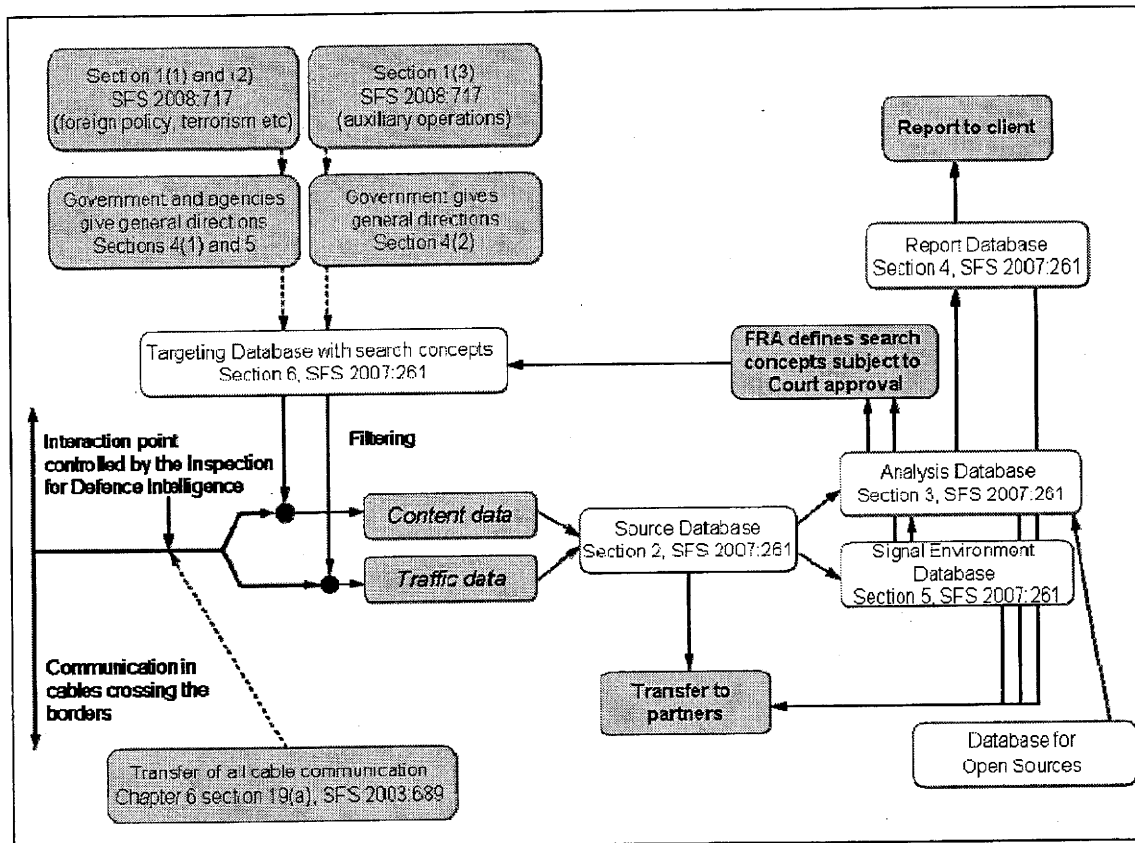
¹⁷³ Source: M. Klamberg, (2010), 'FRA and the European Convention on Human Rights', *Nordic Yearbook of Law and Information Technology*, Bergen 2010, pp. 96-134.

¹⁷⁴ Source: Statement by Duncan Campbell at the European Parliament's LIBE Committee Inquiry on Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013; A. Tomkvist (2013), 'Bildt: surveillance in Sweden "not like Prism"', *The Local*, 13 June 2013.

¹⁷⁵ Source: M. Klamberg, (2010), 'FRA and the European Convention on Human Rights', *Nordic Yearbook of Law and Information Technology*, Bergen 2010, pp. 96-134.

¹⁷⁶ Source: M. Klamberg, (2010), 'FRA and the European Convention on Human Rights', *Nordic Yearbook of Law and Information Technology*, Bergen 2010, pp. 96-134.

Figure 2. Diagram illustrating how the FRA processes communication and information



Source: M. Nilsson, M. Klamberg and A. Petersson, 2008.

Concerning the profile of individuals targeted by the FRA's mass data interception programme, the initial targets again appear to be indiscriminate. As in the UK, the bulk retention of data is, under the Swedish legal regime, only meant to cover communications entering or exiting Swedish borders and not internal communications. However, internal communications that have been routed through nodes based outside Swedish territory are likely to also be classed as 'foreign' communications and retained for analysis. The Swedish legislative framework regulating the collection of signals intelligence provides that if there is uncertainty whether data is foreign or domestic, the data may be collected and retained.¹⁷⁷

Final (processed) intelligence, described as "reports to clients" is discriminate and does not include citizens in general. The legislation differentiates between 'defence intelligence operations' and 'auxiliary operations.' Defence intelligence operations concern a relatively small faction of the communications that is deemed to directly relate to external military threats, international terrorism and similar phenomena. The content of such communications associated to such threats is selected and reserved for detailed analysis. By contrast, the 'auxiliary operations' - which make up the lion's share of communications intercepted, is analysed as metadata, not content, and are not intended for generating intelligence reports to FRA's clients.¹⁷⁸

However, academic experts argue that the division between these modes of processing these two kinds of data is not clear-cut. Dr. Klamberg states that this division:

¹⁷⁷ Section 2(a) of the Act 2008:717 on signals intelligence.

¹⁷⁸ Prop. (Government Bill) 2006/07:63, En anpassad försvarsunderrättelseverksamhet (Adapted Defence Intelligence Operations): <http://www.regeringen.se/content/1/c6/07/83/67/2ee1ba0a.pdf>

"...creates the impression that a wall has been erected where the large amounts of traffic data [metadata] collected through the auxiliary operations is used purely for some abstract technical matters and not for intelligence purposes. This is a misconception."¹⁷⁹

This misconception is due to the fact that the preparatory works for the Swedish law on signals intelligence state that since the auxiliary operations "aim to facilitate the defence intelligence operations it would not be incompatible with the purpose for which the data is collected that the data is also used to some extent in the defence intelligence operations."¹⁸⁰

Second, the preparatory works explain that reports to clients may involve extensive descriptions of meta-data patterns and therefore, despite being intended for auxiliary operations, may also be used for defence intelligence purposes.¹⁸¹

While there is no explicit statement as to which national entities receive the data or resulting intelligence drawn from this programme, to the Swedish legislative framework, data collected by the FRA may be shared with the following 'customers':¹⁸²

- 1) the Government offices (Regeringskansliet),
- 2) National Police Board (Rikspolisstyrelsen - RPS) which includes the National Bureau of Investigation and the Secret Service,
- 3) the Swedish Agency for Non-Proliferation and Export Controls (Inspektionen för strategiska produkter - ISP),
- 4) the Defence forces (Försvarmakten),
- 5) Swedish Defence Materiel Administration (Försvarets materielverk - FMV),
- 6) Swedish Defence Research Agency (Totalförsvarets forskningsinstitut - FOI),
- 7) Swedish Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap - MSB)
- 8) Swedish Customs (Tullverket)

2.2. Cooperation with foreign intelligence services

There is evidence that FRA may be sharing substantial quantities of the data it collects with foreign intelligence services including the NSA. The Swedish legislation allows for the bulk transfer of data to other states if authorised by the Government.¹⁸³ Reports from media, experts as well as government statements indicate that Swedish authorities have made use of this possibility through exchanges of large amounts of raw data with the US as well as the Baltic states.¹⁸⁴

Duncan Campbell, during his testimony to the European Parliament hearing on 5 September 2013 stated that Sweden's FRA has become a new and important partner of Five Eyes, by providing major satellite and undersea cable interception arrangements, stating that FRA "is deemed, according to the documents, to be the biggest collaborating

¹⁷⁹ Source: Expert input by Dr. Mark Klamberg, Uppsala University. See also M. Klamberg, (2010), 'FRA and the European Convention on Human Rights', *Nordic Yearbook of Law and Information Technology*, Bergen 2010, pp. 96-134.

¹⁸⁰ Source: Prop. (Government Bill) 2006/07:46, Personuppgiftsbehandling hos Försvarmakten och Försvarets radioanstalt (Processing of Personal Data by the Armed Forces and the National Defence Radio Establishment):

<http://www.regeringen.se/content/1/c6/07/73/05/7ac2933f.pdf>

¹⁸¹ Source: SOU (Swedish Government Official Reports) 2009:66, Signalspaning för polisiära behov (Signal Intelligence for Law Enforcement Purposes):

<http://www.regeringen.se/content/1/c6/12/99/11/e20e1ef6.pdf>

¹⁸² Section 9 Förordning (2007:261) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet (Decree 2007:261 on processing of personal data by the FRA)

¹⁸³ Section 9 Act 2008:717 on signals intelligence.

¹⁸⁴ NyTeknik, FRA:s metoder granskas efter ny avlyssningsskandal, 27 August 2008. Cited in M. Klamberg, (2010), 'FRA and the European Convention on Human Rights', *Nordic Yearbook of Law and Information Technology*, Bergen 2010, pp. 96-134.

partner of GCHQ outside the English speaking countries." Code-named 'Sardine', he highlighted that Sweden makes an important contribution to the UK-USA Five Eyes organisation, having access to cables that were hitherto inaccessible (those from the Baltic states and Russia).

In a statement following the revelations by Campbell, Defence Minister Karin Enstrom said Sweden's intelligence exchange with other countries is "critical for our security" and that "intelligence operations occur within a framework with clear legislation, strict controls, and under parliamentary oversight."¹⁸⁵ Likewise a FRA spokesperson has acknowledged that the FRA shares data with other countries, but declined to specify which countries or to provide further details of the types of data shared.¹⁸⁶ Similarly, there is no indication of whether Sweden has been the recipient of data from other states, including data from the NSA's PRISM and other mass surveillance programmes.

2.3. Legal framework and oversight

2.3.1. Legal framework

The legal authorisation for Sweden signals intelligence gathering operations are issued by an intelligence court (Underrättelsesdomstolen - UNDOM). However, according to the legislative framework governing the issuing of warrants – namely Act 2008:717 on signals intelligence within defence intelligence operations, Act 2009:966 on the Intelligence Court, and Decree 2009:968 with instructions for the Intelligence court - warrants can be sweeping and are not limited to a specific individual.¹⁸⁷

2.3.2. Oversight

The surveillance activities of the FRA are monitored by a national oversight body, the Inspection for Defence Intelligence Operations (Statens inspektion för försvarsunderrättelseverksamheten – SIUN) which is composed of representatives from the Government and Opposition parties.¹⁸⁸

However, academic experts have critiqued the weak system of checks and balances when it comes to Swedish collection of signals intelligence. With regard to the UNDOM and the SIUN, Dr. Mark Klamberg contends that:

All of these institutions are under very tight control of the Government, an entity that can issue requests for signals intelligence operations. The intelligence court has one chief judge, one or two deputy chief judges. The judges are appointed by the Government. One of the three nominees for the next chief judge is currently the chief legal advisor at the Ministry of Defence. The current head of the signals intelligence agency was previously the chief legal advisor at the Ministry of Defence when the legislation was drafted. The members of SIUN do represent different political parties but are appointed by the Government and report to the Government. Most of the

¹⁸⁵ Source: Quoted in D. Landes (2013), 'Sweden's Spy Links 'deeply troubling'', *The Local*, 6 September 2013.

¹⁸⁶ Source: N. Nielsen (2013), 'EU asks for answers on UK snooping programme', *EU Observer*, 26 June 2013.

¹⁸⁷ Expert input by Dr. Mark Klamberg, Uppsala University. See Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet (Act 2008:717 on signals intelligence within defence intelligence operations), section 4(a); Lag (2009:966) om Försvarsunderrättelsesdomstol (Act 2009:966 on Intelligence court); Förordning (2009:968) med instruktion för Försvarsunderrättelsesdomstolen (Decree 2009:968) with instructions for the Intelligence court). For further information on the Swedish legal framework covering communications surveillance, see M. Klamberg, (2010), 'FRA and the European Convention on Human Rights', *Nordic Yearbook of Law and Information Technology*, Bergen 2010, pp. 96-134.

¹⁸⁸ Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet (Act 2008:717 on signals intelligence within defence intelligence operations), Sections 10 and (10(a)); Förordning (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten (Decree 2009:969 with instructions for the Inspection for Defence Intelligence Operations).

members of SIUN are former parliamentarians, which weakens the parliamentary oversight in comparison to a system where the responsibility for oversight is conducted by a committee of parliament, i.e. parliamentarians in office. All in all, the Swedish system of checks and balances is weak when it comes to signals intelligence.¹⁸⁹

¹⁸⁹ Source: M. Klamberg (2013), Blogpost on EU Metadata Collection, Lawfare, 29 September 2013, at: <http://www.lawfareblog.com/2013/09/mark-klamberg-on-eu-metadata-collection/>

3. France¹⁹⁰

Since 2008 France has been constantly improving its architecture for the large-scale collection of data, with the main intelligence agency in France, the DGSE (Direction générale de la sécurité extérieure) increasing its foreign intelligence capabilities in recent years.¹⁹¹ A report of 30 April 2013 by the French National Assembly highlighted the fact that:

Since 2008, progress has been made in terms of pooling of capabilities, in particular concerning electro-magnetic intelligence activities operated by the DGSE to benefit the entire intelligence community.¹⁹²

In this report, the French MPs also suggested strengthening the data collection structure of the DGSE and the links between all levels of intelligence.¹⁹³

Experts consulted for this study claim that France now ranks fifth in the world of metadata collection after the USA, Great Britain, Israel and China and runs the second most important intelligence data collection and processing centre in Europe after the UK. Claims of this nature have been made publicly by Bernard Barbier, a Technical Director at the DGSE, in 2010.¹⁹⁴

3.1. Programme(s) for large-scale surveillance

Reportedly, France's communications surveillance and collection architecture rests primarily on a supercomputer operated by the DGSE in Paris.¹⁹⁵ This super computer intelligence centre, allegedly installed on three levels in the basement of the DGSE headquarters, is reported to be capable of collecting, processing and storing dozens of petabytes of data. Data is intercepted and collected by approximately twenty interception sites located on both national and overseas territory, comprised of both satellite stations and interception of fibre-optic submarine cables.¹⁹⁶

In February and March 2013 the French National Assembly's Committee on National Defence and Armed Forces conducted hearings during which the heads of the main French intelligence services all confirmed the existence of a metadata intelligence centre located at the DGSE capable of intercepting and processing internet flows, social network and phone communications.¹⁹⁷ For instance, on 20 February 2013, the then Head of the

¹⁹⁰ The data presented here was gathered on the basis of news articles and official documents and complemented by an interview with an expert academic source who wishes to remain anonymous.

¹⁹¹ Source: Assemblée Nationale (2013), Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2012, Rapport n° 1012 par Mme Patricia ADAM, Députée, Délégation parlementaire au renseignement, 30 April 2013, available at: www.assemblee-nationale.fr/14/rap-off/i1012.asp

¹⁹² Assemblée Nationale (2013), Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2012, Rapport n° 1012 par Mme Patricia ADAM, Députée, Délégation parlementaire au renseignement, 30 April 2013, available at: www.assemblee-nationale.fr/14/rap-off/i1012.asp (the original text states « depuis 2008, des progrès ont été réalisés en matière de mutualisation des capacités, notamment en ce qui concerne le renseignement d'origine électromagnétique, opéré par la DGSE au profit de l'ensemble de la communauté du renseignement. »)

¹⁹³ Ibid., pt. II.

¹⁹⁴ Source: Speech by Bernard Barbier on 30 September 2010 at the French Association of Reservists for Ciphering and Information Security. His remarks were reported in the following specialised blog article: <http://bugbrother.blog.lemonde.fr/2010/10/02/frenchelon-la-dgse-est-en-1ere-division>

¹⁹⁵ Source: J. Follorou and F. Johannes (2013), 'Révélations sur le Big Brother français,' *Le Monde*, 4 July 2013.

¹⁹⁶ Source: J. Follorou and F. Johannes (2013), 'Révélations sur le Big Brother français,' *Le Monde*, 4 July 2013.

¹⁹⁷ See Assemblée Nationale (2013), Commission de la défense nationale et des forces armées, Comptes-rendus n° 52, 54, 55, 56, 59 et 62 des réunions du 12 février, 13 février, 19 février, 20 février, 26 février et 13 mars 2013 respectivement, available on the following website: www.assemblee-nationale.fr/14/cr-cdef/12-13/index.asp

DGSE, Érarid Corbin de Mangoux, alluded to France's communications surveillance capabilities when he stated before the Committee that:

Regarding the technical means, we have at our disposal the entire capabilities for electro-magnetic intelligence. Following the recommendations of the 2008 White Paper, we have developed an important apparatus for intercepting Internet flows.¹⁹⁸

Data storage appears to relate primarily to metadata from phone and internet use. Concerning the use of this information, evidence indicates that the 'metadata centre operated by DGSE forms an 'intelligence platform' which feeds a range of intelligence, defence and law enforcement bodies within France. The following six agencies have been cited as 'customers' of the DGSE metadata bank (named "mutualisation infrastructure" by French officials):¹⁹⁹

- National Directorate of Customs Intelligence and Investigations (DNRED), responsible for carrying out investigations on smuggling, counterfeit money and customs fraud;
- Directorate for Defence Protection and Security (DPSD), responsible for military counter-espionage;
- Directorate of Military Intelligence (DRM), tasked with centralising all military intelligence information;
- Central Directorate of Interior Intelligence (DCRI), soon to be replaced by the General Direction of Interior Security (DGSI), responsible for counter-espionage and counter-terrorism;
- TRACFIN service (Intelligence Analysis and Action against Clandestine Financial Circuits), responsible for the fight against illegal financial operations, money laundering and terrorism financing.
- The intelligence arm of the Police Prefecture of Paris

According to reports from *Le Monde* newspaper, these services send a request to the DGSE and the DGSE searches the database on a hit/no-hit basis. They then forward intelligence reports on the basis of the data analysed to the client agencies.²⁰⁰ This is allegedly carried out routinely, discreetly and without any form of parliamentary control.²⁰¹ According to a French Senate report, this logic of "mutualisation" is a longstanding one:

...the logic of pooling of resources between services has been continued for several years. Therefore, the DGSE is specialised in communication interception and cryptography to the benefit of the entire intelligence community. The Directorate of Military Intelligence (DRM) is in charge of the observation satellites and radar signal surveillance. Approximately 80% of the annual budget of the DGSE is invested in projects linked to the other intelligence agencies.²⁰²

¹⁹⁸ Source: Hearing of Érarid Corbin de Mangoux, Director-General of the DGSE, on 20 February 2013, before the French National Assembly's Committee on National Defence and Armed Forces. See *Assemblée Nationale* (2013), *Commission de la défense nationale et des forces armées, Compte-rendu n° 56*, available on www.assemblee-nationale.fr/14/cr-cdef/12-13/c1213056.asp. The original text states: « S'agissant des moyens techniques, nous disposons de l'ensemble des capacités de renseignement d'origine électromagnétique (ROEM). À la suite des préconisations du Livre blanc de 2008, nous avons pu développer un important dispositif d'interception des flux Internet. »

¹⁹⁹ Source: J. Follorou and F. Johannes (2013), 'Révélations sur le Big Brother français,' *Le Monde*, 4 July 2013.

²⁰⁰ Source: J. Follorou and F. Johannes (2013), 'Révélations sur le Big Brother français,' *Le Monde*, 4 July 2013.

²⁰¹ Source: Input by anonymous expert.

²⁰² See *Sénat* (2013), *Projet de loi de finances pour 2013 - Défense : environnement et prospective de la politique de défense, Avis n° 150 (2012-2013) de MM. Jeanny LORGEUX et André TRILLARD*, 22 November 2012, paragraph III a) 1) d) available at: www.senat.fr/rap/a12-150-5/a12-150-5.html (original text: « Cet effort s'effectue dans la logique de mutualisation des moyens entre services retenue depuis plusieurs années. Ainsi, la DGSE est spécialisée sur l'interception des communications et la cryptologie, au bénéfice de l'ensemble de la communauté du renseignement. La direction du renseignement militaire (DRM) met en oeuvre quant à elle les satellites d'observation et les moyens

There are currently no confirmed reports or evidence that agreements exist between the French intelligence services and French telecommunications operators such as SFR, Bouygues, Orange etc. exist giving access to data traffic.²⁰³

3.2. Cooperation with foreign intelligence services

The French intelligence services engage in wide cooperation with foreign intelligence services. During the above-mentioned hearing, Head of DGSE Énard Corbin de Mangoux declared before the French Parliament that the Agency was working with more than 200 foreign services, among which 50 formed part of the "second circle" engaged in 'frequent' collaboration, while 10 were considered part of a "first circle" engaged in intense cooperation. The states with which the DGSE engages were not named, nor the nature of the cooperation detailed beyond a reference to joint analysis of information and research.²⁰⁴ He added that, on the initiative of the USA, western intelligence services have set up a database allowing each nation to immediately get access to all the information gathered.²⁰⁵

These statements supplement revelations from 2005 that, according to disclosures by the Washington Post, France has been hosting a secret intelligence centre in Paris named "Alliance Base" where six countries, namely USA, UK, France, Germany, Canada and Australia routinely exchange information.²⁰⁶ It was reported that Alliance Base is headed by a French general assigned to the DGSE and hosts case officers from Britain, France, Germany, Canada, Australia and the United States. Alliance base is believed to have ended in 2009 due to tensions between the French and the US.²⁰⁷

3.3. Legal framework and oversight

3.3.1. Legal framework

Electronic surveillance is regulated by the Code de la Sécurité Intérieure, a legislative code established in 2012 and regrouping various laws and rules related to French internal security.²⁰⁸ The specific rules on "security intercepts" (interceptions de sécurité) can be found in Book 2, Title IV of this Code. They strictly regulate security intercepts authorised by the Prime Minister on the advice of the National Advisory Commission on security intercepts (CNCIS), an independent administrative authority reviewing surveillance requests. The Code de la Sécurité Intérieure abrogated a 1991 law on secrecy of correspondence²⁰⁹ which had, until 2012, regulated the conditions for wiretaps (which required permission of an investigative judge). The new Code was strongly criticised by the CNCIS in its activity report²¹⁰ for including security intercepts in a broader and

d'écoute des signaux radar. Environ 80 % du budget annuel d'investissement de la direction technique de la DGSE financent des projets intéressant également d'autres organismes. »)

²⁰³ Source: Statement by Jacques Follorou at the European Parliament's LIBE Committee Inquiry on Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013.

²⁰⁴ Source: Assemblée Nationale (2013), Compte-rendu no. 56, op. cit.

²⁰⁵ Ibid. The original statement was « Ainsi à l'initiative des Américains, les services occidentaux ont mis en place une base de données permettant à chacun de disposer immédiatement de l'ensemble des informations recueillies »

²⁰⁶ Source: D. Priest (2013), 'Help From France Key In Covert Operations', Washington Post, 3 July 2005.

²⁰⁷ Source: D. Servenay (2010), 'Terrorisme: pourquoi Alliance Base a fermé à Paris', Rue89, 24 May 2010, available at: <http://www.rue89.com/2010/05/24/terrorisme-fermeture-dalliance-base-a-paris-152349>

²⁰⁸ Available (in French) at: <http://bit.ly/1dimLYp>

²⁰⁹ Loi no 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.

²¹⁰ See Commission nationale de contrôle des interceptions de sécurité (2012), 20e rapport d'activité 2011-2012, Paris.

vaguer package of rules along with, for instance, "security in public transportation" or "security guards in buildings". The report underlined the fact that any exception to the right to secrecy of correspondence should be provided for in a specific law and not in a code.²¹¹

In addition, a new Anti-Terror Act enacted on 23 January 2006²¹² granted increased powers to the police and intelligence services, allowing them to get telecom data directly from ISPs and extended telecom data retention possibilities.

The law strictly regulates security intercepts authorised by the Prime Minister on the advice of the National Advisory Commission on security intercepts (CNCIS). However, there is a gap in the legal framework regarding the large-scale interception and storage of data, leaving a degree of legal uncertainty which intelligence services appear to have exploited. Hence a senior member of the intelligence services interviewed by *Le Monde* journalists is reported to have claimed that collection of meta-data by DGSE is not illegal but 'alegal' - conducted 'outside the law'.²¹³ This was however contrasted by the CNIL, the independent body which stated that:

Le régime juridique des interceptions de sécurité interdit la mise en œuvre par les services de renseignement, d'une procédure telle que Prism. Chaque demande de réquisition de données ou d'interception est ciblée et ne peut pas être réalisée de manière massive, aussi quantitativement que temporellement. De telles pratiques ne seraient donc pas fondées légalement.²¹⁴

3.3.2. Oversight

Parliamentary oversight over communications surveillance in France is deemed to be relatively weak.²¹⁵ First, because all requests for classified documents from parliamentary committees to intelligence services are rejected since all data transmitted by a foreign service remain property of the service to which the data have been directed. A senator or representative has no right to hear or question a member of a defined intelligence service. The directors of intelligence agencies can only be subjected to official hearings.²¹⁶

The main body responsible for the oversight of interception surveillance in France is the CNCIS (Commission nationale pour les interceptions de sécurité).²¹⁷ The CNCIS is mandated to exert an a priori control on security interceptions (wiretapping) and to assess whether the purpose of the interception meets principles of proportionality etc. However, its reach is judged to be substantially constrained by its limited personnel (only five members),²¹⁸ budget and administrative capacity.²¹⁹ Moreover it is doubtful that it

²¹¹ *Ibid.*, p. 38: "S'agissant de dispositions portant sur la protection des libertés publiques, il résulte des travaux parlementaires ayant conduit à l'adoption, tant de la loi n° 91-646 du 10 juillet 1991 que de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme, que la consécration législative du secret des correspondances électroniques privées, ainsi que les exceptions à ce principe, doivent être prévues par une loi spéciale, comme pour toute liberté publique. Or ces dispositions se retrouvent désormais fondues dans un vaste ensemble normatif couvrant des domaines multiples et variés."

²¹² Loi No. 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

²¹³ Source: J. Follorou and F. Johannes (2013), 'Révélation sur le Big Brother français,' *Le Monde*, 4 July 2013; See also testimony of Jacques Follorou, EP Hearing 5 September 2013.

²¹⁴ Source: J. Follorou and F. Johannes (2013), 'Révélation sur le Big Brother français,' *Le Monde*, 4 July 2013.

²¹⁵ A. Wills et al. (2011), *Parliamentary oversight of security and intelligence agencies in the European Union*, Study for LIBE Committee of the European Parliament.

²¹⁶ Source: input of anonymous expert.

²¹⁷ CNCIS was established by the law of 10 July 1991 on secrecy of correspondence via electronic communication.

²¹⁸ Composed of both Parliamentarians and judges.

²¹⁹ A. Wills et al. (2011), *Parliamentary oversight of security and intelligence agencies in the European Union*, Study for LIBE Committee of the European Parliament; Statement by Jacques Follorou at the

has been routinely consulted (if at all) during the DGSE's metadata collection activities.²²⁰

It is relevant here to note that two French human rights NGOs are attempting to launch an official judicial investigation into the surveillance scandals in France. The Paris prosecutor's office has opened a preliminary inquiry following the submission of a joint complaint by the NGOs Fédération internationale des droits de l'homme (FIDH) and Ligue des droits de l'homme (LDH) on 11 July 2013.²²¹ Both NGOs claim that infringements of personal liberties have taken place through automated data processing. On the basis of the French Criminal Code, they challenge the fraudulent access to an automated data processing system, collection of personal data by fraudulent means, wilful violation of the intimacy of the private life and the use and conservation of recordings and documents obtained through such means.

European Parliament's LIBE Committee Inquiry on Inquiry on Electronic Mass Surveillance of EU Citizens, 1st Hearing, 5 September 2013; CNCIS (2012), *CNCIS: 20^e rapport d'activité 2011 – 2012*, available at: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/134000156/0000.pdf>.

²²⁰ Source: input of anonymous expert.

²²¹ See C. Labbe and N. Vinocur (2013), "French prosecutor investigates U.S. Prism spying scheme", Reuters, 28 August 2013, available at: www.reuters.com/article/2013/08/28/us-usa-security-france-idUSBRE97R0WE20130828. See also the official complaint on the website of the FIDH: www.fidh.org/en/europe/France,568/fidh-and-ldh-file-a-complaint-for-infringement-of-personal-data-13648

4. Germany²²²

Evidence gathered on the surveillance activities of the German intelligence services also indicate that Germany has been engaging in large-scale surveillance of communications data, and that these activities are linked to a network of exchange and transfer of data with both domestic intelligence and law enforcement agencies as well as with international partners, despite the existence of a strong constitutional and legal framework for the protection of privacy.

4.1. Programme(s) for large-scale surveillance

At the centre of the allegations concerning German large-scale surveillance activities is the **Bundesnachrichtendienst** (BND) or Federal Intelligence Service which is responsible for conducting foreign intelligence analysis and electronic surveillance of 'threats to German interests' from abroad. It employs approximately 6,500 persons and had a budget of 504.8 Million EUR for the year 2012.²²³ However, also implicated are the **Militärischen Abschirmdienst** (MAD) the Military Counterintelligence Service²²⁴ and the **Bundesamt für Verfassungsschutz** (BfV) the Federal Office for the Protection of the Constitution which is tasked with "*intelligence-gathering on threats concerning the democratic order, the existence and security of the federation or one of its states, and the peaceful coexistence of peoples; with counter-intelligence; and with protective security and counter-sabotage*". The latter is under the responsibility of the Ministry of Interior and specific regional offices exist in all 16 Länder. The BfV employed 2,757 persons and had a budget of 210 Million EUR in 2012.²²⁵

According to the information available to the public, the BND operates a service capable of **directly connecting to digital traffic nodes** through which most of the foreign communications flow.²²⁶ This is legally authorised by the G-10 Law (see below) which allows the three intelligence agencies mentioned above (the BND, the MAD and the BfV) to search up to 20% of communications having a foreign element according to certain keywords for specific purposes such as the fight against terrorism or the protection of the Constitution.²²⁷

In terms of data flows, the biggest node in Germany – and, according to certain figures, in the world – is the DE-CIX (German Commercial Internet Exchange) in Frankfurt.²²⁸ According to the Spiegel newspaper, the BND has set up special offices at this location to divert incoming traffic, copy the data and analyse it later in the BND headquarters in

²²² Data presented in this section has been gathered primarily on the basis of press reports and official documentation (e.g. Parliamentary questions, reference to official legal texts and case law).

²²³ The number of employees for the BND is mentioned on the BND's website: www.bnd.bund.de/DE/Karriere/Allgemeine%20Informationen/Allgemeine%20Informationen_node.html, the budget of the BND can be found in the Official federal budget for 2012, Section 04, available at www.bundesfinanzministerium.de/bundeshaushalt2012/pdf/epl04.pdf, p.21.

²²⁴ German Ministry of Interior (2013) Verfassungsschutzbericht 2012, BMI 13006, p. 13, available at <http://www.verfassungsschutz.de/embed/vsbericht-2012.pdf>

²²⁵ *Ibidem*.

²²⁶ Source: P. Beuth (2013) 'Wie der BND das Netz überwacht', Zeit Online, 18 June 2013, available at www.zeit.de/digital/datenschutz/2013-06/internet-ueberwachung-bnd

²²⁷ The G-10 Law, in its § 10(4), states "In den Fällen der §§ 5 und 8 sind die Suchbegriffe in der Anordnung zu benennen. Ferner sind das Gebiet, über das Informationen gesammelt werden sollen, und die Übertragungswege, die der Beschränkung unterliegen, zu bezeichnen. Weiterhin ist festzulegen, welcher Anteil der auf diesen Übertragungswegen zur Verfügung stehenden Übertragungskapazität überwacht werden darf. In den Fällen des § 5 darf dieser Anteil höchstens 20 vom Hundert betragen." (www.gesetze-im-internet.de/g10_2001/BJNR125410001.html)

²²⁸ Weller, D., Woodcock, B. (2013) 'Internet Traffic Exchange: Market Developments and Policy Challenges'. *OECD Digital Economy Papers*, 207, p. 41.

Pullach, Bavaria.²²⁹ This was confirmed by a reply to a parliamentary question by the government,²³⁰ as well as by Germany's Justice Minister Sabine Leutheusser-Schnarrenberger and by the head of the G-10 Committee Hans De With.²³¹ The gathered data is then analysed through the use of keywords and selectors on terrorism.²³²

According to the Spiegel,

Via this hub, the largest in Europe, e-mails, phone calls, Skype conversations and text messages flow from *regions that interest the BND like Russia and Eastern Europe*, along with crisis areas like *Somalia*, countries in the *Middle East*, and states like *Pakistan and Afghanistan*.²³³ (Emphasis added)

The same article mentions that the head of the BND, Gerhard Schindler, recently requested an increase in the BND's budget of 100 Million euros for the next five years in order to hire new agents and improve the technological surveillance capabilities. This modernisation project has been given the name of "Technikaufwuchsprogramm" (which can be translated into "Technological Coming-of-age Programme").²³⁴ Several sources of information hint at a possible German system collecting data through private companies, similar to the US PRISM programme. Private companies such as Internet service providers allegedly copy the data requested by the BND on its special servers. The hardware and software architecture used in that case could be the so-called "SINA-Box" which is a means of transferring sensitive data in unsecure environments.²³⁵

It is also worth mentioning that the Federal Police has set up a computerised architecture called 'INPOL-neu' which contains millions of data extracted from police and judicial investigations and from the SIS database. Intelligence services have complete access to the INPOL database, which is also linked to the Europol Information System (EIS).

As seen in the French case, there is considerable pooling of resources/data exchange between the various German intelligence and law enforcement bodies. Since 2001 the three intelligence services have been authorised to extend their domain of investigation in terms of information collection, analysis and dissemination and may exchange information between themselves as well as with police agencies, something which was once regulated and restricted by federal laws.

In particular, the **MAD** has been allowed to collect information on the national borders and exchange information with the two other intelligence services, which has broken the long established German tradition of complete separation between a military intelligence service and its civilian counterparts.

Concerning police-intelligence cooperation, it is interesting to note that the **BfV** has implemented a common database on Islamic terrorism with the **Federal Criminal Police Office (Bundeskriminalamt, BKA)**, a first tool bridging the historical gap between federal police and secret service. A recent bill also extended the powers of the BKA to secretly gather data on private computers through the use of highly specialised software

²²⁹ Source: Spiegel Online (2013) '100-Millionen-Programm: BND will Internet-Überwachung massiv ausweiten', 16 June 2013, available at www.spiegel.de/politik/deutschland/internet-ueberwachung-bnd-will-100-millionen-investieren-a-905938.html

²³⁰ German Parliament (2012) Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Jan van Aken, weiterer Abgeordneter und der Fraktion DIE LINKE - „Strategische Fernmeldeaufklärung" durch Geheimdienste des Bundes, Drucksache 17/9640, available at <http://dip21.bundestag.de/dip21/btd/17/096/1709640.pdf>

²³¹ See M. Ermert (2013), "PRISM scandal: internet exchange points as targets for surveillance", H-Online, 2 July 2013, available at www.h-online.com/security/news/item/PRISM-scandal-internet-exchange-points-as-targets-for-surveillance-1909989.html

²³² Source: Spiegel Online (2013) 'The German Prism: Berlin Wants to Spy Too', 17 June 2013, available at www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129-2.html

²³³ Ibid.

²³⁴ Ibid.

²³⁵ Source: P. Beuth (2013) 'Wie der BND das Netz überwacht', *op. cit.*

(so called "Bundestrojaner" or Federal Trojan Horses) for the purposes of criminal investigations.²³⁶ It is also worth noting the existence of integrated police services that have been set up at federal level to boost data exchange and analysis at all levels, such as the **GTAZ (Gemeinsames Terrorismusabwehrzentrum)**. The GTAZ, located in Berlin, is aiming at strengthening national cooperation between Länder and State, ie between regional and federal police forces, the military, the customs, intelligence services, financial services, and at fostering international cooperation against Islamic terrorism.

4.2. Cooperation with foreign intelligence services

Reports publishing the Snowden revelations concerning German surveillance programmes such as the Spiegel, also highlighted evidence regarding cooperation between the German intelligence services and their US counterparts.

Allegedly, millions of metadata collected by the BND were transferred to the NSA via data collection sites on German territory:

The Snowden documents mention two data collection sites known as signals intelligence activity designators (SIGADs), through which the controversial US intelligence agency gathered about 500 million pieces of metadata in December 2012 *alone*. The code names cited in the documents are "US-987LA" and "US-987LB." The BND now believes that the first code name stands for Bad Aibling. Day after day and month after month, the BND passes on to the NSA massive amounts of connection data relating to the communications it had placed under surveillance. The so-called *metadata* -- telephone numbers, email addresses, IP connections -- then flow into the Americans' giant databases.²³⁷

The same article underlines the fact that copies of two pieces of software developed by the German BND have also been given to NSA agents: "Mira4" and "Veras".²³⁸ These two programmes are allegedly similar in nature to the US XKeyscore system, but there is a clear lack of information on the functions and scope of such software. According to the Spiegel information, the NSA and the BND jointly presented the XKeyscore programme to the civilian Bundesamt für Verfassungsschutz in 2011. Also, according to disclosures by the Washington Post, Germany participates in meetings in the framework of the secret intelligence "Alliance Base" in France, mentioned above, along with US, UK, French, Canadian and Australian representatives which routinely exchange information.²³⁹

Many articles mention the long history of data exchanges between Germany and its Western allies, mostly during the Cold War in the 1960s but also after the 9/11 attacks.²⁴⁰ Bilateral data transfer agreements with the former powers that occupied West Germany – United States, UK and France – have recently been cancelled following the PRISM scandal. These agreements included a task foreseen for the German intelligence agencies to spy on post and radio communications for the purpose of protecting Western troops stationed in Germany.²⁴¹

²³⁶ See Federal Office of Crime Prevention Act (Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten, BKA-Gesetz), available at www.gesetze-im-internet.de/bkag_1997/

²³⁷ Source: H. Gude, L. Poitras and M. Rosenbach (2013) 'Mass Data: Transfers from Germany Aid US Surveillance', Spiegel Online, 5 August 2013, available at www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html

²³⁸ *Ibidem*.

²³⁹ Source: D. Priest (2013), 'Help From France Key In Covert Operations', *op. cit.*

²⁴⁰ Source: M. Eddy (2013) 'For Western Allies, a Long History of Swapping Intelligence', The New York Times, 9 July 2013, available at www.nytimes.com/2013/07/10/world/europe/for-western-allies-a-long-history-of-swapping-intelligence.html

²⁴¹ Der Standard (2013) 'Deutschland beendet Geheimdienst-Abmachung mit Frankreich', 6 August 2013, available at <http://derstandard.at/1375625808305/Deutschland-beendet-Geheimdienst-Abmachung-mit-Frankreich>

4.3. Legal framework and oversight

4.3.1. Legal framework

Article 10 of the German Constitution on the privacy of correspondence, posts and telecommunications states that

- 1) *The privacy of correspondence, posts and telecommunications shall be inviolable.*
- 2) *Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature.²⁴²*

The main federal law in Germany regulating communications surveillance is the G-10 Law, which allows for certain limitations to the secrecy of communications as provided in the Article 10 of the Constitution.²⁴³ Under the G-10 Law, intelligence services may operate warrantless automated wiretaps of domestic and international communications for specific purposes such as the fight against terrorism or the protection of the Constitution. The G-10 Law was amended in 1994 and 2001 to add electronic and voice communications to the list of communications that intelligence agencies may monitor. Also, the law in its paragraph 10 allows the BND to search up to 20% of foreign communications according to certain keywords – these communications include telephone conversations, e-mails, chats etc.

Two major decisions of the German Federal Constitutional Court have limited the scope of the G-10 Law in recent years:

- In March 2004, the Court ruled that the G-10 Law infringed the German Constitution, especially its Article 1 on human dignity and Article 13 on the inviolability of private homes.²⁴⁴ The court held that certain communications, such as contacts with close family members, doctors, priests or lawyers, are protected by an absolute area of intimacy that no government may infringe.
- In February 2008, in a landmark decision, the Court declared certain provisions of a regional law unconstitutional.²⁴⁵ The regional law (of North-Rhine Westphalia) allowed the regional Office for the Protection of the Constitution to secretly gather data on private computers. The Court interpreted Articles 1 and 2 of the German Constitution as containing a fundamental right for every citizen to have the integrity and confidentiality of IT systems guaranteed by the state. The possibility of secret online searches on computers is not categorically ruled out – the Court specified that such measures can only be justified under strict conditions and when there is an imminent threat to the life, physical integrity or liberty of persons, or to the foundations of the state or the existence of mankind.

4.3.2. Oversight

Two oversight bodies exist at Parliamentary level for controlling the activities of German intelligence services:

²⁴² See the translated version of the German Grundgesetz here: http://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html

²⁴³ The full text of the G-10 Law is available online (in German): http://www.gesetze-im-internet.de/g10_2001/BJNR125410001.html

²⁴⁴ Federal Constitutional Court (Bundesverfassungsgericht) decision of 3 March 2004, reference number: 1 BvR 2378/98, available at http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.html (in German).

²⁴⁵ Federal Constitutional Court (Bundesverfassungsgericht) decision of 27 February 2008, reference number: 1 BvR 370/07, available at www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html (in German);

- The G-10 Committee is a committee of the German Parliament (Bundestag) which has the task to decide on the necessity and legitimacy of the measures taken by the three intelligence agencies mentioned above which could infringe upon the fundamental rights enshrined in Article 10 of the German Constitution.²⁴⁶ It is composed of 4 Members of the German Parliament. The G-10 Committee is triggered when an intelligence service makes an official request for a surveillance measure to the German Ministry of Interior and this request is granted. The G-10 also follows the whole procedure, including the collection of the personal data, its analysis and its use. The G-10 also checks whether fundamental rights of German citizens have been violated following individual complaints. Compared with oversight authorities in the USA and in other member states examined in this briefing paper, the German G-10 is the only oversight body that does not only authorise surveillance requests, but also checks how the collection, storage, and analysis of personal data is carried out, investigate individual complaints and holds responsibility for the implementation of the surveillance programmes.²⁴⁷
- The PKGr – Parliamentary Control Committee is the oversight body responsible for controlling the three federal intelligence services mentioned above.²⁴⁸ The German government is obliged to inform the PKGr and to provide all relevant information on the activities of the intelligence agencies to its members. The PKGr is composed of 11 Members of Parliament. According to a recent report by the PKGr on the 2011 activities of the BND, more than 2,9 million of e-mails and text messages have been the subject of surveillance measures.²⁴⁹

In parallel to these two oversight authorities, several other official bodies may have an influence on the ways in which the intelligence services operate in Germany:

- The Committee on Budget of the Bundestag (Haushaltsausschuss),²⁵⁰
- The Courts at national and regional levels,
- The Federal Court of Auditors (Bundesrechnungshof),²⁵¹
- And the Data Protection Authority (Federal Commissioner for Data Protection and Freedom of Information).²⁵²

German data protection bodies at the federal and the regional levels have, in a joint statement, called for increasing the control powers of the two German oversight bodies and strengthening the links with data protection authorities.²⁵³

²⁴⁶ <http://www.bundestag.de/bundestag/gremien/g10/index.html>

²⁴⁷ Refer to S. Heumann, B. Scott (2013), "Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany", Stiftung Neue Verantwortung / Open Technology Institute publication, September 2013.

²⁴⁸ <http://www.bundestag.de/bundestag/gremien/pkgr/index.jsp>

²⁴⁹ German Parliament (2013) Unterrichtung durch das Parlamentarische Kontrollgremium (PKGr) - Bericht gemäß § 14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8 dieses Gesetzes - (Berichtszeitraum 1. Januar bis 31. Dezember 2011), Drucksache 17/12773, 14 March 2013, available at: <http://dip21.bundestag.de/dip21/btd/17/127/1712773.pdf> (in German).

²⁵⁰ See <http://www.bundestag.de/bundestag/ausschuesse17/a08/index.jsp>

²⁵¹ http://www.bundesrechnungshof.de/en?set_language=en

²⁵² http://www.bfdi.bund.de/EN/Home/homepage_node.html

²⁵³ See the joint statement at <http://bit.ly/17yD7nn> (last accessed 22 October 2013)

5. The Netherlands²⁵⁴

There are currently no publicly disclosed programmes of mass cyber surveillance in the Netherlands. Current discussions around large-scale surveillance are limited to expert arenas and are linked to the mandate and capabilities of a new Sigint and Cyber agency, the Joint Sigint Cyber Unit (JSCU) to be established in 2014.

5.1. (Potential) programmes for large-scale surveillance

The Joint Sigint Cyber Unit (JSCU), codenamed "Project Symbolon", will start to function in 2014²⁵⁵. The unit was announced as part of the Dutch Ministry of Defense's Cyber Strategy in 2012²⁵⁶ as a joint effort of the AIVD (General Intelligence and Security Service) and MIVD (Military Intelligence and Security Service). It will replace the current National Signals Intelligence Organisation (NSO), also created with staff from AIVD and MIVD in 2003.

The JSCU is expected to centralise all Signals and Cyber surveillance in the Netherlands²⁵⁷ and will have a staff of 350.²⁵⁸ Its headquarters should be located in the offices of the AIVD in Zoetermeer, while other departments will be located in MIVD premises in The Hague. The signals location in Burum and the analysis location in Eibergen, currently operated by the NSO, will stay active.²⁵⁹

There is currently little knowledge about the budget that will be dedicated to the JSCU. Project Argo II (establishment of the agency) has a budget of € 17 million²⁶⁰.

Concerning the objectives of the new agency, traditionally, Dutch SIGINT activities have focused on supporting military missions abroad and increasingly on counterterrorism activities,²⁶¹ but their official mandate also includes non-security related tasks, such as the collection of economic intelligence. The official objectives of the new agency are both defensive and offensive cyber activity. Offensive activities are being justified by recent cyber-attacks, such as the compromising of the security of government services by the hijacking of electronic signatures issued by certificate authority DigiNotar.²⁶²

²⁵⁴ The data presented here was gathered on the basis of news articles, checked and complemented by interviews with the following experts: Ot van Daalen, Bits of Freedom, 9/10/2013; Jelle van Buuren, Leiden University, Center for Terrorism and Counter-terrorism 10/10/2013; Axel Arnabak, cybersecurity and information law researcher at the Institute for Information Law, University of Amsterdam, 14/10/2013.

²⁵⁵ The renovation operation was codenamed "Argo II". A description of the project can be found on the Dutch Rijks ICT-Dashboard website <http://bit.ly/18Pqw32> Accessed 9/10/2013

²⁵⁶ Netherlands Ministry of Defense, *The Defense Cyber Strategy*, The Hague, September 2012. Available at : <http://bit.ly/GIGC40> Accessed 9/10/2013

²⁵⁷ Letter of the Dutch Ministry of Interior to Dutch MP Van Raak, 21/06/2013, available on the website of the NGO Bits of Freedom <http://bit.ly/18PpGn3> Accessed 9/10/2013

²⁵⁸ NRC Handelsblad, 24/09/2013. Translation in English available at : <http://bit.ly/1hwMyK2> Accessed 9/10/2013

²⁵⁹ NRC Handelsblad, 24/09/2013 Translation in English available at : <http://bit.ly/1hwMyK2> Accessed 9/10/2013

²⁶⁰ Dutch Rijks ICT-Dashboard website <http://bit.ly/18Pqw32> Accessed 9/10/2013

²⁶¹ The need for autonomous Dutch SIGINT was made particularly pressing after the debacle of the 'Dutchbat' (Dutch Battalion under the command of the United Nations Protection Force) in Srebrenica during the war in Bosnia-Herzegovina, which was largely based on misleading intelligence. Source: Interview with Axel Arnabak.

²⁶² NRC Handelsblad, 24/09/2013. Translation in English available at : <http://bit.ly/1hwMyK2> Accessed 9/10/2013

The official objectives of the program, as reported in the 2012 Cyber Strategy prepared by the Ministry of Defence²⁶³, are the following:

- Infiltration of computers and networks to acquire data: mapping out relevant sections of cyberspace; monitoring vital networks; gaining a profound understanding of the functioning of and technology behind offensive cyber assets.
- The gathered information will be used for: early-warning intelligence products; the composition of a cyber threat picture; enhancing the intelligence; production in general; conducting counterintelligence activities.
- Cyber intelligence capabilities cannot be regarded in isolation from intelligence capabilities such as: signals intelligence (SIGINT); human intelligence (HUMINT) and the MIVD's existing counterintelligence capability.

At the moment, SIGINT activities in the Netherlands are limited to targeting specific individuals, both citizens and non-citizens, domestically and abroad. The MIVD is responsible for overseas SIGINT, while the AIVD is responsible for domestic targeted searches.

As mentioned previously, Dutch intelligence agencies are prohibited from conducting mass cable surveillance. Telecommunication interceptions are focused on individuals, and have to receive ministerial approval. In the meantime, both the AIVD and the MIVD working within the NSO are allowed to collect and store internet communications. This data can be searched through queries and keywords, but these also need to receive prior ministerial approval. It is worth noting however the potential for large-scale surveillance that the Netherlands holds given that the Amsterdam Internet Exchange Point (IXP) is the second largest in Europe after Frankfurt.²⁶⁴ As noted above, the Amsterdam IXP has partnered with other contractors in the development of Project Argos II.

The information currently gathered by the NSO and in the future by the JSCU will be available to both AIVD and the MIVD. It is not known yet which other law enforcement agencies will have access to the information produced by the JSCU. Concerning the involvement of private actors, it is worth noting that private sector companies have been involved in project Argos II: the Amsterdam Internet Exchange (AMS-IX), NICE Systems, an Israeli firm specialising in cyber security, as well as Accenture, an American consulting firm.²⁶⁵

5.2. Cooperation with foreign intelligence services

Anonymous sources from the Dutch intelligence agencies have told the Telegraaf newspaper that the AIVD has routine access to information from the NSA "within five minutes".²⁶⁶ This would allegedly allow Dutch intelligence services to have access to information on Dutch individuals from the US PRISM programme without the need for an express warrant as required by Dutch law. The Dutch Parliament has launched an inquiry into the role of the AIVD in this context to assess whether they have used private data obtained through the NSA's activities.²⁶⁷ Dutch officials such as Home Affairs Minister

²⁶³ Netherlands Ministry of Defense, *The Defense Cyber Strategy*, The Hague, September 2012. Available at: <http://bit.ly/GIGC40> Accessed 9/10/2013

²⁶⁴ Weller, D., Woodcock, B. (2013) 'Internet Traffic Exchange: Market Developments and Policy Challenges'. *OECD Digital Economy Papers*, 207, p. 41.

²⁶⁵ Letter of the Dutch Ministry of Interior to Dutch MP Van Raak. 21/06/2013 Available on the website of the NGO Bits of Freedom <http://bit.ly/18PpGn3> Accessed 9/10/2013

²⁶⁶ Source: B. Olmer (2013), 'Ook AIVD bespiedt internetter', De Telegraaf, 11 June 2013, available at: www.telegraaf.nl/binnenland/21638965/Ook_AIVD_bespiedt_online.html See also the official condemnation by the Dutch digital rights organization Bits of Freedom « Persbericht: Bits Of Freedom Eist Einde Gebruik Prism Door Nederlandse Geheime Diensten » <http://bit.ly/HeBh6l> Accessed 10/10/2013.

²⁶⁷ Source: Amsterdam Herald (2013), 'Inquiry into role of Dutch intelligence agencies in Prism data harvesting scandal', The Amsterdam Herald, 3 July 2013, available at:

Ronald Plasterk have denied that AIVD and MIVD make direct use of the PRISM programme.²⁶⁸ The Dutch government also released an official statement rebuffing the allegation.²⁶⁹

5.3. Legal framework and oversight

5.3.1. Legal framework

The current legislative framework the Dutch Intelligence and Security Act 2002 (Wiv 2002) does not permit the services to wiretap "cable-bound communications" under any circumstances.²⁷⁰ The establishment of the JSCU will therefore require a modification of the law. A commission, headed by C.W.M. Dessens, has been established to investigate if and under which conditions should the law be modified.²⁷¹ The conclusions of the commission, initially expected in September 2013, are likely to be made public before the end of 2013.²⁷² On the basis of the composition of the commission, two of our respondents suggested that it is likely that the law will be amended to permit the tapping of cable-bound communications.

5.3.2. Oversight

Currently, wiretapping activities require the approval of the minister of interior, who signs off all wiretapping orders. The main institution in charge of the monitoring of the AIVD and MIVD activities is the CTIVD (Review Committee on the Intelligence and Security Services). The CTIVD does not have direct access to all activities of the services, but is allowed to "sample" some of their activities for compliance. A recent report showed that when the committee looked into the compliance in the context of international SIGINT assistance, "it found that such assessments were not always made properly".²⁷³

There is currently no information about the structure of checks and balances that will apply to the new JSCU, although it is likely that it will fall under CTIVD mandate.

<http://amsterdamherald.com/index.php/rss/906-20130703-inquiry-role-dutch-intelligence-agencies-prism-data-harvesting-scandal-united-states-nsa-europe-aivd-mivd-netherlands-dutch-security>

²⁶⁸ See A. Eigenraam (2013), 'Plasterk: Nederland maakt geen gebruik van Prism', 21 June 2013, NRC Handelsblad, available at: www.nrc.nl/nieuws/2013/06/21/plasterk-nederland-maakt-geen-gebruik-van-prism/

²⁶⁹ See www.rijksoverheid.nl/nieuws/2013/06/21/geen-onbelemmerde-toegang-tot-internet-en-telefoon-voor-aivd-en-mivd.html

²⁷⁰ NRC Handelsblad, 24/09/2013 Translation in English available at: <http://bit.ly/1hwMyK2> Accessed 9/10/2013

²⁷¹ The commission is composed of : Luitenant-generaal b.d. M.A. Beuving; prof. dr. mr. E.R. Muller; vice-admiraal b.d. W. Nagtegaal; mr. H.J.I.M. de Rooij; prof. mr. W.M.E. Thomassen; prof. dr. W.J.M. Voermans. See "Regeling instelling Evaluatiecommissie Wiv 2002" <http://bit.ly/18PuM2J> Accessed 9/10/2013

²⁷² NRC Handelsblad, 24/09/2013 Translation in English available at : <http://bit.ly/1hwMyK2> Accessed 9/10/2013

²⁷³ See CTIVD, 'Toezichtsrapportage inzake de inzet van SIGINT door de MIVD', CTIVD nr. 28, 23 August 2011, pp. 59-60. Quoted in Hoboken, Arnbak, van Eijk (2013) Obscured by Clouds, or How to Address Governmental Access to Cloud Data From Abroad. Paper presented at the Privacy Law Scholars Conference 2013, 6-7 June, Berkeley, CA. <http://bit.ly/18PxyVK> Accessed 9/10/2013; See also the most recent report of the CTIVD, "TOEZICHTSRAPPORT inzake de inzet van de af luisterbevoegdheid en de bevoegdheid tot de selectie van Sigint door de AIVD", July 2013, <http://bit.ly/H1KA8R> Accessed 9/10/2013.



EUROPEAN PARLIAMENT

CATALOGUE BA-01-13-601-EN-C

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS **C**

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

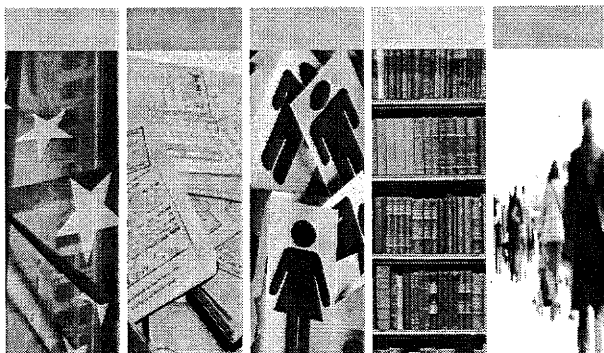
Policy Areas

- Constitutional Affairs
- Justice, Freedom and Security
- Gender Equality
- Legal and Parliamentary Affairs
- Petitions

Documents

Visit the European Parliament website: <http://www.europarl.europa.eu/studies>

PHOTO CREDIT: iStock International Inc.



ISBN 978-92-823-4965-6

doi: 10.2861/4180



Publications Office

Dokument 2014/0067380

Von: Peters, Reinhard
Gesendet: Mittwoch, 30. Oktober 2013 09:59
An: Kaller, Stefan; ALOES_; Jergl, Johann; PGNSA
Betreff: WG: BRUEEU*5038: 2472. AStV-2 am 29.10.2013

Vertraulichkeit: Vertraulich

z.K.: In der Nachbereitung des jüngsten Europäischen Rats durch den AStV wurde das Thema "NSA" ausweislich des Drahtberichts nicht thematisiert.

Mit besten Grüßen
Reinhard Peters

-----Ursprüngliche Nachricht-----

Von: frdi [mailto:ivbbgw@BONNFMZ.Auswaertiges-Amt.de]

Gesendet: Mittwoch, 30. Oktober 2013 09:20

Cc: 'krypto.betriebsstell@bk.bund.de'; BMAS Referat SV; 'bmbf@bmbf.bund.de'; BMELV Poststelle; 'aa-telexe@bmf.bund.de'; 'tkz@bmfsfj.bund.de'; BMG Posteingangsstelle, Bonn; Zentraler Posteingang BMI (ZNV); 'posteingang@bmu.bund.de'; 'fernshr@bmvbs.bund.de'; 'poststelle@bmwi.bund.de'; 'poststelle@bmz.bund.de'; 'eurobmwi@bmwi.bund.de'

Betreff: BRUEEU*5038: 2472. AStV-2 am 29.10.2013

Vertraulichkeit: Vertraulich

VS - Nur fuer den Dienstgebrauch

WTLG

Dok-ID: KSAD025558080600 <TID=099089870600>

BKAMT ssnr=2044

BMAS ssnr=2916

BMBF ssnr=2986

BMELV ssnr=3959

BMF ssnr=7372

BMFSFJ ssnr=1487

BMG ssnr=2814

BMI ssnr=5455

BMU ssnr=3305

BMVBS ssnr=2441

BMWI ssnr=8630

BMZ ssnr=5577

EUROBMWI ssnr=4270

aus: AUSWAERTIGES AMT

an: BKAMT, BMAS, BMBF, BMELV, BMF, BMFSFJ, BMG, BMI, BMU, BMVBS, BMWI, BMZ, EUROBMWI

Bl. 153-154

Entnahme wegen fehlenden Bezugs zum
Untersuchungsgegenstand

Dokument 2014/0067386

Von: Peters, Reinhard
Gesendet: Dienstag, 29. Oktober 2013 19:37
An: PGNSA
Betreff: WG: BRUEDIP*143: BEL Presse zur Abhöraffaire

Vertraulichkeit: Vertraulich

erl.: -1
erl. : -1

zK

Mit besten Grüßen
Reinhard Peters

-----Ursprüngliche Nachricht-----

Von: Binder, Thomas
Gesendet: Dienstag, 29. Oktober 2013 18:12
An: Peters, Reinhard
Betreff: WG: BRUEDIP*143: BEL Presse zur Abhöraffaire
Vertraulichkeit: Vertraulich

Z.K.

Mit freundlichen Grüßen
Thomas Binder

-----Ursprüngliche Nachricht-----

Von: BMIPoststelle, Postausgang.AM1
Gesendet: Dienstag, 29. Oktober 2013 15:25
An: GII1_
Cc: UALGII_; IDD_
Betreff: BRUEDIP*143: BEL Presse zur Abhöraffaire
Vertraulichkeit: Vertraulich

-----Ursprüngliche Nachricht-----

Von: frdi [mailto:ivbbgw@BONNFMZ.Auswaertiges-Amt.de]
Gesendet: Dienstag, 29. Oktober 2013 15:10
Cc: 'krypto.betriebsstell@bk.bund.de'; Zentraler Posteingang BMI (ZNV); 'poststelle@bmwi.bund.de'; 'reg.4@bpa.bund.de'
Betreff: BRUEDIP*143: BEL Presse zur Abhöraffaire
Vertraulichkeit: Vertraulich

WTLG

Dok-ID: KSAD025557420600 <TID=099081570600>
BKAMT:ssnr=2019

BMI ssnr=5442
 BMWI ssnr=8615
 BPA ssnr=1819

aus: AUSWAERTIGES AMT
 an: BKAMT, BMI, BMWI, BPA

aus: BRUESSEL DIPLO
 nr 143 vom 29.10.2013, 1458 oz
 an: AUSWAERTIGES AMT

Fernschreiben (verschlüsselt) an E10
 eingegangen: 29.10.2013, 1458
 auch fuer ATHEN DIPLO, BKAMT, BMI, BMWI, BPA, BRUESSEL EURO,
 BRUESSEL NATO, BUDAPEST, DEN HAAG DIPLO, DUBLIN DIPLO,
 HELSINKI DIPLO, KOPENHAGEN DIPLO, LISSABON DIPLO, LUKSEMBURG DIPLO,
 MADRID DIPLO, PARIS DIPLO, PRAG, ROM DIPLO, WARSCHAU, WASHINGTON,
 WIEN DIPLO

auch für 013
 Verfasser: Margret Pollmeier
 Gz.: Pr 312.08/2 291455
 Betr.: BEL Presse zur Abhöraffaire
 hier: Abhöraffaire dominiert europäischen Gipfel
 Bezug: ohne

-- zur Unterrichtung --

I. Zusammenfassung:

Auch in der BEL Presse dominiert die NSA-Abhöraffaire die Berichterstattung über den europäischen Gipfel von letzter Woche. Während Donnerstag und Freitag noch bloße Empörung über die Lauschangriffe der NSA auf europäische Regierungschef vorherrscht, spekulieren die Zeitungen am Wochenende und am Montag mehr darüber, wieviel und seit wann der amerikanische Präsident Obama von den Abhöraktionen gewusst und sie womöglich sogar gebilligt habe. Obwohl fast alle Zeitungen in den Lauschangriffen eine Chance für die Europäer sehen, den USA einmal entschlossen gemeinsam entgegenzutreten, geht niemand davon aus, dass die europäisch-amerikanischen Handels- und Wirtschaftsbeziehungen durch die Affäre ernsthaft gestört würden.

II. Im einzelnen:

1. Empörung über NSA Lauschangriffe

"Europa böse auf Obama" titelt die flämischsprachige Tageszeitung De Standaard am 25.10., nachdem De Morgen schon am Vortag verkündet hatte "Merkel böse wegen abgehörten Mobiltelefon". Und La Libre Belgique wundert sich am Freitag "Oh grand frère, comme tu as de grandes oreilles..." (beide 25.10.) Alle Zeitungen zitieren Angela Merkel mit "Entre amis, cela ne se fait pas" (z.B. Le Soir, 25.10.) und betonen, dass nach Aussagen der Kanzlerin "das gegenseitige Vertrauen durch die Vereinigten

Staaten geschädigt worden sei und wieder neu aufgebaut werden müsse"(z.B. De Morgen, 25.10.). De Standaard und De Morgen betonen am 24.10. auch die große "Deutlichkeit", mit der Merkel bei Obama um eine Klärung der Angelegenheit gebeten habe.

2. Lauschangriffe dominieren EU-Gipfel

"EU-Top im Bann der Spionage" (De Morgen, 25.10.) und "L'affaire du 'téléphone de Merkel', un parasite sur le sommet européen" (Le Soir, 25.10.). Aber obwohl laut Le Soir vom 25.10. die Lauschangriffe auf Merkels Handy das einzige Thema der Journalistenfragen bei der Ankunft der Regierungschefs am Donnerstag waren, stellt De Standaard vom selben Tag klar, dass das Thema besonders in den "Wandelgangen" (Fluren)heiß diskutiert worden sei. Bezug zum Gipfelthema digitale Wirtschaft habe der Abhörskandal natürlich auch, da Merkel ihn z.B. nutzen könne, um eine Annahme des Textes der umstrittenen Richtlinie von Barroso/Reding zum besseren Schutz der Privatsphäre etwas rascher durchzusetzen (Le Soir 25.10.). Da aber De Morgen am gleichen Tag das genaue Gegenteil berichtet ("Auffallend genug war Merkel - zusammen mit GB PM Cameron - gegen einen besseren Schutz der Privatsphäre"), sollte das Thema wohl zunächst in die "Wandelgangen" der Reaktionen zurückverwiesen werden.

3. Einigkeit im Auftreten der Europäer gegenüber den USA

Unter den Überschriften "Merkel und Hollande: eine Front gegen USA" (De Standaard, 25.10.), "Les dirigeants européens grondent les Etats-Unis" (La Libre Belgique, 26./27.10.) und "L'espionnage de Merkel, l'affaire que unit les Européens" (De Tijd, 25.10.) beschwören die BEL Zeitungen die neue deutsch-französische Einigkeit in der Verurteilung der NSA-Abhörpraktiken gegenüber den USA, der sich anderen europäischen Staaten anschließen könnten(De Standaard 26./27.10.). Hier hätten laut De Morgen (25.10.), De Standaard (26./27.10.) und La Libre Belgique (26./27.10.) die Europäer endlich die Chance gegenüber den USA gemeinsam aufzutreten, um Aufklärung zu fordern und solche Abhörpraktiken in Zukunft zu verhindern. Allerdings weisen De Morgen (25.10.) und La Libre Belgique (26./27.10.) daraufhin, dass die neue Einigkeit der Europäer etwas darunter leide, dass ja auch europäische Geheimdienste, wie z.B. der britische, durchaus bereit seien, bei befreundeten MS zu spionieren. In dieser Situation habe v.a. der BEL MP Di Rupo schnell eigene Sicherheitsmaßnahmen getroffen und verfügt, dass seine Minister bei geheimen Besprechungen gar keine Handys mehr bei sich haben dürften (De Standaard, 29.10.) Und das, obwohl er selbst offenbar (noch) gar nicht von der NSA abgehört worden sei. (La Libre Belgique, 25.10.)

4. Keine Konsequenzen für Wirtschaftsbeziehungen zu den USA

"Europa bellt, aber es beißt nicht" titelt De Morgen am Wochenende, während La Libre Belgique mit "L'Europe s'émeut. Et après?" in dasselbe Horn bläst. Inhaltlich merken alle großen Zeitungen an, dass es bei aller Empörung letztlich keine Reaktion der Europäer auf die Lauschangriffe gegeben habe, nicht einmal eine gemeinsame Erklärung zur Verurteilung der Abhörpraktiken (De Morgen, 25.10.). Der Vorschlag eines Abbruchs der Gespräche über das Freihandelsabkommen mit den USA werde zurückgewiesen und auch die Verhandlungen über den Transfer von Bank- und Passagierdaten seien nicht gefährdet (De Standaard, De Morgen, La Libre Belgique 26./27.10.)- nicht nur weil man Obama nicht verärgern wolle (La Libre Belgique(25.10.), sondern letztlich auch deshalb, weil sich die Europäer darauf nicht einigen könnten (La Libre Belgique, 25.10.)

5. Wieviel wußte Obama?

Dies ist die Frage, die sich die Zeitungen unter Berufung auf deutsche Medien (z.B. Der Spiegel, Bild am Sonntag) v.a. am Montag stellen. Alle gehen davon aus, dass Merkel seit 2002 bespitzelt werde und dass Obama spätestens seit 2010 davon gewußt habe. Einigkeit besteht auch darin, dass vermutet werde, die Bespitzelung sei von der Berliner US-Botschaft ausgegangen (De Morgen, Le Soir, La Libre Belgique). Und obwohl Le Soir und La Libre Belgique berichten, Obama habe Merkel persönlich versichert, nichts von den Lauschangriffen gewusst zu haben, betont v.a. De Standaard (28.10.), dass gerade die Glaubwürdigkeit Obamas unter dem Skandal gelitten habe und fragt, ob er "wirklich so unschuldig und naiv" sei.

III. Wertung:

Auffällig ist, dass der Lauschangriff auf Angela Merkel deutlich mehr Aufmerksamkeit in den BEL Zeitungen bekommt als der auf 70 Millionen Franzosen und - vielleicht - den F Präsidenten kurz vorher. Das Thema Abhörskandal hat klar die Berichterstattung über den Gipfel dominiert, dessen eigentliche Themen deutlich weniger kommentiert wurden. Die BEL Zeitungen sehen die amerikanischen Abhörpraktiken als Chance und Herausforderung für Europa an, sind sich aber sehr im Zweifel, ob Europa in seiner

Zerrissenheit ersteres nutzen kann und letzterem gewachsen ist. Obama, der "eiskalte Freund" (De Standaard, 26./27.10.) solle zwar ein schlechtes Gewissen bekommen, aber nicht ernsthaft verärgert werden. So scheint am Ende die große Gemeinsamkeit der Europäer v.a. in ihrem gemeinsamen Schicksal zu bestehen: "Dear Europeans, Uncle Sam is watching you" (La Libre Belgique, 25.10.).

Im Auftrag

Margret Pollmeier

Dokument 2014/0067388

Von: GII2_
Gesendet: Mittwoch, 30. Oktober 2013 12:21
An: OESI4_ ; B4_ ; PGDS_ ; IT1_ ; IT3_ ; O1_
Cc: GII2_ ; GII3_ ; GII4_ ; GII5_ ; GIII1_ ; GIII5_ ; GIII4_ ; OESI2_ ; OESI3AG_ ; OESII2_ ; OESIII3_ ; PGDBOS_ ; PGNSA ; MI1_ ; MI3_ ; MI4_ ; MI5_ ; VII4_ ; IT5_ ; O2_ ; O4_ ; O5_ ; Hübner, Christoph, Dr. ; Wolf, Katharina ; Popp, Michael ; AA Konther, Michael
Betreff: BRUEEU*5038: 2472. AStV-2 am 29.10.2013; hier: TOP 31: Weiteres Vorgehen im Anschluss an den Europäischen Rat 24./25.10.2013

Vertraulichkeit: Vertraulich

Nachstehender o.a. DB auch Ihnen

z.K.

(Ratssekretariat kündigte für Nov. Vorlage einer Roadmap für die Vorbereitungen des Dez.-ER 2013 an)

Mit freundlichen Grüßen
 Im Auftrag
 Roland Arhelger

BMI-Referat G II 2
 EU-Grundsatzfragen einschließlich
 Schengenangelegenheiten;
 Beziehungen zum Europäischen Parlament;
 Europabeauftragte
 Bundesministerium des Innern
 Alt-Moabit 101 D,
 10559 Berlin
 Tel. +49 (0)30 18 681 - 2370
 Fax +49 (0)30 18 681 - 52370
 e-mail: roland.arhelger@bmi.bund.de

Von: BMIPoststelle, Posteingang.AM1
 Gesendet: Mittwoch, 30. Oktober 2013 09:22
 An: GII2_
 Cc: GII1_ ; GII2_ ; MI5_ ; UALGII_ ; VI4_ ; UALOESI_ ; Korff, Annegret
 Betreff: VS-NfD: BRUEEU*5038: 2472. AStV-2 am 29.10.2013

-----Ursprüngliche Nachricht-----

Von: frdi [mailto:ivbbgw@BONNFMZ.Auswaertiges-Amt.de]
 Gesendet: Mittwoch, 30. Oktober 2013 09:20
 Cc: 'krypto.betriebsstell@bk.bund.de'; BMAS Referat SV; 'bmbf@bmbf.bund.de'; BMELV Poststelle; 'aa-

telexe@bmf.bund.de'; 'tkz@bmfsfj.bund.de'; BMG Posteingangstelle, Bonn; Zentraler Posteingang BMI (ZNV); 'posteingang@bmu.bund.de'; 'fernschr@bmvbs.bund.de'; 'poststelle@bmwi.bund.de'; 'poststelle@bmz.bund.de'; 'eurobmwi@bmwi.bund.de'

Betreff: BRUEEU*5038: 2472. AStV-2 am 29.10.2013

Vertraulichkeit: Vertraulich

 VS-Nur fuer den Dienstgebrauch

WTLG

Dok-ID: KSAD025558080600 <TID=099089870600> BKAMT ssnr=2044 BMAS ssnr=2916 BMBF ssnr=2986 BMELV ssnr=3959 BMF ssnr=7372 BMFSFJ ssnr=1487 BMG ssnr=2814 BMI ssnr=5455 BMU ssnr=3305 BMVBS ssnr=2441 BMWI ssnr=8630 BMZ ssnr=5577 EUROBMWI ssnr=4270

aus: AUSWAERTIGES AMT

an: BKAMT, BMAS, BMBF, BMELV, BMF, BMFSFJ, BMG, BMI, BMU, BMVBS, BMWI, BMZ, EUROBMWI

aus: BRUESSEL EURO

nr 5038 vom 30.10.2013, 0915 oz

an: AUSWAERTIGES AMT

 Fernschreiben (verschlüsselt) an E01
 eingegangen: 30.10.2013, 0918

VS-Nur fuer den Dienstgebrauch

auch fuer ATHEN DIPLO, BKAMT, BMAS, BMBF, BMELV, BMF, BMFSFJ, BMG, BMI, BMJ, BMU, BMVBS, BMVG, BMWI, BMZ, BRUESSEL DIPLO, BUDAPEST, BUKAREST, DEN HAAG DIPLO, DUBLIN DIPLO, EUROBMWI, HELSINKI DIPLO, KOPENHAGEN DIPLO, LISSABON DIPLO, LONDON DIPLO, LUKSEMBURG DIPLO, MADRID DIPLO, PARIS DIPLO, PRESSBURG, RIGA, ROM DIPLO, SOFIA, STOCKHOLM DIPLO, TALLINN, WASHINGTON, WIEN DIPLO, ZAGREB

 im AA auch für: EKR, E02, E03, E04, E05, E06, EUKOR

Verfasser: Jahnke

Gz.: Pol 421.30 300915

Betr.: 2472. AStV-2 am 29.10.2013

hier: TOP 31: Weiteres Vorgehen im Anschluss an den Europäischen Rat am 24./25.10.2013

Bezug: Weisung von EKR vom 28.10.2013

-- Zur Unterrichtung --

1. Zum weiteren Vorgehen im Anschluss an den ER am 24./25.10.13 hob Vorsitz hervor:

a. Wirtschafts- und Währungsunion: Sherpas trafen sich am 26.11. zur Vorbereitung des Dezember-ER. Die am SRM teilnehmenden MS seien aufgefordert worden, für die umfassende Bewertung der Kreditinstitute durch die EZB einen koordinierten europ. Ansatz festzulegen. Rat müsse diesen Ansatz vor Ende November beschließen.

b. Gesetzgebung: EP und Rat seien ersucht worden, die Vorschläge zum Digitalen Binnenmarkt sowie zur Bankenunion beschleunigt zu behandeln.

c. Kommission: KOM sei ersucht worden, die Überprüfung des EU-Rechtsrahmens für Urheberrecht im Frühjahr 2014 abzuschließen, im Zuge der Überprüfung der MwSt.-Vorschriften auch die digitalen Wirtschaft zu berücksichtigen, bzgl. der Dienstleistungs-RL den MS Orientierungshilfe bei der Verhältnismäßigkeit zu geben.

d. Jugendarbeitslosigkeit: MS seien aufgefordert worden, vor Ende 2013 Pläne zu deren Bekämpfung zu verabschieden.

e. Migration: Die Task Force "Mittelmeerraum" sei ersucht worden, vorrangige Maßnahmen für wirksamere kurzfristige Nutzung der europäischen Strategien und Instrumente festzulegen. KOM werde dem J/I-Rat am 5./6.12. berichten, Vorsitz werde dem Dezember-ER berichten.

2. Ratssekretariat kündigte für November die Vorlage einer Roadmap für die Vorbereitungen des Dezember-ER an.

3. Aus der kurzen Aussprache ist festzuhalten:

Bzgl. strategischer Technologien wie Big Data und Cloud-Computing, sowie bzgl. der Besteuerung des digitalen Sektors baten FRA und DNK um Empfehlungen der KOM zum weiteren Vorgehen. KOM sagte Prüfung zu.

Bzgl. der Migrationsströme wiesen BLG und MT darauf hin, dass die notwendigen Entscheidungen beim Dezember-ER getroffen werden müssten.

Bzgl. des Wirtschafts- und Handelsabkommens mit CAN kritisierten ROU und BLG die "überraschende" Einfügung des Textes. Texte sollten künftig früher vorgelegt werden.

Tempel

Dokument 2014/0067365

Von: Fax 1438 <BMIXPRAM1/FAXG3/+4930186811438>
Gesendet: Dienstag, 5. November 2013 09:25
An: Weinbrenner, Ulrich
Betreff: MID=17403: Eingehendes FAX von +4930186811438 (MID=17405)
Anlagen: 17403_FAX_131105-092434.PDF

Sehr geehrter/e Empfänger/in
anbei ein neues Faxdokument von der Faxnummer
+4930186811438

Es wurden 001-Seite/n empfangen für Sie um 09:24:34 Uhr am 05.11.2013

ANLAGEERKLÄRUNG DER STAATS- UND REGIERUNGSCHEFS

Die Staats- und Regierungschefs haben die jüngsten Entwicklungen in Bezug auf mögliche Fragen im Zusammenhang mit der Nachrichtengewinnung und die große Besorgnis, die diese Ereignisse unter den europäischen Bürgern ausgelöst haben, erörtert.

Sie betonen die engen Beziehungen zwischen Europa und den USA und den Wert dieser Partnerschaft. Sie sind davon überzeugt, dass die Partnerschaft auf Respekt und Vertrauen beruhen muss, auch was die Arbeit und die Zusammenarbeit der Geheimdienste betrifft.

Sie heben hervor, dass die Nachrichtengewinnung ein wesentlicher Bestandteil des Kampfes gegen den Terrorismus ist. Dies gilt für die Beziehungen zwischen den europäischen Ländern wie auch für die Beziehungen zu den USA. Ein Mangel an Vertrauen könnte die notwendige Zusammenarbeit auf dem Gebiet der Nachrichtengewinnung beeinträchtigen.

Die Staats- und Regierungschefs nehmen zur Kenntnis, dass Frankreich und Deutschland bilaterale Gespräche mit den USA führen wollen, um bis zum Jahresende zu einer Verständigung über die gegenseitigen Beziehungen auf diesem Gebiet zu gelangen. Sie vermerken, dass sich andere EU-Länder gerne an dieser Initiative beteiligen können.

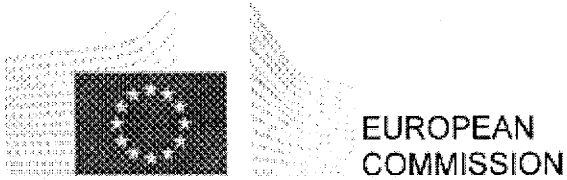
Sie verweisen zudem auf die bestehende Arbeitsgruppe zwischen der EU und den USA zur damit zusammenhängenden Frage des Datenschutzes und rufen dazu auf, diesbezüglich rasch konstruktive Fortschritte zu erzielen.

Dokument 2014/0067383

Von: .BRUEEU POL-IN2-2-EU Eickelpasch, Joerg <pol-in2-2-eu@brue.auswaertiges-amt.de>
Gesendet: Donnerstag, 21. November 2013 12:17
An: Weinbrenner, Ulrich; Peters, Reinhard; Stentzel, Rainer, Dr.; Spitzer, Patrick, Dr.
Cc: 't.pohl@diplo.de'
Betreff: sehr vertraulich - KOM-Entwurf Mitteilung "rebuilding trust in EU-US data flows"
Anlagen: COM draft - Rebuilding trust in EU-US data flows (2).PDF
Wichtigkeit: Hoch

Bitte vertraulich behandeln, um unsere Quelle zu schützen. KOM will die Mitteilung am 27.11.2013 veröffentlichen.

Viele Grüße,
Jörg Eickelpasch



Brussels, XXX
[...] (2013) XXX draft

COMMUNICATION FROM THE COMMISSION

[mandatory element]

COMMUNICATION FROM THE COMMISSION

Rebuilding trust in EU-US data flows

INTRODUCTION: THE CHANGING ENVIRONMENT OF EU-US DATA PROCESSING

Concerns have been expressed at both EU and Member State level at revelations of large-scale US intelligence collection programmes, in particular as regards the protection of personal data of EU citizens.¹ Trust has been affected. Yet the European Union and the United States are strategic partners. This relationship is critical for our security, the promotion of our shared values, and our common leadership in global affairs.

Transfers of personal data are an essential element of the transatlantic relationship. They form an integral part of commercial exchanges across the Atlantic. They also constitute a crucial component of EU-US co-operation in the law enforcement field, and of the cooperation between Member States and the US in the field of national security. In order to facilitate data flows, while ensuring a high level of data protection as required under EU law, the US and the EU have put in place a series of agreements and arrangements.

Commercial exchanges are addressed by Decision 2000/520/EC² (hereafter "the Safe Harbour Decision"). This Decision provides a legal basis for transfers of personal data from the EU to companies established in the US which have adhered to the Safe Harbour Privacy Principles.

Exchange of personal data between the EU and the US for the purposes of law enforcement, including the prevention and combating of terrorism and other forms of serious crime, is governed by a number of agreements at EU level. These are the Mutual Legal Assistance Agreement³, the Agreement on the use and transfer of Passenger Name Records (PNR)⁴, the Agreement on the processing and transfer of Financial Messaging Data for the purpose of the Terrorist Finance Tracking Program (TFTP)⁵, and the Agreement between Europol and the US. These Agreements respond to important security challenges and meet the common

¹ For the purposes of this Communication, references to EU citizens include non-EU citizens present in the European Union.

² Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25.8.2000, p. 7.

³ Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 291, 7.11. 2009, p. 40.

⁴ Council Decision 2012/472/EU of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L 215, 11.8.2012, p. 4.

⁵ Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195, 27.7.2010, p. 3.

security interests of the EU and US, whilst fully guaranteeing the protection of personal data. In addition, the EU and the US are currently negotiating a framework agreement on data protection in the field of police and judicial cooperation ("umbrella agreement")⁶. The aim is to ensure a high level of data protection for citizens whose data is exchanged thereby further advancing EU-US cooperation in the combating of crime and terrorism on the basis of shared values and agreed safeguards.

These instruments operate in an environment in which personal data flows are acquiring increasing relevance.

On the one hand, the development of the digital economy has led to exponential growth in the quantity, quality and diversity of data processing activities. The use of telecommunication services by citizens in their daily lives has increased. Personal data has become a highly valuable asset: the estimated value of EU citizens' data was €315bn in 2011 and has the potential to grow to nearly €1tn annually by 2020⁷. The market for the analysis of large sets of data is growing by 40% per year worldwide.⁸

The increase in the use of electronic communications and data processing services, including cloud computing, has also substantially expanded the scope and significance of transatlantic data transfers. Elements such as the central position of US companies in the digital economy⁹, the transatlantic routing of a large part of electronic communications and the volume of electronic data flows between the EU and the US have become even more relevant.

On the other hand, modern methods of personal data processing raise new and important questions. This applies both to new means of large-scale processing of consumer data by private companies for commercial purposes, and to the increased ability of large-scale surveillance of communications data by intelligence authorities.

Large-scale US intelligence collection programmes, such as PRISM affect the fundamental rights of Europeans and, specifically, their right to privacy and to the protection of personal data. They have also made a connection between Government surveillance and the collection of data by private companies. As a result, they may have an economic impact. If citizens are concerned about the large-scale processing of their personal data by private companies or by the surveillance of their data by security agencies when using Internet services, this may affect their trust in the digital economy, with potential negative consequences on growth.

These developments expose the EU-US data flows to new challenges. This Communication addresses these challenges. It explores the way forward on the basis of the findings contained

⁶ Council adopted the negotiating mandate on 3 December 2010.

⁷ See Boston Consulting Group, "The Value of our Digital Identity", November 2012.

⁸ See McKinsey, "Big data: The next frontier for innovation, competition, and productivity", 2011

⁹ For example, the combined number of unique visitors to Microsoft Hotmail, Google Gmail and Yahoo! Mail from European countries in June 2012 totalled over 227 million, eclipsing that of all other providers. The combined number of unique European users accessing Facebook and Facebook Mobile in March 2012 was 196.5 million, making Facebook the largest social network in Europe. Google is the leading internet search engine with 90.2% of worldwide internet users. US mobile messaging service What's App was used by 91% of iPhone users in Germany in June 2013.

in the annexed Report of the EU Co-Chairs of the ad hoc EU-US Working Group (Annex I) and the Report of the functioning of the Safe Harbour Scheme (Annex II).

In this context, it should also be recalled that whilst the EU can take action in areas of EU competence, in particular to safeguard the application of EU law,¹⁰ national security remains the sole responsibility of each Member State.¹¹

This Communication addresses the EU-US relationship in the light of the surveillance revelations. It seeks to provide an effective way forward to rebuild trust following recent surveillance revelations. The goal is to reinforce EU-US cooperation in these fields and strengthen the broader transatlantic relationship.

Sharing relevant information, including personal data, is an essential element of this relationship and its protection standard should be addressed in its proper context, without affecting other dimensions of EU-US relations, including the on-going negotiations for a Transatlantic Trade and Investment Partnership. For this reason, data protection standards will not be negotiated within the Transatlantic Trade and Investment Partnership, but fully respect the legitimate data protection rules on either side.

2. THE IMPACT ON THE INSTRUMENTS FOR DATA TRANSFERS

As regards data transferred for commercial purposes, the Safe Harbour has proven to be an important vehicle for EU-US data transfers. Its commercial importance has grown as personal data flows have taken on greater prominence in the transatlantic commercial relationship. Over the past 13 years, the Safe Harbour scheme has evolved to include more than 3.000 companies, over half of which have signed up within the last five years. Yet concerns about the level of protection of personal data of EU citizens transferred to the US under the Safe Harbour scheme have grown. The voluntary and declaratory nature of the scheme has sharpened focus on its transparency and enforcement. While a majority of US companies apply its principles, some self-certified companies do not. The non-compliance of some self-certified companies with the Safe Harbour Privacy Principles places such companies at a competitive advantage in relation to European companies operating in the same markets.

Moreover, while under the Safe Harbour, limitations to data protection rules are permitted where necessary on grounds of national security¹², the question has arisen whether the large-scale collection and processing of personal information under U.S. surveillance programmes is necessary and proportionate to meet the interests of national security. It is also clear from the findings of the ad hoc EU-US Working Group that, under these programmes, EU citizens do not enjoy the same rights and procedural safeguards as Americans.

The reach of these surveillance programmes, combined with the unequal treatment of EU citizens, brings into question elements of the Safe Harbour Agreement. The personal data of

¹⁰ See Judgment in Case C-300/11. ZZ v Secretary of State for the Home Department

¹¹ Article 4 (3) TEU.

¹² See e.g. Safe Harbour Decision, Annex I.

EU citizens sent to the US under the Safe Harbour may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the EU and the purposes for which it was transferred to the US. A majority of the US internet companies that appear to be more directly concerned by these programmes are certified under the Safe Harbour scheme.

As regards exchanges of data for law enforcement purposes, the existing Agreements (PNR, TFTP) have proven highly valuable tools to address common security threats linked to serious transnational crime and terrorism, whilst laying down safeguards that ensure a high level of data protection¹³. These safeguards extend to EU citizens, and the Agreements provide for mechanisms to review their implementation and to address issues of concern related thereto.

Against the backdrop of concerns raised in the EU about US surveillance programmes, the European Commission has used those mechanisms to check how the agreements are applied. In the case of the PNR Agreement, a joint review was conducted, involving data protection experts from the EU and the US, looking at how the Agreement has been implemented.¹⁴ That review did not give any indication that US surveillance programmes extend to or have any impact on the passenger data covered by the PNR Agreement. In the case of the TFTP Agreement, the Commission opened formal consultations after allegations were made of US intelligence agencies directly accessing personal data in the EU, contrary to the Agreement. Those consultations did not provide evidence of a breach of the TFTP Agreement, and they led the US to provide written assurance that no direct data collection has taken place contrary to the provisions of the Agreement.

The large-scale collection and processing of personal information under US surveillance programmes call, however, for very close attention by the EU to how the PNR and TFTP Agreements are implemented in practice. [*Text on PNR and TFTP to be completed after 18/11*].

Third, the increase in the volume of processing of personal data underlines the importance of the legal and administrative safeguards that apply. One of the goals of the Ad Hoc EU-US Working Group was to establish what safeguards apply to minimise the impact of the processing on the fundamental rights of EU citizens. Safeguards are also necessary to protect companies. Certain US laws such as the Patriot Act, enable US security authorities to directly request companies access to data stored in the EU. Therefore, European companies, and US companies present in the EU, may be required to transfer data to the US in breach of EU and Member States' laws, and companies are therefore caught between conflicting legal obligations. Legal uncertainty deriving from such direct requests may hold back the development of new digital services, such as cloud computing, which can provide efficient, lower-cost solutions for individuals and businesses.

3. ENSURING THE EFFECTIVENESS OF DATA PROTECTION

¹³ On the value of the TFTP for ..., see ... [Report on TFTP data for fighting terrorism...]

¹⁴ See COM ... [Report of joint review]

Transfers of personal data between the EU and the US are an essential component of the transatlantic commercial relationship. Information sharing is also an essential component of EU-US security cooperation, critically important to the common goal of preventing and combating serious crime and terrorism. However, recent revelations about US intelligence collection programmes have affected the trust on which this cooperation is based. In particular, it has affected trust in the way personal data is processed. The following steps should be taken to restore trust in data transfers for the benefit of the digital economy, security both in the EU and in the US, and the broader transatlantic relationship.

3.1. The EU data protection reform

The data protection reform proposed by the Commission in January 2012¹⁵ provides a key response as regards the protection of personal data. Four components of the proposed General Data Protection Regulation are of particular importance.

First, as regards territorial scope, the proposed regulation makes clear that companies that are not established in the Union will have to apply EU data protection law when they offer goods and services to European consumers or monitor their behaviour. In other words, the fundamental right to data protection will be respected, independently of the geographical location of a company or of its processing facility.¹⁶

Secondly, on international transfers, the proposed regulation establishes the conditions under which data can be transferred outside the EU. Transfers can only be allowed where these conditions, which safeguard the individuals' rights to a high level of protection, are met.¹⁷

Thirdly, concerning enforcement, the proposed rules provide for proportionate and dissuasive sanctions (up to 2% of a company's annual global turnover) to make sure that companies comply with EU law¹⁸. The existence of credible sanctions in place will increase companies' incentive to comply with EU law.

¹⁵ COM(2012) 10 final: Proposal for a Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25.1.2012, and COM(2012) 11 final: Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

¹⁶ The European Parliament confirmed and strengthened this important principle, enshrined in Art. 3 of the proposed Regulation, in its vote of 21 October 2013 on the data protection reform reports of MEPs Jan-Philipp Albrecht and Dimitrios Drouzas in the Committee for Civil Liberties, Justice and Home Affairs (LIBE).

¹⁷ In this regard, in its vote of 21 October 2013, the LIBE Committee of the European Parliament has proposed to include a provision in the future Regulation that would subject requests from foreign authorities to access personal data collected in the EU to the obtaining of a prior authorisation from a national data protection authority, where such a request would be issued outside a mutual legal assistance treaty or another international agreement.

¹⁸ In its vote of 21 October 2013, the LIBE Committee has proposed strengthening the Commission's proposal by providing that fines can go up to 5% of the annual worldwide turnover of a company.

Fourthly, the proposed regulation includes clear rules on the obligations and liabilities of data processors such as cloud providers, including on security¹⁹. As the revelations about US intelligence collection programmes have shown, this is critical because these programmes affect data stored in the cloud. Also, companies providing storage space in the cloud which are asked to provide personal data to foreign authorities will not be able to escape their responsibility by reference to their status as data processors rather than data controllers.

The proposed regulation is currently being discussed by the European Parliament and the Council.²⁰

3.2. Making Safe Harbour safer

The Safe Harbour scheme is an important component of the EU-US commercial relationship, relied upon by companies on both sides of the Atlantic.

The Commission's report on the functioning of Safe Harbour has identified a number of weaknesses in the scheme. As a result of a lack of transparency and of enforcement, some self-certified Safe Harbour members do not, in practice, comply with its principles. This has a negative impact on EU citizens' fundamental rights. It also creates a disadvantage for European companies competing with US companies operating under the scheme but in practice not applying its principles. This weakness also affects the majority of US companies which properly apply the scheme. Safe Harbour also acts as a conduit for the transfer of the personal data of EU citizens from the EU to the US by companies required to surrender data to US national security authorities under the US intelligence collection programmes. In its present form, it therefore constitutes a competitive disadvantage for EU business and a threat to the fundamental right to data protection of EU citizens.

The shortcomings of the Safe Harbour scheme have been underlined by the response of European Data Protection Authorities to the recent surveillance revelations. Article 3 of the Safe Harbour Decision authorises these authorities to suspend, under certain conditions, data flows to certified companies²¹. German data protection commissioners have decided not to issue new permissions for data transfers to non-EU countries (for example for the use of certain cloud services). They will also examine whether data transfers on the basis of the Safe

¹⁹ In its vote of 21 October 2013, the LIBE Committee has endorsed the strengthening of the obligations and liabilities of data processors, in the particular with regard to Art. 26 of the proposed Regulation.

²⁰ The Conclusions of the October 2013 European Council state that: "It is important to foster the trust of citizens and businesses in the digital economy. The timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015."

²¹ Specifically, pursuant to Art. 3 of the Safe Harbour Decision, such suspensions may take place in cases where there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond

Harbour should be suspended²². The risk is that such measures will create differences in coverage which will mean that Safe Harbour will cease to be a core mechanism for the transfer of personal data between the EU and the US.

The Commission has the authority under Directive 95/46/EC to suspend or revoke the Safe Harbour decision if the scheme no longer provides an adequate level of protection. Furthermore, Article 3 of the Safe Harbour Decision provides that the Commission may reverse, suspend or limit the scope of the decision, while, under article 4, it may adapt the decision at any time in the light of experience with its implementation.

Against this background, a number of policy options can be considered, including:

- Maintaining the *status quo*;
- Strengthening the Safe Harbour scheme and launching a review of its functioning;
- Suspending or revoking the Safe Harbour decision.

Given the weaknesses identified, the current implementation of Safe Harbour cannot be maintained. However, its revocation would adversely affect the interests of member companies in the EU and in the US. The Commission considers that Safe Harbour should rather be strengthened.

The changes should address both the structural shortcomings related to transparency and enforcement, the substantive Safe Harbour principles and the operation of the national security exception.

More specifically, for Safe Harbour to work as intended, the monitoring and supervision by US authorities of the compliance of certified companies with the Safe Harbour Privacy Principles needs to be more effective and systematic. The transparency of certified companies' privacy policies needs to be improved, including as regards the conditions applicable in cases of onward transfers and subcontracting of some of their processing activities (e.g. cloud computing services). The availability and affordability of dispute resolution mechanisms also needs to be ensured to EU citizens.

As a matter of urgency, the Commission will engage with the US authorities to discuss the shortcomings identified. Remedies should be identified by summer 2014 and implemented as soon as possible. This should be the first stage in a broader review process of the way in which Safe Harbour functions. Building on discussion with the US authorities, this process should be also involve open consultation and a debate in the European Parliament and the Council.

It is also important that the national security exception foreseen by the Safe Harbour Decision, is used only to an extent that is strictly necessary and proportionate.

3.3. Strengthening data protection safeguards in law enforcement cooperation

The EU and the US are currently negotiating a data protection "umbrella" agreement on transfers and processing of personal information in the context of police and judicial co-

²² Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, press release of 24 July 2013.

operation in criminal matters. The conclusion of such an agreement providing for a high level of protection of personal data would represent a major contribution to strengthening trust across the Atlantic. By advancing the protection of EU data citizens' rights, it would help strengthen transatlantic cooperation aimed at preventing and combating crime and terrorism.

According to the decision authorising the Commission to negotiate the umbrella agreement²³, the aim of the negotiations should be to ensure a high level of protection in line with the EU data protection *acquis*. This should be reflected in agreed rules and safeguards on, *inter alia*, how and for what purposes the data can be transferred and processed, the conditions and duration of the retention of the data. In the context of the negotiation, the Commission should also obtain commitments as to existence of enforceable rights including judicial redress mechanisms for EU citizens not resident in the US. Close EU-US cooperation to address common security challenges should be mirrored by efforts to ensure that citizens benefit from the same rights when the same data is processed for the same purposes on both sides of the Atlantic. It is also important that derogations based on national security needs are narrowly defined. Safeguards and limitations should be agreed in this respect.

In addition, these negotiations provide an opportunity to clarify that personal data held by private companies and located in the EU will not be accessed by or transferred to US law enforcement authorities outside of formal channels of co-operation, such as Mutual Legal Assistance agreements or sectorial EU-US Agreements authorising such transfers. Access by other means should be excluded, unless it takes place in clearly defined, exceptional and judicially reviewable situations. The agreement should contain or be accompanied by binding commitments in that regard.

An "umbrella agreement" agreed along those lines, should provide the general framework to ensure a high level of protection of personal data when transferred to the US for the purpose of preventing or combating crime and terrorism. Sectoral agreements should, where necessary due to the nature of the data transfer concerned, lay down additional rules and safeguards, building on the example of the EU-US PNR and TFTP Agreements, which set strict conditions for transfer of data and safeguards for EU citizens.

3.4. Addressing European concerns in the on-going US reform process

US President Obama has announced a review of US national security authorities' activities, including of the applicable legal framework. This on-going process provides an important opportunity to address EU concerns raised by recent revelations about US intelligence collection programmes. The most important changes would be extending the safeguards available to US citizens and residents to EU citizens not resident in the US, increased transparency of intelligence activities, and their oversight. Such changes would strengthen trust in EU-US data exchanges, and promote the use of Internet services by Europeans.

With respect to extending the safeguards available to US citizens and residents to EU citizens, legal standards in relation to US surveillance programmes which treat US and EU citizens differently should be reviewed, keeping in mind the close transatlantic security partnership

²³ See IP/10/1661 of 3 December 2010.

based on common values, rights and freedoms. This would reduce the extent to which Europeans are affected by US intelligence collection programmes.

More transparency is needed on the legal framework of US intelligence collection programmes and its interpretation by US Courts as well as on the quantitative dimension of US intelligence collection programmes. EU citizens would also benefit from such changes.

The oversight of US intelligence collection programmes would be improved by strengthening the role of the Foreign Intelligence Surveillance Court and by introducing remedies for individuals. These mechanisms could reduce the processing of personal data of Europeans that are not relevant for national security purposes.

3.5. Promoting privacy standards internationally

Issues raised by modern methods of data protection are not limited to data transfer between the EU and the US. A high level of protection of personal data should also be guaranteed at global level. EU rules on collection, processing and transfer of data should be promoted internationally.

Recently, a number of initiatives have been proposed to promote the protection of privacy, particularly on the internet²⁴. The EU should ensure that such initiatives, if pursued, fully take into account the principles of protecting fundamental rights, freedom of expression, personal data and privacy as set out in EU law and in the Joint EU Cyber Security Strategy, and do not undermine the freedom, openness and security of cyber space. This includes a democratic and efficient multi stakeholder governance model.

In view of promoting privacy standards internationally, accession to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), which is open to countries which are not member of the Council of Europe²⁵, should also be favoured. Safeguards and guarantees agreed in international fora should result in a high level of protection compatible with what is required under EU law.

The on-going reforms of data protection laws on both sides of the Atlantic also provide the EU and the US a unique opportunity to set the standard for global privacy rules. Data exchanges across the Atlantic and beyond would greatly benefit from the strengthening of the US domestic legal framework, including the passage of the "Consumer Privacy Bill of Rights" announced by President Obama in February 2012 as part of a comprehensive blueprint to improve consumers' privacy protections. The existence of a set of strong and enforceable data protection rules enshrined in both the EU and the US would constitute a solid basis for cross-border data flows.

4. CONCLUSIONS AND RECOMMENDATIONS

²⁴ See in this respect the draft resolution proposed to the UN General Assembly by Germany and Brazil – calling for the protection of privacy online as offline, including in the context of the surveillance of communications. This resolution discusses the proposal to adopt an additional protocol to Article 17 of the International Covenant on Civil and Political Rights (ICCPR).

²⁵ The US is already party to another Council of Europe convention: the 2001 Convention on Cybercrime (also known as the "Budapest Convention").

The issues identified in this Communication require action to be taken by the EU.

The concerns around transatlantic data exchanges are, first of all, a wake-up call for the EU and its Member States to advance swiftly and with ambition on the data protection reform. It shows that a strong legislative framework with clear rules that are enforceable also in situations when data are transferred abroad is, more than ever, a necessity. The EU institutions should therefore continue working towards the adoption of the EU data protection reform by spring 2014, to make sure that personal data is effectively and comprehensively protected.

Given the significance of transatlantic data flows, it is essential that the instruments on which these exchanges are based appropriately address the challenges and opportunities of the digital era. Existing and future arrangements and agreements should ensure that the continuity of a high level of protection is guaranteed over the Atlantic.

A robust Safe Harbour scheme is in the interests of EU and US citizens and companies. It should be strengthened by better monitoring and implementation in the short term, and, on this basis, by a broader review of its functioning. Changes are necessary to ensure that the original objectives of the Safe Harbour Decision – i.e. continuity of data protection, legal certainty and free EU-US flow of data – are still met.

These improvements should focus on the need for the US authorities to better supervise and monitor the compliance of self-certified companies with the Safe harbour Privacy Principles.

It is also important that the national security exception foreseen by the Safe Harbour Decision, is used only to an extent that is strictly necessary and proportionate.

In the area of law enforcement, the current negotiations of an “umbrella agreement” should result in a high level of protection for citizens on both sides of the Atlantic. Such an agreement would strengthen the trust of Europeans in EU-US data exchanges, and provide a basis to further develop EU-US security cooperation and partnership. In the context of the negotiation, commitments should be secured to the effect that procedural safeguards, including judicial redress, are available to Europeans who are not resident in the US.

Commitments should be sought from the US administration to ensure that personal data held by private entities in the EU will not be accessed by law enforcement agencies outside of formal channels of co-operation, such as Mutual Legal Assistance agreements and sectorial EU-US Agreements such as PNR and TFTP authorising such transfers under strict conditions, except in clearly defined, exceptional and judicially reviewable situations.

The EU should also make the case for extending the safeguards available to US citizens and residents to EU citizens not resident in the US, greater transparency and oversight in the legal framework applicable to US national security authorities.

Areas listed in this communication will require constructive engagement from both sides of the Atlantic. Together, as strategic partners, the EU and the US have the ability to overcome this crisis and rebuild trust. Developing joint political and legal commitments on further cooperation in these areas will strengthen the overall transatlantic relationship.

Dokument 2014/0067396

Von: .BRUEEU POL-IN2-2-EU Eickelpasch, Joerg <pol-in2-2-eu@brue.auswaertiges-amt.de>
Gesendet: Freitag, 22. November 2013 13:44
An: Weinbrenner, Ulrich; Peters, Reinhard; Stentzel, Rainer, Dr.; Spitzer, Patrick, Dr.
Cc: 't.pohl@diplo.de'
Betreff: AW: sehr vertraulich - KOM-Entwurf Mitteilung "rebuilding trust in EU-US data flows"
Anlagen: 131121 ANNEX Joint Report.doc

Anbei ergänzend noch die Anlage „Joint report zum TFTP-Abkommens“.
Viele Grüße,
Jörg Eickelpasch

Von: .BRUEEU POL-IN2-2-EU Eickelpasch, Joerg
Gesendet: Donnerstag, 21. November 2013 12:17
An: Weinbrenner, Ulrich; 'reinhard.peters@bmi.bund.de'; Rainer.Stentzel@bmi.bund.de; 'patrick.spitzer@bmi.bund.de'
Cc: 't.pohl@diplo.de'
Betreff: sehr vertraulich - KOM-Entwurf Mitteilung "rebuilding trust in EU-US data flows"
Wichtigkeit: Hoch

Bitte vertraulich behandeln, um unsere Quelle zu schützen. KOM will die Mitteilung am 27.11.2013 veröffentlichen.
Viele Grüße,
Jörg Eickelpasch

Bl. 177-192

Entnahme wegen fehlenden Bezugs zum
Untersuchungsgegenstand

Von: Kotira, Jan
Gesendet: Mittwoch, 27. November 2013 09:40
An: Weinbrenner, Ulrich; Stöber, Karlheinz, Dr.; Spitzer, Patrick, Dr.;
Jergl,
Johann; Schäfer, Ulrike; Richter, Annegret
Betreff: WG: 16:29 (Zusammenfassung 1630) EU fordert von USA konkrete
Taten für
mehr Datenschutz

-----Ursprüngliche Nachricht-----

Von: IDD, Platz 2
Gesendet: Dienstag, 26. November 2013 16:32
An: PGNSA
Cc: IDD, Platz 3
Betreff: dpa: 16:29 (Zusammenfassung 1630) EU fordert von USA konkrete
Taten
für mehr Datenschutz

bdt0525 3 pl 630 dpa 1165

EU/USA/Geheimdienste/
(Zusammenfassung 1630)
EU fordert von USA konkrete Taten für mehr Datenschutz =

Das Vertrauen der EU in die USA ist seit der NSA-Affäre geschwunden.
Nun versuchen US-Abgeordnete, die Wogen zu glätten. Bei ihrem Besuch in
Brüssel bekamen die Amerikaner von EU-Kommissaren und Abgeordneten eine
Menge
Forderungen zu hören: Auf Worte müssten Taten folgen.

Brüssel (dpa) - Nach der NSA-Affäre fordert die EU-Kommission von den
USA
konkrete Schritte für einen besseren Datenschutz. Beim Besuch einer US-
Delegation am Dienstag in Brüssel bekräftigte EU-Justizkommissarin
Viviane
Reding ihre Forderung, dass Europäer in den USA gleiche Datenschutzrechte
haben müssten wie Amerikaner in Europa. In Bereichen, wo es bereits
Abkommen
gebe, hielten sich die Amerikaner schon heute daran.

Die EU will durch neue Vereinbarungen die USA zu einem sorgsameren
Umgang
mit Daten bringen. Das Ziel laute, bis kommenden Sommer ein umfassendes
Abkommen zum Datenschutz bei der transatlantischen Zusammenarbeit von
Polizei
und Justiz zu erreichen, sagte Reding.
Dafür müssten die USA die notwendigen Gesetzesänderungen «eher früher als
später» vornehmen. Die EU-Kommissarin betonte: «Ich hoffe, dass Worte
jetzt zu
Taten werden.»

Trotz heftiger Kritik stellt die EU-Kommission die bestehenden
Datenschutzabkommen mit den USA nicht infrage. In der Praxis halte
Amerika
beim Zugriff auf Daten europäischer Bankkunden und Fluggäste die mit den
Europäern geschlossenen Vereinbarungen ein. Zu diesem Ergebnis kommt die
EU-
Behörde in einem Bericht, der am Mittwoch (27.) veröffentlicht wird. Das

verlautete aus Kommissionskreisen. Die Prüfung habe «keinen Hinweise auf einen Rechtsbruch» ergeben.

Die EU-Kommission hält auch an der «Safe Harbor»-Vereinbarung mit den USA fest. Diese erlaubt es Unternehmen, personenbezogene Daten von EU-Bürgern legal in die USA zu übermitteln - obwohl die USA kein dem EU-Datenschutz vergleichbares Niveau haben. Allerdings empfiehlt Brüssel bis Sommer 2014 mehr als ein Dutzend Verbesserungsvorschläge. Grundlage für «Safe-Harbor» sind Selbstverpflichtungen von US-Firmen, Standards beim Datenschutz zu beachten. Reding nannte «Safe Harbor» im Sommer «eher ein Schlupfloch denn eine Absicherung unserer Bürger.»

Aus dem Europaparlament gibt es immer wieder Forderungen, die Abkommen mit den USA zu kündigen. Die SPD-Europaabgeordnete Birgit Sippel kritisierte am Dienstag den «Kuschelkurs der EU-Kommission» gegenüber den USA. «Die EU-Kommission übt sich in diplomatischen Verrenkungen statt klare Worte zu finden», schrieb Sippel.

Die US-Abgeordneten um den demokratischen Senator Chris Murphy bemühten sich bei ihrem Besuch um Schadensbegrenzung in der Affäre und trafen auch Europaabgeordneten. Der CDU-Europaparlamentarier Axel Voss sagte danach: «Es ist eine kleine Beruhigung eingetreten, weil wir das Gefühl haben, die Amerikaner haben Interesse, zu einer gemeinsamen Lösung zu kommen.» Man habe klar gemacht, dass gewisse Standards beim Datenschutz unbedingt eingehalten werden müssten.

Auch Kommissarin Reding sprach von einer Annäherung: «Wir reden und hören einander zu - wir spähen uns nicht gegenseitig aus.»

Schon im Sommer war bekanntgeworden, dass der Geheimdienst NSA die EU intern als Spionageziel führt und EU-Einrichtungen ausspioniert. Zudem soll die NSA mit dem US-Spionageprogramm «PRISM» massenhaft Daten von Internetnutzern bei Unternehmen wie Google, Facebook, Apple und Yahoo gesammelt haben.

Die EU pocht seit Jahren auf mehr Datenschutz, so erlaubt das Swift-Abkommen seit 2010 US-Terrorfahndern Einblick in Kontobewegungen von Verdächtigen - aber nur unter strengen Auflagen. Bei Flügen müssen Europas Fluglinien für alle Verbindungen in und aus den USA 19 Daten von EU-Bürgern an US-Behörden weiterleiten.

Die US-Delegation hatte am Montag bereits in Berlin politische Gespräche geführt und sich um eine Annäherung bemüht.

dpa-Notizblock

Internet

- [Text des Swift-Abkommens] (<http://dpaq.de/uOQ3g> und <http://dpaq.de/sQM4y>)
- [Text des Abkommens EU-USA zur Weitergabe von Passagierdaten] (<http://dpaq.de/Twa3k>)
- [EU-Kommission zum neu ausgehandelten Abkommen] (<http://dpaq.de/qcmt9>)
- [EU-Kommission zu Safe Harbor 26.7.2000] (<http://dpaq.de/XSkqL>)
- [US-Handelsministerium zu Safe Harbor - Englisch] (<http://dpaq.de/FHi19>)
- [EU-Datenschutzrichtlinie vom 24.10.1995] (<http://dpaq.de/iLxTP>)

Orte

- [EU-Kommission] (Rue de la Loi 200, 1049 Brüssel, Belgien)
- [EU-Parlament] (Rue Wiertz, B-1047 Brüssel, Belgien)

* * * *

Die folgenden Informationen sind nicht zur Veröffentlichung bestimmt

dpa-Kontakte

- Autorin: Marion Trimborn, +32 2 2303691, <trimborn.marion@dpa.com>
- Redaktion: Thomas Cronenberg, +49 30 2852 31302, <politik-ausland@dpa.com>

dpa mt xx z2 cro

261629 Nov 13

Dokument 2013/0519987

Von: OESI3AG_
Gesendet: Mittwoch, 27. November 2013 10:46
An: BMJ Bader, Jochen; BK Rensmann, Michael; AA Oelfke, Christian; AA Kinder, Kristin; AA Wendel, Philipp; BMWI Scholl, Kirsten; BMJ Henrichs, Christoph; BMWI Smend, Joachim; BMWI BUERO-EA2; BK Wolff, Philipp; BMJ Harms, Katharina; OESIII1_; Bender, Ulrike; Riemer, André
Cc: Jergl, Johann; Stöber, Karlheinz, Dr.; PGDS_; Stentzel, Rainer, Dr.; VI4_; IT1_; OESI3AG_; Weinbrenner, Ulrich; RegOeSI3; 'ref601@bk.bund.de'
Betreff: WG: Sitzung JI-Referenten am 29.11.2013 um 10 Uhr: EU-Beitrag zu US-review von Überwachungsprogrammen
Anlagen: CM05465.EN13.DOC; ST16824 EN13.doc

ÖS I 3 - 52001/1#9

Liebe Kolleginnen und Kollegen,

die als Anlage beigefügte vorläufige TO für die Sitzung der JI-Referenten am kommenden Freitag (29.11.) sowie das zugehörige Vorbereitungspapier der Präsidentschaft ("EU contribution in the context of the US review of surveillance programmes") übersende ich zunächst zK. Ich werde mit einem Weisungsentwurf zur Abstimmung kurzfristig auf Sie zukommen. Darüber hinaus bitte ich um einen kurzen Hinweis, wenn aus Ihrer Sicht weitere Adressaten bei der Abstimmung berücksichtigt werden sollten.

Freundliche Grüße

Patrick Spitzer

im Auftrag
Dr. Patrick Spitzer

Bundesministerium des Innern
Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,
BKA-Gesetz, Datenschutz im Sicherheitsbereich)
Alt-Moabit 101D, 10559 Berlin
Telefon: +49 (0)30 18681-1390
E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?



**COUNCIL OF
THE EUROPEAN UNION**
GENERAL SECRETARIAT

Brussels, 26 November 2013

CM 5465/13

**JAI
DATAPROTECT**

COMMUNICATION

NOTICE OF MEETING AND PROVISIONAL AGENDA

Contact: guy.stessens@consilium.europa.eu
Tel.: + 32.2-281.67.11 (secr.: + 32.2-281.75.97)

Subject: **JHA Counsellors meeting**
Date: Friday 29 November 2013 at 10h00
Venue: COUNCIL
 JUSTUS LIPSIUS BUILDING
 Rue de la Loi 175, 1048 Brussels

1. **Adoption of the agenda**

2. **EU contribution in the context of the US review of surveillance programmes**
 16824/13 JAI 1066 USA 59 RELEX 1069 DATAPROTECT 182 COTER 147
 RESTREINT UE/EU RESTRICTED

3. **Any other business**

NB: To reduce costs, only documents produced in the week preceding the meeting will be

available in the meeting room.



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 26 November 2013

16824/13

RESTREINT UE/EU RESTRICTED

**JAI 1066
USA 59
RELEX 1069
DATAPROTECT 182
COTER 147**

NOTE

from : Presidency
to : JHA Counsellors/COREPER

Subject : EU contribution in the context of the US review of surveillance programmes

As announced in COREPER on 14 November 2013 and as a response to repeated requests by the US side in the EU-US Ad Hoc Working Group on Data Protection, the Presidency herewith circulates a draft non-paper with suggestions on how the concerns of the EU and its Member States could be addressed in the context of the ongoing US review of surveillance programmes. This non-paper will be discussed by JHA counsellors, and a revised version will be submitted to COREPER for approval. The US side stressed the urgency of receiving the EU input. The finalized paper will be handed over to US authorities by the EU delegation in Washington. It could also be used for further outreach, as appropriate.

EU contribution in the context of the US review of surveillance programmes

The EU and the US are strategic partners. This relationship is critical for our security, the promotion of our shared values, and our common leadership in world affairs. Since 9/11 and subsequent terrorist attacks in Europe, the EU, its Member States, and the US have stepped up cooperation in the police, criminal justice and security sectors. Sharing relevant information, including personal data, is an essential element of this relationship. This requires trust between governments and from citizens on both sides.

Concerns have been expressed at both EU and Member State level at revelations of large-scale US intelligence collection programmes, in particular as regards the protection of personal data of Europeans. If citizens are concerned about the surveillance of their personal data by intelligence agencies when using Internet services and in the context of large-scale processing of their data by private companies, this may affect their trust in the digital economy, with potential negative consequences on growth.

The EU welcomes President Obama's launch of a review on US surveillance programmes. It is good to know that the Administration has recognised that the rights of Europeans deserve special attention in the context of this review, as Attorney-General Eric Holder has stated: "The concerns we have here are not only with American citizens. I hope that the people in Europe will hear this, people who are members of the EU, nations of the members of the EU. Our concerns go to their privacy as well."

Under US law, EU citizens who are not resident in the US do not benefit from the same privacy rights and safeguards as US persons. Different rules apply, including as regards surveillance and data stored in the US.

This contrasts with European law, under which US citizens (residents or not) enjoy the same privacy protections as European citizens, including the right to seek judicial redress in all Member States up to the European Court of Human Rights.

The EU appreciates the discussions which took place in the EU-US ad hoc working group. The EU welcomes the invitation expressed by the US side in this dialogue to provide input on how its concerns could be addressed in the context of the US review.

EU citizens not resident in the US would benefit from stronger general rules on transparency, additional safeguards on necessity and proportionality, and effective remedies in cases of abuse. In addition, specific safeguards should be introduced to reduce the risk of large-scale collection of data of EU citizens which is not necessary for foreign intelligence purposes.

The following points could be considered in the review in order to address some of the concerns:

1. Privacy rights of non-US persons

The review could lead to the recognition of data protection and privacy rights for non-US persons, including EU citizens non-resident in the US. This is particularly important in cases where their data is stored inside the US.

2. Scope, necessity, and proportionality of the programmes

In order to address concerns with regard to the scope of the programmes, it is important that the proportionality principle is respected with regard to the collection of and access to the data.

The definition of "foreign intelligence information" in US law includes broad categories such as "conduct of the foreign affairs of the US" and establishes different standards for US and non-US persons: With regard to US persons, the information has to be "necessary", while with regard to non-US persons, it is enough if the information is "relevant" to achieve a foreign intelligence purpose.

In the context of the review, the US could consider extending the "necessity" standard, which is crucial to respect of the proportionality principle, to non-US persons.

The review should include an assessment of whether the collection of data is truly necessary and proportionate, and **recommend strict procedures to minimize the collection and processing of data** that is not necessary and proportionate for legitimate foreign intelligence purposes, including data of non-resident EU citizens. In line with US law, current targeting and minimization procedures are designed to protect the privacy of US persons only. Among other things, the US could consider strict maximum retention periods applicable to the data of non-US persons.

The introduction of such requirements would extend the benefit of the US oversight system to non-US persons.

3. Remedies

The review should also consider how European citizens not resident in the US can benefit from oversight and have remedies available to them to ensure that their personal data has not been collected illegally or mishandled. This could include different forms of administrative or judicial redress; for example, the appointment of an Ombudsman or a mediator who could review individual complaints and verify, in relation with relevant oversight authorities within the executive branch, whether US laws have been respected in the cases that were submitted to him.

4. Transparency

De-classification should continue and programmes should be explained to the maximum extent possible without prejudice to the security of the US. Further facts and figures could be published that would help citizens better assess the scope of the programmes.

Companies could be authorized to publish not only the number of government requests related to national security, but also the amount of data submitted and the number of customers concerned.

Dokument 2013/0519970

Von: Spitzer, Patrick, Dr.
Gesendet: Freitag, 29. November 2013 11:11
An: PGDS_; VI4_; IT1_; OESIII1_; 'ref601@bk.bund.de'; 'ref132@bk.bund.de'; BMWI BUERO-EA2; AA Oelfke, Christian; AA Kinder, Kristin; AA Wendel, Philipp
Cc: BMWI Bölhoff, Corinna; BMJ Henrichs, Christoph; BMJ Harms, Katharina; BK Rensmann, Michael; BK Wolff, Philipp; BMWI Scholl, Kirsten; Bender, Ulrike; Merz, Jürgen; Riemer, André; Schlender, Katharina; Marscholleck, Dietmar; OESI3AG_; Jergl, Johann; Stöber, Karlheinz, Dr.; Weinbrenner, Ulrich; OESII2_; Peters, Reinhard; RegOeSI3
Betreff: Sitzung JI-Referenten am 29.11.2013 um 10 Uhr: EU-Beitrag zu US-review von Überwachungsprogrammen; Weisung (finale Fassung)
Anlagen: 131129__Weisung_JI_Empfehlungenl-fin.doc

ÖS I 3 - 52001/1#9

Liebe Kolleginnen und Kollegen,

anbei übersende ich die finalisierte Fassung der Weisung für das Treffen der JI-Referenten. Für Ihre Unterstützung möchte ich mich bedanken.

Freundliche Grüße

Patrick Spitzer

im Auftrag
 Dr. Patrick Spitzer

Bundesministerium des Innern
 Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,
 BKA-Gesetz, Datenschutz im Sicherheitsbereich)
 Alt-Moabit 101D, 10559 Berlin
 Telefon: +49 (0)30 18681-1390
 E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

Von: Spitzer, Patrick, Dr.
Gesendet: Donnerstag, 28. November 2013 19:41
An: PGDS_; VI4_; IT1_; OESIII1_; 'ref601@bk.bund.de'; 'ref132@bk.bund.de'; BMWI BUERO-EA2; AA Oelfke, Christian; AA Kinder, Kristin; AA Wendel, Philipp
Cc: BMWI Bölhoff, Corinna; BMJ Henrichs, Christoph; BMJ Harms, Katharina; BK Rensmann, Michael; BK Wolff, Philipp; BMWI Scholl, Kirsten; Bender, Ulrike; Merz, Jürgen; Riemer, André; Schlender, Katharina; Marscholleck, Dietmar; OESI3AG_; Jergl, Johann; Stöber, Karlheinz, Dr.; Weinbrenner, Ulrich; OESII2_; Peters, Reinhard
Betreff: WG: Sitzung JI-Referenten am 29.11.2013 um 10 Uhr: EU-Beitrag zu US-review von

Überwachungsprogrammen; Weisung
Wichtigkeit: Hoch

ÖS I 3 - 52001/1#9

Liebe Kolleginnen und Kollegen,

herzlichen Dank für Ihre Anmerkungen zur Weisung für die morgige Sitzung. Als Anlage übersende ich eine überarbeitete Version des Dokuments (wegen der Vielzahl der Änderungswünsche nicht im Änderungsmodus). Neu hinzugekommen ist eine Vorschlag für eine weitere Empfehlung (Ziff. 5), die die Achtung der jeweiligen nationalen Rechtsordnungen der MS zum Gegenstand hat (Formulierungsvorschlag anbei). Darüber hinaus wurde nunmehr durchgängig auf „EU residents“ anstelle von „non-US persons“ umgestellt. Aus Sicht von BMI sind darüber hinaus auch die aufgeworfenen kompetenzrechtliche Fragen noch nicht beantwortet (siehe Weisungstext).

Ich möchte Sie bitten, mir weitere Änderungswünsche bis morgen **29.11., 09.00 Uhr (Verschweigen)** mitzuteilen.

Herzlichen Dank für Ihre Unterstützung und freundliche Grüße

Patrick Spitzer

im Auftrag
Dr. Patrick Spitzer

Bundesministerium des Innern
Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,
BKA-Gesetz, Datenschutz im Sicherheitsbereich)
Alt-Moabit 101D, 10559 Berlin
Telefon: +49 (0)30 18681-1390
E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

Von: Spitzer, Patrick, Dr.

Gesendet: Donnerstag, 28. November 2013 11:26

An: PGDS_; VI4_; IT1_; OESIII1_; 'ref601@bk.bund.de'; 'ref132@bk.bund.de'; BMWI BUERO-EA2; AA Oelfke, Christian; AA Kinder, Kristin; AA Wendel, Philipp

Cc: BMWI Bölhoff, Corinna; BMJ Henrichs, Christoph; BMJ Harms, Katharina; BK Rensmann, Michael; BK Wolff, Philipp; BMWI Scholl, Kirsten; Bender, Ulrike; Merz, Jürgen; Riemer, André; Schlender, Katharina; Marscholleck, Dietmar; OESI3AG_; Jergl, Johann; Stöber, Karlheinz, Dr.; Weinbrenner, Ulrich; Eickelpasch, Jörg

Betreff: Sitzung JI-Referenten am 29.11.2013 um 10 Uhr: EU-Beitrag zu US-review von Überwachungsprogrammen; Weisung

Wichtigkeit: Hoch

ÖS I 3 - 52001/1#9

Liebe Kolleginnen und Kollegen,

als Anlage übermittele ich – wie angekündigt – den Weisungsentwurf für den morgigen Sitzung der JI-Referenten zum Thema „EU contribution in the context of the US review of surveillance programmes“. Die Bezugsdokumente habe ich der Vollständigkeit halber ebenfalls noch einmal beigelegt.

Ich bitte um Mitzeichnung (gerne mit weiteren Vorschlägen zur Ergänzung/Änderung des Bezugsdokumentes) bis heute, **28. November, 15.00 Uhr**.

Freundliche Grüße

Patrick Spitzer

im Auftrag
Dr. Patrick Spitzer

Bundesministerium des Innern
Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,
BKA-Gesetz, Datenschutz im Sicherheitsbereich)
Alt-Moabit 101D, 10559 Berlin
Telefon: +49 (0)30 18681-1390
E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

Von: OESI3AG_

Gesendet: Mittwoch, 27. November 2013 10:46

An: BMJ Bader, Jochen; BK Rensmann, Michael; AA Oelfke, Christian; AA Kinder, Kristin; AA Wendel, Philipp; BMWI Scholl, Kirsten;; BMWI Smend, Joachim; BMWI BUERO-EA2; BK Wolff, Philipp; BMJ Harms, Katharina; OESIII1_; Bender, Ulrike; Riemer, André

Cc: Jergl, Johann; Stöber, Karlheinz, Dr.; PGDS_; Stentzel, Rainer, Dr.; VI4_; IT1_; OESI3AG_; Weinbrenner, Ulrich; RegOeSI3; 'ref601@bk.bund.de'

Betreff: WG: Sitzung JI-Referenten am 29.11.2013 um 10 Uhr: EU-Beitrag zu US-review von Überwachungsprogrammen

ÖS I 3 - 52001/1#9

Liebe Kolleginnen und Kollegen,

die als Anlage beigelegte vorläufige TO für die Sitzung der JI-Referenten am kommenden Freitag (29.11.) sowie das zugehörige Vorbereitungspapier der Präsidentschaft ("EU contribution in the context of the US review of surveillance programmes") übersende ich zunächst zK. Ich werde mit einem Weisungsentwurf zur Abstimmung kurzfristig auf Sie zukommen. Darüber hinaus bitte ich um einen kurzen Hinweis, wenn aus Ihrer Sicht weitere Adressaten bei der Abstimmung berücksichtigt werden sollten.

Freundliche Grüße

Patrick Spitzer

im Auftrag
Dr. Patrick Spitzer

Bundesministerium des Innern
Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,
BKA-Gesetz, Datenschutz im Sicherheitsbereich)
Alt-Moabit 101D, 10559 Berlin
Telefon: +49 (0)30 18681-1390
E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

BMI – AG ÖS I 3

Berlin, den 27.11.2013

Bearbeiter: Dr. Spitzer

Sitzung der JI-Referenten am 29. November 2013

TOP EU contribution in the context of the US review of surveillance programmes

Dok. 16824/13

1. Ziel des Vorsitzes

- Diskussion des **Dok. Nr. 16824/13** mit inhaltlichen Vorschlägen zur Einbringung in die laufende interne Untersuchung der US-Überwachungsprogramme.

2. Deutsches Verhandlungsziel / Weisungstenor

- **Grundsätzliche Zustimmung** zur Ausarbeitung eines politischen Positionspapiers unter Wahrung der unionsvertraglichen Kompetenzverteilung. Hierzu ist kurzfristig zu klären, ob die vorliegenden Empfehlungen kompetenzrechtlich „durch die EU“ abgegeben werden können oder alternativ durch „die im Rat der Europäischen Union vereinigten Vertreter der Mitgliedstaaten“. **Im Hinblick hierauf wird ein Prüfvorbehalt eingelegt. Eine Klärung sollte kurzfristig durch das Ratssekretariat erfolgen.**
- Dokument bedarf einer grundlegenden **Überarbeitung**. **Inhaltlich muss die zentrale Forderung** zum einen sein, dass allgemein der **Grundsatz der Verhältnismäßigkeit (Proportionality)** bei allen Maßnahmen der US-Geheimdienste gewahrt wird. Dies gilt unabhängig davon, ob US- oder EU-Bürger betroffen sind. **Vorbehaltlich der auch insoweit noch zu klärenden Frage nach der Reichweite der Kompetenz der EU** muss für alle Betroffenen, also auch für EU-Bürger, in gleicher Weise effektiver Rechtsschutz gewährleistet sein. Der Text muss in diesem Sinne durchgehend überarbeitet werden.
- Inhaltliche Änderungen im Einzelnen:
 - S. 2, 2. Absatz Satz 1: Ersetze „revelations of“ durch „media reports about“, da Einzelheiten nach wie vor unbekannt sind.
 - S. 2, 4. Absatz: Ersetzung von „EU citizens who are not resident in the US“ durch „EU residents“.
 - S. 3, 3. Absatz Satz 1: Ersetzung von „EU citizens not resident in the US“ durch „EU residents“
 - S. 3, 3. Absatz Satz 2: Ersetzung von „EU citizens“ durch „EU residents“.
 - S. 3 Ziffer 1 (Überschrift): Ersetzung von „non US-persons“ durch „EU residents“

- S.3, Ziff. 1, Satz 1: **Konkretisierung**. Es wird nicht deutlich welche Empfehlung abgegeben werden soll. Statt „could“ sollte hier „should“ verwendet werden.
- S.3, Ziff. 1, Satz 1: Bitte um Erläuterung, warum neben „privacy rights“ hier „data protection“ aufgeführt wird (ansonsten aber nur auf „privacy rights“) abgestellt wird.
- S. 3 Ziffer 1: Ersetzung von „non US-persons“ durch „EU residents“
- S. 4, 1. Absatz: Ersetzung von „non US-persons“ durch „EU residents“
- S. 4, 2. Absatz, Satz 1: Ersetzung von „non resident EU citizens“ durch „EU residents“
- S. 4, 2. Absatz, Satz 3 am Ende: Ersetzung von „non US-persons“ durch „EU residents“
- S. 4, 3. Absatz: Ersetzung von „non US-persons“ durch „EU residents“
- S. 4, 4. Absatz: Ersetzung von „European citizens not resident in the US“ durch „EU residents“.
- DEU legt im Übrigen Prüfvorbehalt ein und behält sich weitere Änderungsvorschläge vor.

3. Sprechpunkte

- **Dank** für die Ausarbeitung der Empfehlungen. DEU ist der Ansicht, dass das Angebot der US-Seite, sich in den US-internen Prozess einzubringen, wahrgenommen werden sollte. Hierbei kann es – u.a. wegen des nur teilweise aufgeklärten Sachverhalts – nur um **Empfehlungen allgemeiner Art** gehen. Diese sollten – auch vor dem zeitlichen Hintergrund der US-Untersuchung – möglichst klar formuliert sein.
- Das hierzu vorliegende Dokument wird diesem Anspruch nur teilweise gerecht und bedarf einer grundsätzlichen **Überarbeitung**.
- DEU legt zunächst Prüfvorbehalt ein. Es sollten aber mindestens folgende **Änderungen** aus Sicht von DEU vorgenommen werden (s.o.).
- Bitte um Darstellung des **weiteren Verfahrens**. Es bestehen **Zweifel**, ob die vorliegenden Empfehlungen kompetenzrechtlich „durch die EU“ abgegeben werden können oder alternativ durch „die im Rat der Europäischen Union vereinigten Vertreter der Mitgliedstaaten“. Das Ratssekretariat sollte hierzu kurzfristig eine Prüfung einleiten.
- **Klarstellung**, dass etwaige follow-up Maßnahmen, reziproke Empfehlungen der USA o.ä. alleine an die Adresse der MS zu richten sind, da nur so die kompetenzrechtliche Aufteilung trennscharf abgebildet werden kann.

4. Ergänzende Erläuterungen zur Kompetenzfrage

Kompetenzrechtlich ist festzuhalten, dass EU nachrichtendienstliche Fragestellungen der MS nicht regeln darf. Es sollte schon der Anschein vermieden werden, die Tätigkeit der Nachrichtendienste der MS werde durch europäisches Primär- oder Sekundärrecht erfasst. Das gilt auch, wenn die EU – wie hier - auf dem Gebiet der Außenbeziehungen oder des Datenschutzes tätig wird (keine „Annexregelung“). Der Vollständigkeit halber bleibt anzumerken, dass weder die Union noch ihre MS eine

Zuständigkeit für die Regelung der nachrichtendienstlichen Tätigkeit von Drittstaaten reklamieren können.

Allerdings liegt – nach dem Prinzip der begrenzten Einzelermächtigung und mangels anderweitiger Regelung in den Verträgen - die Zuständigkeit für die nachrichtendienstliche Zusammenarbeit mit Drittstaaten ebenfalls bei den MS. Die Union besitzt zwar eine recht umfassende Zuständigkeit für den Datenschutz. Insofern kann unionsrechtlich geregelt werden, unter welchen Voraussetzungen natürliche und juristische Personen personenbezogene Daten an Stellen in Drittstaaten übermittelt werden dürfen. Deshalb mag man der Union ein Aufklärungsinteresse daran zugestehen, ob unionsrechtlich verlangte Voraussetzungen für diese Datenübermittlung durch Maßnahmen von/in Drittstaaten ausgehebelt werden. Eine Zuständigkeit für nachrichtendienstliche Tätigkeiten ergibt sich hieraus jedoch weder mit Blick auf EU-MS noch mit Blick auf Drittstaaten.

ÖS-9370/13

Arbeitsgruppe ÖS I 3

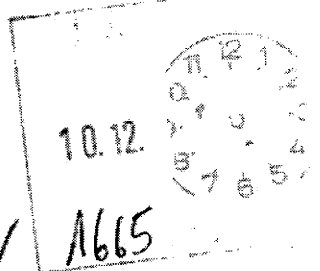
Berlin, den 2. Dezember 2013

ÖS I 3 - 52001/1#9 52000/3#2

Hausruf: -1390

AGL: MinR Weinbrenner
AGM: MinR Taube
Ref.: RR Dr. Spitzer

3. in Schema und
zum Vergleich
ÖS I 3 5200/3#2
Sp 2/01



PKDFIV

~~Antrag an ÖS I 3, um
Antrag ABT, zu nach-
nehmen.~~

Herrn Minister

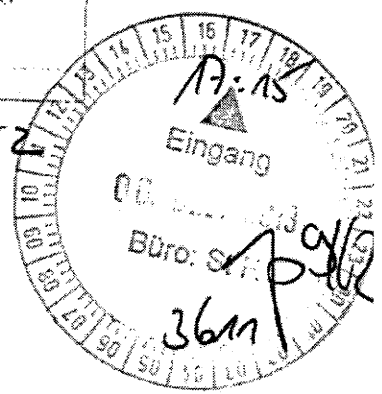
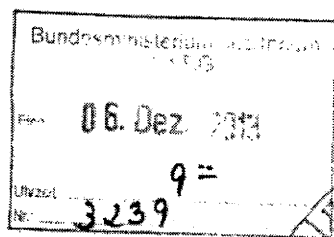
[Handwritten signature]

~~Abdruck: *[Handwritten]* elektr. versendet~~

über

P St S, LLS, AL B, Presse

- Herrn Staatssekretär Fritsche
- Frau Staatssekretärin Rogall-Grothe
- Herrn AL ÖS *[Handwritten]*
- Herrn AL V *[Handwritten]*
- Herrn UAL ÖS I *[Handwritten]*
- Herrn UAL VII *[Handwritten]*



[Handwritten:] sowie GII 1 und GII 2
zugeleitet und

PG DS sowie Referate ÖS II 1, B 2 und VI 4 haben mitgezeichnet.

Betr.: EU-Position zu Überwachungsprogrammen der NSA sowie zum PNR-
Abkommen

Anlagen: - 6 -

[Handwritten:] Dr. Spitzer
Witz

1. **Votum**
Kenntnisnahme

2. **Sachverhalt/Stellungnahme:**

Am 27. November 2013 hat KOM folgende Berichte vorgelegt:

- Feststellungen der "ad hoc EU-US working group on data protection" (Anlage 1); hierauf aufbauend befindet sich zurzeit ein „Empfeh-

lungspapier“ zur Einbringung in die laufende US-interne Evaluierung der Überwachungsprogramme in der Abstimmung (Anlage 2);

- **Strategiepapier über transatlantische Datenströme** (Anlage 3);
- Analyse des Funktionierens des **Safe-Harbor-Abkommens** (Anlage 4);
- Bericht über das **TFTP-Abkommen** (auch SWIFT-Abkommen genannt; Anlage 5)

Darüber hinaus hat KOM am 27. November 2013 ihren Bericht über die 1. **turnusmäßige Überprüfung der Durchführung des geltenden PNR-Abkommens zwischen der EU und den USA** (Anlage 6) vorgelegt, das am 1. Juli 2012 in Kraft getreten war (gem. Art. 23 des Abkommens überprüfen die Parteien die Durchführung des Abkommens ein Jahr nach Inkrafttreten und danach regelmäßig).

Zu den einzelnen Berichten:

- a) **Abschlussbericht der „ad hoc EU-US working group on data protection“ und Empfehlungen für die US-interne Evaluierung der Überwachungsprogramme**

Die „ad hoc EU US working group on data protection“ der KOM (DEU-Vertreter: UAL ÖS I Peters; „Working Group“) wurde im Juli 2013 eingerichtet, um „datenschutzrechtliche Fragestellungen im Hinblick auf personenbezogene Daten von EU-Bürgern, die von den US-Überwachungsprogrammen betroffen sind“, zu erörtern. Sie hat sich von Juli bis November 2013 insgesamt vier Mal in Brüssel und in Washington getroffen. Der Abschlussbericht der KOM (Anlage 1) beschränkt sich iW auf die Darstellung der US-Rechtslage (insbes. sec. 702 FISA, sec. 215 Patriot Act).

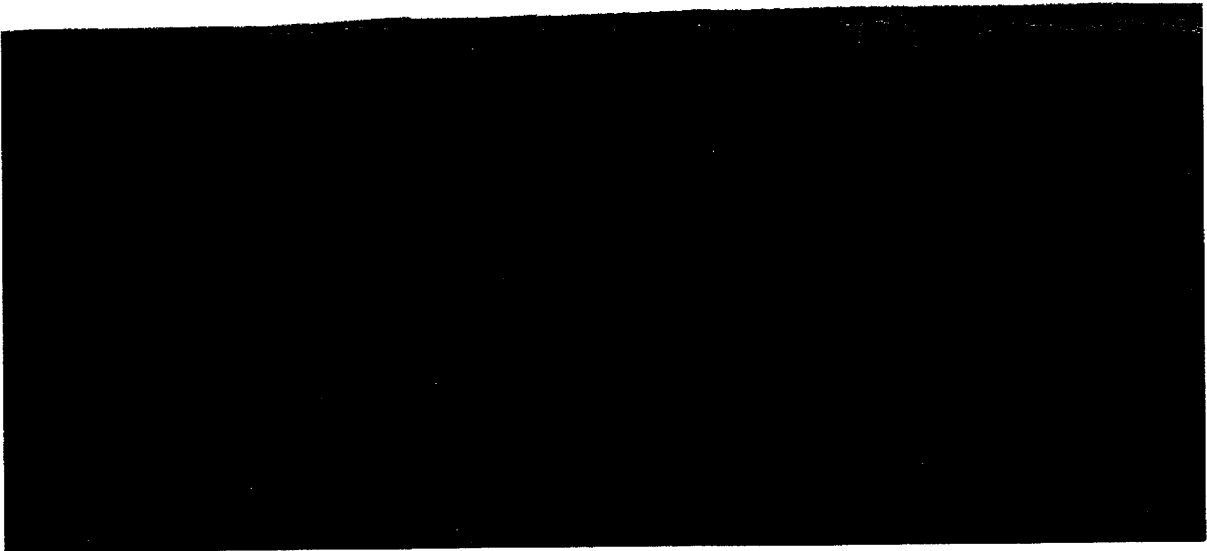
Nachdem die US-Seite im Rahmen der Working Group angeregt hatte, eine EU-Position für den laufenden Prozess der US-internen Evaluierung der Überwachungsprogramme einzubringen, hat PRÄS ein Papier mit Empfehlungen vorgelegt (Anlage 2), das am 3. Dezember 2013 durch den ASTV verabschiedet und an die USA weitergegeben werden soll. Zentrale Forderungen sind die „Gleichbehandlung von US- und EU-Bürgern“, „Wahrung des Verhältnismäßigkeitsprinzips“ sowie Stärkung des Rechtsschutzes (für

von Überwachungsmaßnahmen betroffene EU-Bürger). DEU hat die Erarbeitung der Empfehlungen unterstützt

Kurzstellungnahme

Die vorliegenden Papiere sind **inhaltlich** wenig überraschend und – mit einigen Änderungen in der weiteren Abstimmung – vertretbar. Die Details zu den US-Rechtsgrundlagen sind im Wesentlichen bekannt. Die hieraus abgeleiteten Empfehlungen für eine (rechtliche) Neuaufstellung der US-Überwachungsprogramme sind grundsätzlich zu begrüßen.

In **kompetenzieller** Hinsicht sind allerdings beide Papiere umstritten. Die EU hat ausdrücklich keine Kompetenz zur Regelung der Tätigkeit der nationalen Nachrichtendienste. Es lässt sich auch keine Zuständigkeit für ausländische Nachrichtendienste ableiten, soweit die EU auf dem Gebiet der Außenbeziehungen oder des Datenschutzrechts tätig wird (keine „Annexregelung“). Allenfalls soweit auf US-Seite das FBI (zwar nur als Antragsteller) in das Verfahren nach sec. 215 Patriot Act eingebunden ist, besteht eine EU-Kompetenz. Deshalb hat DEU gefordert, das Papier auch im Namen der Mitgliedstaaten veröffentlichen zu lassen. Es kann nicht ausgeschlossen werden, dass KOM – ggf. auch am Rande des JI-Rates – mit Blick auf die Empfehlungen versuchen wird, für erweiterte Zuständigkeiten auf dem Gebiet der Nationalen Sicherheit zu werben. Das sollte auf jeden Fall verhindert werden.



Bl. 213

Entnahme wegen fehlenden Bezugs zum
Untersuchungsgegenstand

[REDACTED]

[REDACTED]

[REDACTED]

d) Bericht über das TFTP-Abkommen (Anlage 5)

Im Zusammenhang mit der Veröffentlichung der Snowden-Dokumente wurde in der Presse der Vorwurf erhoben, die NSA habe unter Umgehung des TFTP-Abkommens, das die Weiterleitungsmöglichkeiten von Daten des Finanzdienstleisters SWIFT aus der EU an die USA regelt und begrenzt, direkten Zugriff auf die SWIFT-Server genommen. Am 23. Oktober 2013 hat das EP in einer Entschließung KOM aufgefordert, das zwischen der EU und den USA geschlossene Abkommen auszusetzen. KOM'n Malmström hat nach Bekanntwerden der Vorwürfe Konsultationen mit den USA eingeleitet. Diese sind zwischenzeitlich abgeschlossen worden. KOM ist zu dem Schluss gelangt, dass keine Anhaltspunkte für einen Verstoß gegen das Abkommen vorliegen.

Parallel dazu hat die KOM (wie in Art. 6 Abs. 6 des Abkommens vorgesehen) drei Jahre nach Inkrafttreten des Abkommens (Stichtag: 1. August 2013) gemeinsam mit den USA den Nutzen der bereitgestellten TFTP-Daten evaluiert und den betreffenden Bericht (Anlage 6) am 27. November 2013 veröffentlicht. KOM und USA kommen darin zu dem Schluss, dass die generierten Daten einen signifikanten Beitrag zur Bekämpfung der Terrorismusfinanzierung leisten. Durch die Rekonstruktion von Finanzgeflechten könnten Informationen über Organisationen und Einzelpersonen generiert werden. Auch wird auf die Bedeutung der fünfjährigen Speicherdauer hingewiesen, die keinesfalls verkürzt werden solle.

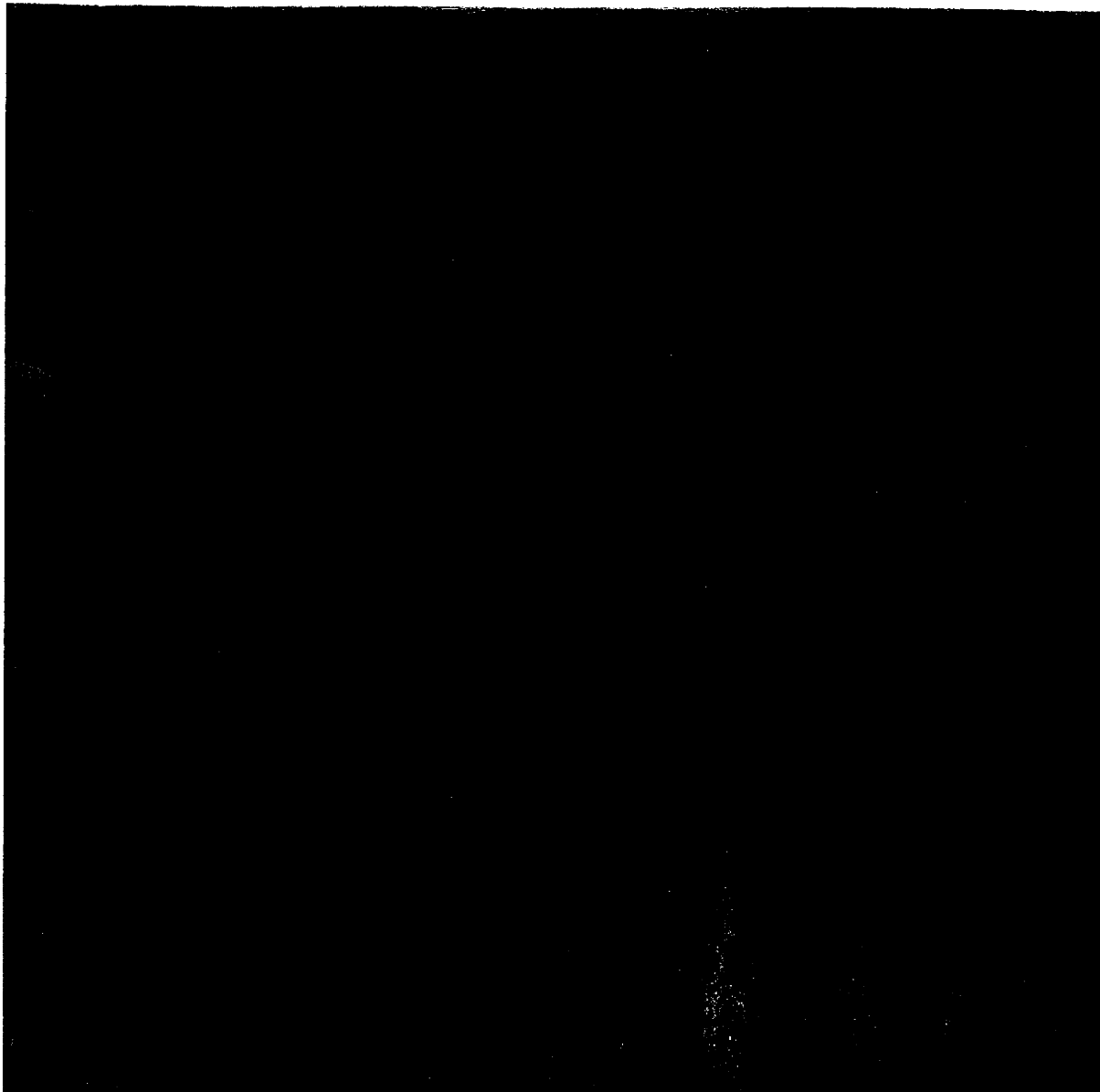
Kurzstellungnahme

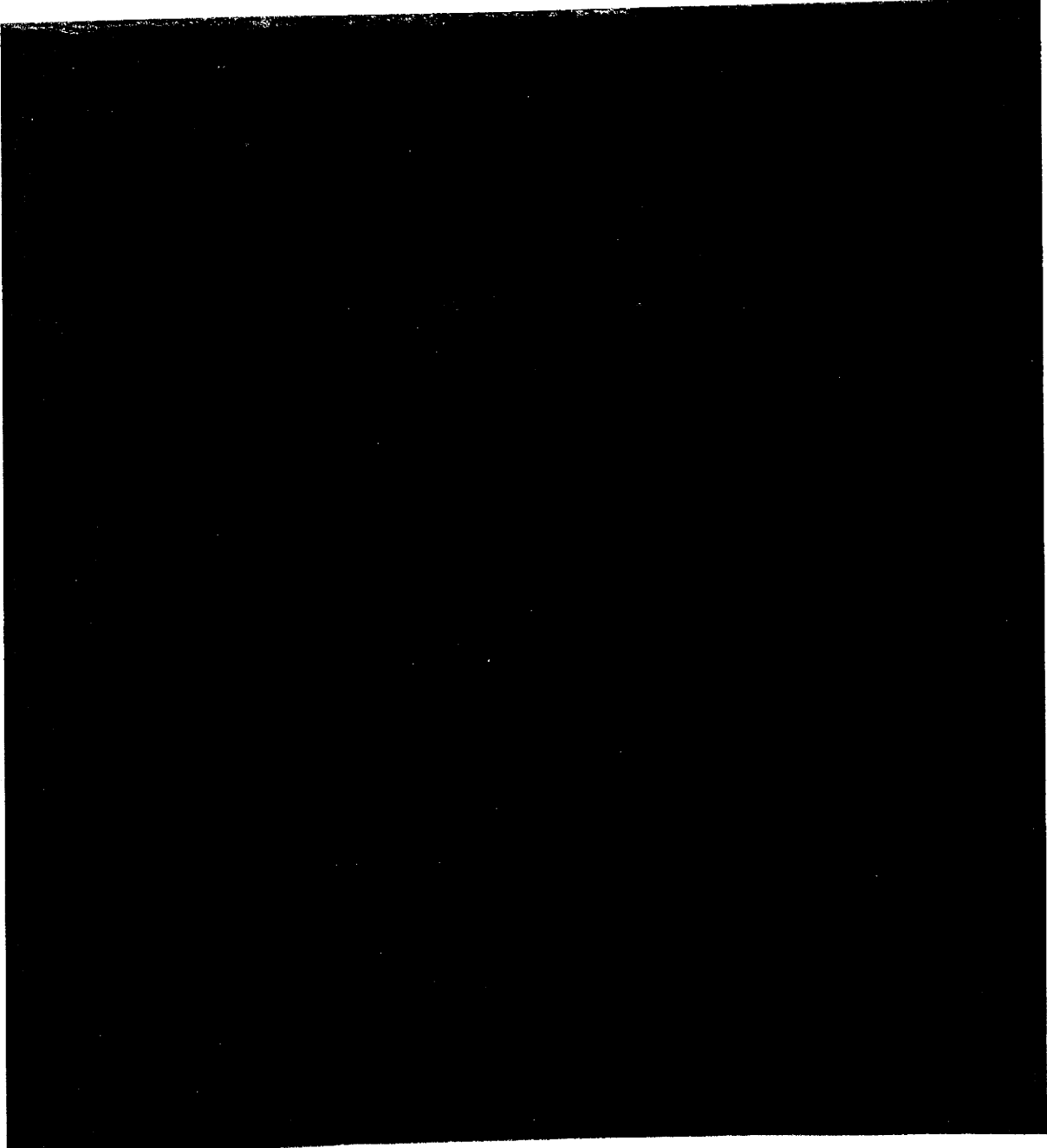
Da Vertragsparteien des TFTP-Abkommens die EU und die USA sind, war es Aufgabe der KOM, die gegen die USA erhobenen Vorwürfe aufzuklären. Erst danach konnte über eine Suspendierung oder Kündigung nachgedacht werden. BMI (sowie BND, BfV, BKA) ist nicht bekannt, dass die NSA unter Umgehung des Abkommens ~~Zugriff~~ auf SWIFT -Daten zugreift. Mit Vorlie-

gen des Untersuchungsergebnisses der KOM, dass kein Verstoß gegen das Abkommen vorliegt, besteht derzeit kein Anlass, das Abkommen auszusetzen.

⇒ *Hintergrundinformation: Der Koalitionsvertrag sieht vor, dass die neue Bundesregierung in der EU auf Nachverhandlungen mit den USA dringen wird, um die im Abkommen enthaltenen Datenschutzregelungen zu verbessern.*

Das Ergebnis des Evaluierungsberichts war aus hiesiger Sicht zu erwarten. Auch BKA und BfV haben bestätigt, dass die von den USA weitergegebenen TFTP-Daten hilfreich waren, da vorhandene Kenntnisse angereichert und/oder bestätigt werden konnten.





W. Weinbrenner
Weinbrenner

Dr. Spitzer
Dr. Spitzer

Dokument 2013/0530201

Von: Spitzer, Patrick, Dr.
Gesendet: Freitag, 6. Dezember 2013 10:48
An: PGDS_; VI4_; IT1_; OESIII1_; 'ref601@bk.bund.de'; 'ref132@bk.bund.de'; BMWI BUERO-EA2; AA Oelfke, Christian; AA Kinder, Kristin; AA Wendel, Philipp
Cc: BMWI Bölhoff, Corinna; BMJ Henrichs, Christoph; BMJ Harms, Katharina; BK Rensmann, Michael; BK Wolff, Philipp; BMWI Scholl, Kirsten; Bender, Ulrike; Merz, Jürgen; Riemer, André; Schlender, Katharina; Marscholleck, Dietmar; OESI3AG_; Jergl, Johann; Stöber, Karlheinz, Dr.; Weinbrenner, Ulrich; OESII2_; Peters, Reinhard; RegOeSI3; Popp, Michael; GI12_
Betreff: Eilt sehr! Weisung JI-Rat TOP 27 (Mitzeichnung) : Empfehlungspapier EU und MS
Anlagen: 13-12-04 Vorl Tagesordnung JI-Rat (ST17017 DE13).pdf; st16824-re02.de13.doc; 15_ Weisung_EU-USA MinTreffen_Empfehlungspapier.docx
Wichtigkeit: Hoch

ÖS I 3-52001/1#9

Liebe Kolleginnen und Kollegen,

unter TOP 27 der für den heutigen Justizteil des JI-Rates beigefügten TO ist eine "Information des zu den Ergebnissen der Tagung der JI-Minister der EU und der USA vorgesehen". Grundlage der Information soll ausweislich der TO auch das am 3.12.21013 im AStV verabschiedete Empfehlungspapier der EU und der MS sein. Das BMI hat kurzfristig die Information erreicht, dass - obwohl in der TO nicht angekündigt - über das Papier (in der nunmehr vorliegenden 2. überarbeiteten Fassung, siehe Anlage 2) heute ggf. formal abgestimmt werden soll.

Die vor diesem Hintergrund angefertigte - zustimmende - Weisung DEU habe ich als weitere Anlage (3) beigefügt. Sie orientiert sich weitestgehend - bis auf wenige "technische" Änderungen an der im Zuge der Vorbereitung des AStV vom 3.12.2013 abgestimmten Weisung. Ich bitte um Mitzeichnung zum Weisungsdokument **bis heute, 6.12.2013, 11.00 Uhr** und um Nachsicht für die sehr knappe Frist.

Freundliche Grüße

Patrick Spitzer

im Auftrag
 Dr. Patrick Spitzer

Bundesministerium des Innern
 Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,
 BKA-Gesetz, Datenschutz im Sicherheitsbereich)
 Alt-Moabit 101D, 10559 Berlin
 Telefon: +49 (0)30 18681-1390
 E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?



**RAT DER
EUROPÄISCHEN UNION**

**Brüssel, den 4. Dezember 2013
(OR. en)**

17017/13

**OJ/CONS 62
JAI 1081
COMIX 645**

VORLÄUFIGE TAGESORDNUNG

Betr.:	3279. Tagung des RATES DER EUROPÄISCHEN UNION (Justiz und Inneres)
Termin:	5. und 6. Dezember 2013
Uhrzeit:	9.30 Uhr, 9.30 Uhr
Ort:	Brüssel

A. DONNERSTAG, 5. DEZEMBER 2013 (09.30 UHR)

INNERES

1. Annahme der vorläufigen Tagesordnung

Beratungen über Gesetzgebungsakte

2. Sonstiges
 - Informationen des Vorsitzes zu aktuellen Gesetzgebungsvorschlägen

Nicht die Gesetzgebung betreffende Tätigkeiten

3. Annahme der Liste der A-Punkte
17019/13 PTS A 84
4. Fragen im Zusammenhang mit dem freien Personenverkehr
 - Abschlussbericht der Kommission
16930/13 JAI 1074 FREMP 198 MI 1083 POLGEN 240 SOC 995
17395/13 JAI 1115 FREMP 205 MI 1129 POLGEN 255 SOC 1019
5. Terrorismusbekämpfung: Ausländische Kämpfer und Rückkehrer aus Sicht der Terrorismusbekämpfung, unter besonderer Berücksichtigung Syriens
 - Erläuterungen des EU-Koordinators für die Terrorismusbekämpfung und Aussprache
16768/13 JAI 1059 PESC 1422 COSI 146 COPS 497 ENFOPOL 384
COTER 146
16878/13 JAI 1069 PESC 1431 COSI 150 COPS 502 ENFOPOL 390
COTER 149 **RESTREINT UE**
17274/13 JAI 1108 PESC 1468 COSI 158 COPS 509 ENFOPOL 403
COTER 156 **RESTREINT UE**
6. Entwurf eines Beschlusses des Rates über den Rahmen für die vollständige Anwendung der Bestimmungen des Schengen-Besitzstands in der Republik Bulgarien und in Rumänien
 - Sachstand
7. Task Force "Mittelmeerraum"
 - Bericht der Kommission
17398/13 JAI 1116 ASIM 108 FRONT 208 RELEX 1123 COMIX 681
8. Lage im Schengen-Raum
Vierter Halbjahresbericht der Kommission an das Europäische Parlament und den Rat über das Funktionieren des Schengen-Raums (1. Mai-31. Oktober 2013)
16933/13 JAI 1072 SCHENGEN 41 COMIX 642
+ REV 1 (en)
9. Vierter Bericht über die Überwachung nach der Visaliberalisierung für die westlichen Balkanstaaten
17144/13 VISA 266 COWEB 179
10. Künftige Entwicklung des JI-Bereichs
17170/13 JAI 1102 JAIEX 114 JUSTCIV 296 CATS 93 DROIPEN 153
COPEN 224 COSI 155 ASIM 106 MIGR 135 VISA 267
FRONT 199 ENFOPOL 400 PROCIV 141 DAPIX 153
CRIMORG 158 EUROJUST 133 GENVAL 88 EJUSTICE 107
+ COR 1
11. Sonstiges
 - Ergebnisse der Tagung der JI-Minister der EU und der USA
= Informationen des Vorsitzes
16682/13 JAIEX 99 RELEX 1048 ASIM 101 CATS 90 JUSTCIV 277 USA 58

B. FREITAG, 6. DEZEMBER 2013 (9.30 Uhr)**JUSTIZ****Beratungen über Gesetzgebungsakte**

12. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) [**erste Lesung**]
 – Wesentliche Aspekte des Konzepts einer einzigen Anlaufstelle
 17025/13 DATAPROTECT 185 JAI 1084 MI 1104 DRS 214 DAPIX 150
 FREMP 200 COMIX 646 CODEC 2771
13. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einführung eines Europäischen Beschlusses zur vorläufigen Kontenpfändung im Hinblick auf die Erleichterung der grenzüberschreitenden Eintreibung von Forderungen in Zivil- und Handelssachen [**erste Lesung**]
 – Allgemeine Ausrichtung
 16991/13 JUSTCIV 291 CODEC 2756
 + ADD 1
14. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EG) Nr. 1346/2000 des Rates über Insolvenzverfahren [**erste Lesung**]
 – Orientierungsaussprache
 17304/13 JUSTCIV 298 EJUSTICE 109 CODEC 2826
15. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EG) Nr. 1215/2012 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen [**erste Lesung**]
 – Allgemeine Ausrichtung
 16982/13 JUSTCIV 290 PI 176 CODEC 2754
 + ADD 1
16. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ein Gemeinsames Europäisches Kaufrecht [**erste Lesung**]
 – Informationen des Vorsitzes
18. Sonstiges
 – Informationen des Vorsitzes zu aktuellen Gesetzgebungsvorschlägen

Nicht die Gesetzgebung betreffende Tätigkeiten

19. (ggf.) Annahme der Liste der A-Punkte
17019/13 ADD 1 PTS A 84
20. Schlussfolgerungen des Rates zur Bekämpfung von Hasskriminalität
– Annahme
17057/13 FREMP 202 JAI 1091 COPEN 223 DROIPEN 152 SOC 998
21. Schlussfolgerungen des Rates zum Bericht über die Unionsbürgerschaft 2013
– Annahme
16783/13 FREMP 194 JAI 1060 COCON 58 COHOM 262 CULT 124
COPEN 215 DROIPEN 148 EJUSTICE 102 FISC 235
JUSTCIV 279 MI 1073 POLGEN 236 SOC 980 TRANS 614
22. Schlussfolgerungen des Rates zur Bewertung der Agentur der Europäischen Union für Grundrechte
– Annahme
16622/13 FREMP 190 JAI 1040 COHOM 260
23. Justizrelevante Aspekte des Europäischen Semesters einschließlich des Justizbarometers
– Erläuterungen der Kommission und Gedankenaustausch
16623/13 JAI 1041 FREMP 191 JUSTCIV 276 COPEN 212
DROIPEN 145 JAIEX 97
15803/13 ECOFIN 984 SOC 904 COMPET 781 EDUC 425
ENV 1025 RECH 509 ENER 502 FISC 214 JAI 1039
+ COR 1
24. Künftige Entwicklung des JI-Bereichs
17170/13 JAI 1102 JAIEX 114 JUSTCIV 296 CATS 93 DROIPEN 153
COPEN 224 COSI 155 ASIM 106 MIGR 135 VISA 267
FRONT 199 ENFOPOL 400 PROCIV 141 DAPIX 153
CRIMORG 158 EUROJUST 133 GENVAL 88 EJUSTICE 107
+ COR 1
25. Beitritt der Europäischen Union zur EMRK
– Sachstand
16860/13 FREMP 197 JAI 1067
26. E-Justiz
a) Strategie für die europäische E-Justiz (2014-2018)
– Annahme
17006/13 EJUSTICE 105 JUSTCIV 293 COPEN 221 JAI 1079
b) Im zweiten Halbjahr 2013 geleistete Arbeit
– Informationen des Vorsitzes
16269/13 EJUSTICE 98 JURINFO 39 JUSTCIV 271 JUSTPEN 13
COPEN 205 DROIPEN 140 FREMP 185

27. Sonstiges

- i) Ergebnisse der Tagung der JI-Minister der EU und der USA
 - Informationen des Vorsitzes
16682/13 JAIEX 99 RELEX 1048 ASIM 101 CATS 90
JUSTCIV 277 USA 58
16824/2/13 REV 2 JAI 1066 USA 59 RELEX 1069 DATAPROTECT 182
COTER 147 **RESTREINT UE**
16987/13 JAI 1078 USA 61 DATAPROTECT 184 COTER 151
COTER 151 ENFOPOL 394
- ii) Vorstellung des Programms des künftigen griechischen Vorsitzes (Januar-Juni 2014)

o

o o

Am Rande der Ratstagung:**Sitzung des GEMISCHTEN AUSSCHUSSES (Donnerstag, 5. DEZEMBER 2013 – 15.00 Uhr)**

1. Entwurf eines Beschlusses des Rates über den Rahmen für die vollständige Anwendung der Bestimmungen des Schengen-Besitzstands in der Republik Bulgarien und in Rumänien
 - Sachstand
2. Task Force "Mittelmeerraum"
 - Bericht der Kommission
17398/13 JAI 1116 ASIM 108 FRONT 208 RELEX 1123 COMIX 681
3. Lage im Schengen-Raum
Vierter Halbjahresbericht der Kommission an das Europäische Parlament und den Rat über das Funktionieren des Schengen-Raums (1. Mai-31. Oktober 2013)
 - Vorstellung und Orientierungsaussprache
16933/13 JAI 1072 SCHENGEN 41 COMIX 642
4. Vierter Bericht über die Überwachung nach der Visaliberalisierung für die westlichen Balkanstaaten
17144/13 VISA 266 COWEB 179
5. Sonstiges
 - a) Informationen des Vorsitzes zu aktuellen Gesetzgebungsvorschlägen
 - b) Fünf Jahre operative Schengen-Zusammenarbeit der Schweiz
 - Erklärung der Schweiz
 - c) Vorstellung des Programms des künftigen griechischen Vorsitzes (Januar-Juni 2014)



**RAT DER
EUROPÄISCHEN UNION**

**Brüssel, den 4. Dezember 2013
(OR. en)**

**16824/2/13
REV 2**

RESTREINT UE/EU RESTRICTED

**JAI 1066
USA 59
RELEX 1069
DATAPROTECT 182
COTER 147**

VERMERK

des	Vorsitzes
für den	Rat
<u>Betr.:</u>	Beitrag der EU und ihrer Mitgliedstaaten im Kontext der von den USA vorgenommenen Überprüfung der Überwachungsprogramme

Wie auf der Tagung des AstV vom 14. November 2013 angekündigt, legt der Vorsitz hiermit – als Reaktion auf die von amerikanischer Seite in der Ad-hoc-Arbeitsgruppe EU–USA "Datenschutz" wiederholt vorgetragene Bitte – den Entwurf eines Non-Papers vor, das Vorschläge enthält, wie im Kontext der von den USA vorgenommenen Überprüfung der Überwachungsprogramme die Bedenken der EU und ihrer Mitgliedstaaten ausgeräumt werden könnten. Die amerikanische Seite hob hervor, dass sie die Beiträge von europäischer Seite dringend benötige.

Der in der Anlage wiedergegebene Beitrag folgt auf den Bericht über die Feststellungen der EU-Ko-Vorsitzenden der Ad-hoc-Arbeitsgruppe EU–USA "Datenschutz"¹ und die Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel "Rebuilding Trust in EU-US Data Flows" (Wiederherstellung des Vertrauens in die Datenübertragung zwischen der EU und den USA)².

¹ Dok. 16987/13 JAI 1078 USA 61 DATAPROTECT 184 COTER 151 ENFOPOL 394.

² Dok. 17067/13 JAI 1095 USA 64 DATAPROTECT 190 COTER 154.

Der in der Anlage wiedergegebene Beitrag greift den Verhandlungen nicht vor, die die Kommission mit den USA im Einklang mit den vom Rat angenommenen Verhandlungsrichtlinien über ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über den Schutz personenbezogener Daten bei deren Übermittlung und Verarbeitung zum Zwecke der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten, einschließlich terroristischer Handlungen, im Rahmen der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen¹ führt.

Der Beitrag wird unbeschadet der Aufteilung der Zuständigkeiten zwischen der EU und den Mitgliedstaaten vorgelegt. Gemäß Artikel 4 Absatz 2 EUV fällt die nationale Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten.

Nach abschließender Bearbeitung wird das Non-Paper der US-Regierung nach den einschlägigen Verfahren im Namen der EU und ihrer Mitgliedstaaten übermittelt. Das Papier kann bei Bedarf auch für weitere Outreach-Maßnahmen verwendet werden.

Der Rat und die Mitgliedstaaten werden ersucht, den in der Anlage wiedergegebenen Beitrag der EU und ihrer Mitgliedstaaten im Kontext der von den USA vorgenommenen Überprüfung der Überwachungsprogramme zu billigen.

¹ Dok. 15840/6/10 REV 6 JAI 914 USA 115 DATAPROTECT 79 RELEX 921.

ANLAGE

**Beitrag der EU und ihrer Mitgliedstaaten
im Kontext der von den USA vorgenommenen Überprüfung der Überwachungsprogramme**

Die EU zusammen mit ihren Mitgliedstaaten und die USA sind strategische Partner. Diese Beziehung ist von wesentlicher Bedeutung für unsere Sicherheit, für die Förderung unserer gemeinsamen Werte und für unsere gemeinsame Führerschaft in weltpolitischen Fragen. Seit dem 11. September und den späteren terroristischen Anschlägen in Europa haben die EU, ihre Mitgliedstaaten und die Vereinigten Staaten ihre polizeiliche Zusammenarbeit, ihre justizielle Zusammenarbeit in Strafsachen und ihre Zusammenarbeit auf dem Gebiet der Sicherheit intensiviert. Der Austausch einschlägiger Informationen, einschließlich personenbezogener Daten, ist ein wesentlicher Bestandteil dieser Beziehung. Hierfür ist Vertrauen zwischen den Regierungen, aber auch das der Bürger beider Seiten erforderlich.

Sowohl die EU als auch die Mitgliedstaaten haben angesichts von Medienberichten über großangelegte nachrichtendienstliche Programme der USA Bedenken, insbesondere in Bezug auf den Schutz der personenbezogenen Daten unserer Bürger, geäußert. Wenn Bürger über die Verarbeitung ihrer Daten durch Privatunternehmen besorgt sind, kann hierdurch das Vertrauen der Bürger in die digitale Wirtschaft erschüttert werden, was sich negativ auf das Wirtschaftswachstum auswirken kann. Tatsächlich ist Vertrauen einer der Schlüssel zu einem sicheren und reibungslosen Funktionieren der digitalen Wirtschaft.

Wir begrüßen, dass Präsident Obama eine Überprüfung der US-Überwachungsprogramme eingeleitet hat. Wir begrüßen ferner, dass sich die US-Regierung dessen bewusst ist, dass den Rechten unserer Bürger im Rahmen dieser Überprüfung besondere Aufmerksamkeit gebührt, wie Justizminister Eric Holder feststellte: "The concerns we have here are not only with American citizens. I hope that the people in Europe will hear this, people who are members of the EU, nations of the members of the EU. Our concerns go to their privacy as well."

Nach amerikanischem Recht gelten für in der EU ansässige Personen weder dasselbe Recht auf Privatsphäre noch dieselben Schutzbestimmungen wie für US-Bürger. Für sie gelten andere Regeln, selbst wenn die Verarbeitung ihrer personenbezogenen Daten in den Vereinigten Staaten erfolgt.

Dies steht im Gegensatz zum europäischen Recht, nach dem für alle personenbezogenen Daten, die an irgendeinem Ort in der EU verarbeitet werden, dieselben Standards gelten, unabhängig von der Staatsangehörigkeit oder dem Aufenthaltsort der Person, um deren Daten es sich handelt. Darüber hinaus ist es für das reibungslose Funktionieren der digitalen Wirtschaft notwendig, dass Kunden amerikanischer IT-Unternehmen Vertrauen in die Art und Weise haben, in der ihre Daten erhoben und verarbeitet werden. Somit könnten amerikanische Internet-Unternehmen wirtschaftlichen Nutzen daraus ziehen, wenn die Überprüfung des amerikanischen Rechtsrahmens so erfolgte, dass sie für größeres Vertrauen unter den EU-Bürgern sorgt.

Wir wissen die Diskussionen zu schätzen, die in der Ad-hoc-Arbeitsgruppe EU–USA geführt wurden, und begrüßen die von amerikanischer Seite ausgesprochene Aufforderung, unsere Vorstellungen zu der Frage darzulegen, wie unsere Bedenken im Rahmen des von den Vereinigten Staaten durchgeführten Überprüfungsprozesses ausgeräumt werden könnten. Die Kommission hat vor dem Hintergrund der Beratungen der Ad-hoc-Arbeitsgruppe EU–USA eine Mitteilung mit dem Titel "Rebuilding Trust in EU-US Data Flows" (Wiederherstellung des Vertrauens in die Datenübertragung zwischen der EU und den USA) übermittelt.

In der EU ansässigen Personen sollten strengere allgemeine Vorschriften, zusätzliche Schutzvorschriften in Bezug auf Notwendigkeit und Verhältnismäßigkeit sowie wirksame Rechtsmittel im Falle von Datenmissbrauch zugute kommen.

Die Gleichbehandlung von US-Bürgern und in der EU ansässigen Personen ist eine wesentliche Frage, und deshalb könnten bei der Überprüfung die folgenden Punkte in Betracht gezogen werden, um einige unserer Bedenken auszuräumen:

1. Das Recht von in der EU ansässigen Personen auf Privatsphäre

Die Überprüfung sollte dazu führen, dass für in der EU ansässige Personen dasselbe durchsetzbare Recht auf Privatsphäre wie für US-Bürger gilt. Dies ist besonders wichtig für die Fälle, in denen die Verarbeitung ihrer Daten in den Vereinigten Staaten erfolgt.

2. Rechtsmittel

Gegenstand der Überprüfung sollte ebenfalls sein, wie für in der EU ansässige Personen sichergestellt werden kann, dass Datenschutzmaßnahmen der USA auch ihnen zugute kommen, und dass ihnen Rechtsmittel zur Verfügung stehen, um ihr Recht auf Privatsphäre zu schützen. Diese Rechtsmittel sollten wirksame administrative und gerichtliche Rechtsbehelfe umfassen.

3. Anwendungsbereich, Notwendigkeit und Verhältnismäßigkeit der Programme

Um Bedenken im Zusammenhang mit dem Anwendungsbereich der Programme auszuräumen, ist es wichtig, dass in Bezug auf die Erhebung von Daten und den Zugang zu diesen Daten der Grundsatz der Verhältnismäßigkeit geachtet wird. In der Europäischen Union sind die Grundsätze der Notwendigkeit und der Verhältnismäßigkeit weithin anerkannt. Die Vereinigten Staaten werden ersucht, in Betracht zu ziehen, ob vergleichbare Grundsätze bei der Überprüfung von Nutzen sein könnten.

Im Kontext der Überprüfung sollten die Vereinigten Staaten in Betracht ziehen, das Gebot der "Notwendigkeit" – eine wesentliche Voraussetzung für die Achtung des Grundsatzes der Verhältnismäßigkeit – auf in der EU ansässige Personen auszuweiten.

Im Rahmen der Überprüfung sollte bewertet werden, ob eine Erhebung von Daten tatsächlich notwendig und verhältnismäßig ist, und die Empfehlung ausgesprochen werden, den Verfahren mehr Gewicht zu verleihen, die darauf abzielen, die Erhebung und Verarbeitung von Daten, die das Notwendigkeits- und das Verhältnismäßigkeitskriterium nicht erfüllen, auf ein Minimum zu beschränken.

Durch die Einführung dieser Vorgaben würde das amerikanische Datenschutzsystem auch in der EU ansässigen Personen zugute kommen.

Referat: EU-KOR

6. Dezember 2013

Verfasser: RR Dr. Spitzer (BMI)

Hausruf: 1390

JI-Rat am 5. und 6. Dezember 2013 in Brüssel

TOP: Ergebnisse der Tagung der JI-Minister der EU und der USA

beizufügende Sitzungsunterlagen: -Outcome of Proceedings (Dok. 16682/13)

-16824/2/13 REV2 16824/2/13 REV

I. Ziel der Ratsbefassung:

- Zustimmung zu den als *follow-up* zu den Ergebnissen der „ad hoc EU US Working Group on data protection“ vorgelegten Empfehlungen der EU und der MS zur Berücksichtigung in der laufenden US-internen Evaluierung der Überwachungsprogramme

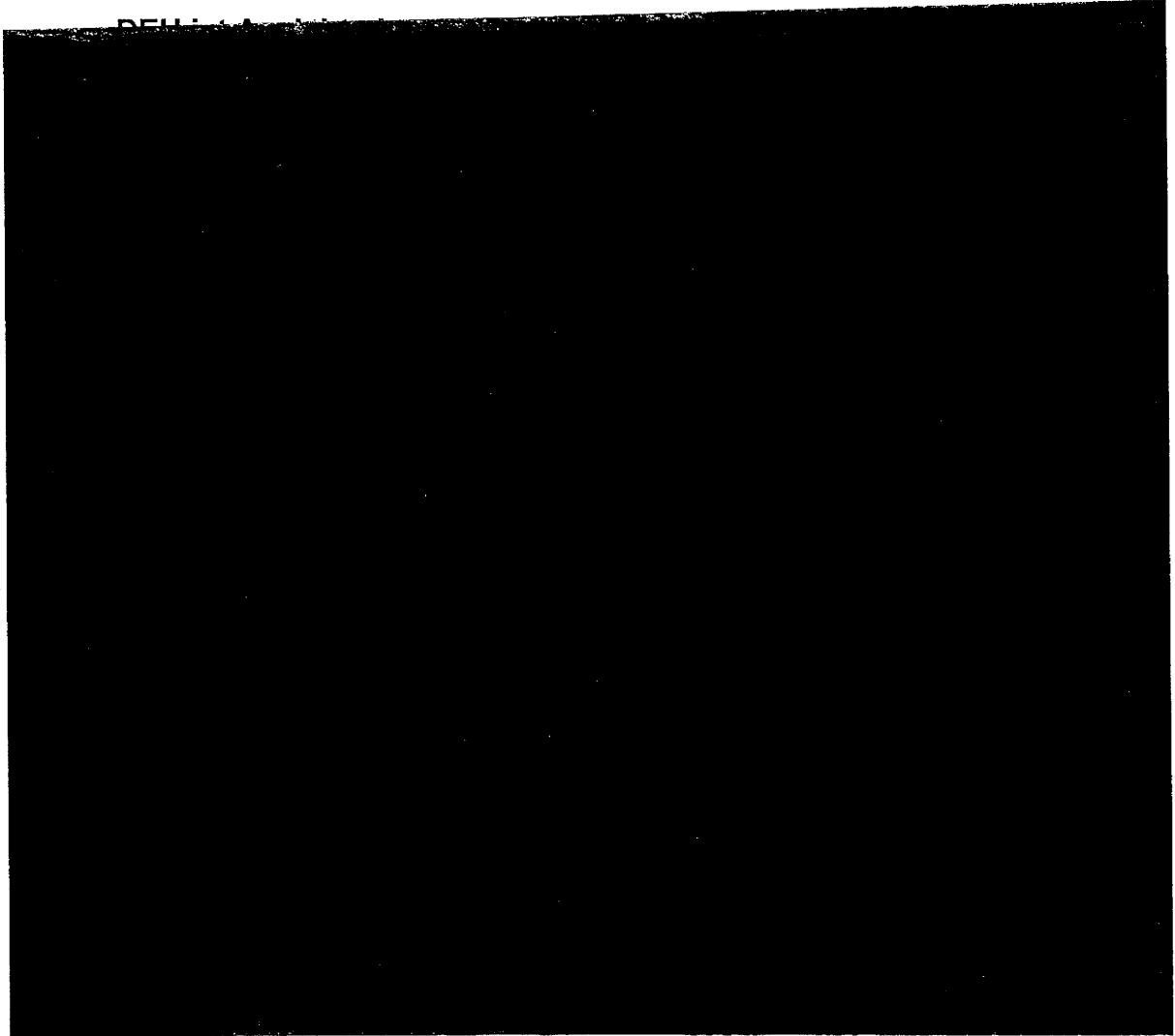
II. Sachverhalt:

- Die „ad hoc EU US working group on data protection“ („Working Group“) wurde im Juli 2013 eingerichtet, um „datenschutzrechtliche Fragestellungen im Hinblick auf personenbezogene Daten von EU-Bürgern, die von den US-Überwachungsprogrammen betroffen sind“, zu erörtern. Die Working Group hat sich von Juli bis November 2013 vier Mal alternierend in Brüssel und in Washington getroffen. Vorsitz und KOM haben am 27.11.2013 den Abschlussbericht der Arbeitsgruppe vorgelegt. Der Bericht geht inhaltlich auf die im Wesentlichen bekannte US-Rechtsslage (insbes. sec. 702 FISA, sec. 215 Patriot Act) ein. Der Bericht spricht u.a. die Ungleichbehandlung von US- und EU-Bürgern, unterschiedliche Auffassungen über die Auslegung des Verhältnismäßigkeitsgrundsatzes und die mangelnden Rechtsschutzmöglichkeiten für EU-Bürger in den USA als zentrale Punkte an.
- Die US-Seite hat im Rahmen der Working Group darüber hinaus angeregt, sich in den laufenden Prozess der US-internen Evaluierung der Überwachungsprogramme einzubringen. PRÄS hat daraufhin Papier mit Empfehlungen zur Abstimmung vorgelegt. Die Empfehlungen wurden am 28.11.2013 im Rahmen eines Treffens der JI-Referenten behandelt und wurde am 3.12.2013 durch den AStV verabschiedet.

III. Interessen/Ziele des BMJ/BMI:

IV. Verhandlungssituation / Haltung anderer MS/KOM:

V. Gesprächsführungsvorschlag



Dokument 2013/0530183

Von: Corinna.Boelhoff@bmwi.bund.de
Gesendet: Freitag, 6. Dezember 2013 11:00
An: Spitzer, Patrick, Dr.; PGDS_; VI4_; IT1_; OESIII1_; 'ref601@bk.bund.de'; 'ref132@bk.bund.de'; BMWI BUERO-EA2; AA Oelfke, Christian; AA Kinder, Kristin; AA Wendel, Philipp
Cc: BMJ Henrichs, Christoph; BMJ Harms, Katharina; BK Rensmann, Michael; BK Wolff, Philipp; BMWI Scholl, Kirsten; Bender, Ulrike; Merz, Jürgen; Riemer, André; Schlender, Katharina; Marscholleck, Dietmar; OESI3AG_; Jergl, Johann; Stöber, Karlheinz, Dr.; Weinbrenner, Ulrich; OESII2_; Peters, Reinhard; RegOeSI3; Popp, Michael; GII2_
Betreff: AW: Eilt sehr! Weisung JI-Rat TOP 27 (Mitzeichnung) : Empfehlungspapier EU und MS

Lieber Herr Spitzer,

BMW i zeichnet mit.

Mit freundlichen Grüßen,
 Corinna Bölhoff

Dr. Corinna Bölhoff

Referat EA2 - Zukunft der EU, Justiz und Inneres, Bessere Rechtsetzung
 Bundesministerium für Wirtschaft und Technologie
 Scharnhorststr. 34-37, 10115 Berlin
 Telefon: +49 (0)30 18615-6937
 Fax: +49 (0)30 18615-50-6937
 E-Mail: corinna.boelhoff@bmwi.bund.de
 Internet: <http://www.bmwi.de>

Von: Patrick.Spitzer@bmi.bund.de [mailto:Patrick.Spitzer@bmi.bund.de]
Gesendet: Freitag, 6. Dezember 2013 10:48
An: PGDS@bmi.bund.de; VI4@bmi.bund.de; IT1@bmi.bund.de; OESIII1@bmi.bund.de; 'ref601@bk.bund.de'; 'ref132@bk.bund.de'; BUERO-EA2; e05-2@auswaertiges-amt.de; e05-3@auswaertiges-amt.de; 200-4@auswaertiges-amt.de
Cc: Bölhoff, Corinna, Dr., EA2; henrichs-ch@bmj.bund.de; harms-ka@bmj.bund.de; Michael.Rensmann@bk.bund.de; Philipp.Wolff@bk.bund.de; Scholl, Kirsten, Dr., EA2; Ulrike.Bender@bmi.bund.de; Juergen.Merz@bmi.bund.de; Andre.Riemer@bmi.bund.de; Katharina.Schlender@bmi.bund.de; Dietmar.Marscholleck@bmi.bund.de; OESI3AG@bmi.bund.de; Johann.Jergl@bmi.bund.de; Karlheinz.Stoeber@bmi.bund.de; Ulrich.Weinbrenner@bmi.bund.de; OESII2@bmi.bund.de; Reinhard.Peters@bmi.bund.de; RegOeSI3@bmi.bund.de; Michael.Popp@bmi.bund.de; GII2@bmi.bund.de
Betreff: Eilt sehr! Weisung JI-Rat TOP 27 (Mitzeichnung) : Empfehlungspapier EU und MS
Wichtigkeit: Hoch

ÖS I 3-52001/1#9

Liebe Kolleginnen und Kollegen,

unter TOP 27 der für den heutigen Justizteil des JI-Rates beigefügten TO ist eine "Information des zu den Ergebnissen der Tagung der JI-Minister der EU und der USA vorgesehen". Grundlage der Information soll ausweislich der TO auch das am 3.12.21013 im AStV verabschiedete Empfehlungspapier der EU und der MS sein. Das BMI hat kurzfristig die Information erreicht, dass - obwohl in der TO nicht angekündigt - über das Papier (in der nunmehr vorliegenden 2. überarbeiteten Fassung, siehe Anlage 2) heute ggf. formal abgestimmt werden soll.

Die vor diesem Hintergrund angefertigte - zustimmende - Weisung DEU habe ich als weitere Anlage (3) beigefügt. Sie orientiert sich weitestgehend - bis auf wenige "technische" Änderungen an der im Zuge der Vorbereitung des AStV vom 3.12.2013 abgestimmten Weisung. Ich bitte um Mitzeichnung zum Weisungsdokument **bis heute, 6.12.2013, 11.00 Uhr** und um Nachsicht für die sehr knappe Frist.

Freundliche Grüße

Patrick Spitzer

im Auftrag
Dr. Patrick Spitzer

Bundesministerium des Innern
Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,
BKA-Gesetz, Datenschutz im Sicherheitsbereich)
Alt-Moabit 101D, 10559 Berlin
Telefon: +49 (0)30 18681-1390
E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

Dokument 2013/0531905

Von: Spitzer, Patrick, Dr.
Gesendet: Montag, 9. Dezember 2013 15:17
An: PGDS_; OESII1_; B3_; VI4_
Cc: OESI3AG_; PGNSA; Weinbrenner, Ulrich; Schlender, Katharina; Papenkort, Katja, Dr.; Wenske, Martina; Bender, Ulrike; RegOeSI3
Betreff: EU-AL-Sitzung am 12.12.2013; hier: Vorbereitung TOP 6
Anlagen: Einladung.pdf; 131213 EU-AL Runde Sprechpunkte PGDS_PGNSA.docx

Wichtigkeit: Hoch

ÖS I 3- 52001/1#9

Liebe Kolleginnen und Kollegen,

für die am 12. Dezember 2013 stattfindende EU-AL Sitzung weist die als Anlage 1 beigefügten TO als TOP 6 das Thema „Datenschutz“ aus. Inhaltlich soll es dabei – siehe unten – um eine „erste inhaltliche Bewertung der KOM-Mitteilungen v. 27.11“. BMI soll in das Thema einführen. Die vor diesem Hintergrund erstellte Vorbereitung (Anlage 2) orientiert sich fast vollständig an der abgestimmten Minister-Vorlage. Ich bitte um Mitzeichnung bis heute, **9. Dezember, 16.30 Uhr** und insbesondere um Überprüfung/Kennzeichnung von aktiven/reaktiven Sprechpunkten sowie – bei Bedarf – Vornahme von inhaltlichen Hervorhebungen.

Freundliche Grüße

Patrick Spitzer
(-1390)

Von: GII2_
Gesendet: Montag, 2. Dezember 2013 16:45
An: PGDS_; PGNSA; VI5_; Arhelger, Roland; Hofmann, Christian; RegGII2; B3_; B4_; D1_; GII1_; GII3_; GII4_; GII5_; GIII1_; IT1_; IT3_; KM1_; MI5_; O1_; OESI4_; SP2_; SP6_; VI4_; ZI2_
Cc: Seedorf, Sebastian, Dr.; Stang, Rüdiger; Hübner, Christoph, Dr.; GII2_
Betreff: Enthält Fristen! EU-AL-Sitzung am 12.12.2013; hier: Themenabfrage und Anforderung

GII2-20200/3#10

Hiermit übersende ich die Tagesordnung für o. g. Sitzung mit der Bitte um Kenntnisnahme.

Sollten aus Ihrer Sicht **dringender Gesprächsbedarf** zu **weiteren Themen** bestehen, bitte ich

bis Donnerstag, 05.12.2013 - 17:00 Uhr um Mitteilung (mit kurzer Begründung) an Referatspostfach G II 2.

Die Grundsatz- und Koordinierungsreferate bitte ich hier um Abfrage in der Abteilung. Fehlanzeige ist **nicht** erforderlich.

Gleichzeitig bitte ich um Übermittlung eines Vermerks (Anlage Formatvorlage) wie nachstehend aufgeführt:

G II 2, H. Arhelger	Top 1 Ausblick ER	
	Top 5 Post-Stockholm-Prozess	BMI und BMJ sind gebeten, über das weitere Vorgehen nach dem JI-Rat zu informieren
VI 4	Top 2 Bankenunion Top 7 Monitoring VVV	
G II 2, H. Hofmann	Top 3 Ausblick GRC-Ratspräsidentschaft	Ressorts sind gebeten zu ergänzen
PG DS / PG NSA	Top 6 Datenschutz	Erste inhaltliche Bewertung der KOM-Mitteilungen v. 27.11.; BMI ist gebeten einzuführen
VI 5	Top 8 Verschiedenes	BMI ist gebeten, über das Verfahren BVerfG und die Auswirkungen auf die Vorbereitung der Wahl in DEU vorzutragen

Bitte senden Sie Ihren Beitrag **bis spätestens Montag, 09.12.2013 – 17:00 Uhr** an Referatspostfach G II 2.

Mit freundlichem Gruß
i. A. Petra Treber
Referat G II 2
Tel: 2402

2) RegGII2: z.Vg. (Anlagen nicht gesondert)

Von: Julia.Grzondziel@bmwi.bund.de [<mailto:Julia.Grzondziel@bmwi.bund.de>]

Gesendet: Freitag, 29. November 2013 16:13

An: BMVBS al-uj; BMZ Boellhoff, Uta; BMBF Burger, Susanne; ALG_; BMELV Guth, Dietrich; BMAS Koller, Heinz; BMFSFJ Linzbach, Christoph; BMJ Meyer-Cabri, Klaus Jörg; BK Neueder, Franz; AA Peruzzo, Guido; BMU Rid, Urban; BMBF Rieke, Volker; BMVG Schlie, Ulrich Stefan; BMG Scholten, Udo; BPA Spindeldreier, Uwe; AA Tempel, Peter; BMF Westphal, Thomas; Winands (BKM), Günter

Cc: BMVG BMVg Pol I 4; AA Scholz, Sandra Maria; AA Klitzing, Holger; laura.ahrens@diplo.de; Arhelger, Roland; BMAS Bechtle, Helena; 3-b-3-vz@auswaertiges-amt.de; BK Becker-Krüger, Maike; BKM-K34_; BMAS Referat VI a 1; 221@bmbf.bund.de; BMELV Referat 612; ea1@bmf.bund.de; BMFSFJ Freitag, Heinz; BMG Z32; euro@bmj.bund.de; EIII2@bmu.bund.de; BMVBS ref-ui22; dokumente.413@bmz.bund.de; AA Brökelmann, Sebastian; BMBF Brunnabend, Birgit; BMWI BUERO-EA1; BMWI BUERO-IB1; BMWI BUERO-IIA1; BMWI BUERO-IIA2; BMWI BUERO-VA3; BMELV Burbach, Rolf; BMVG Deertz, Axel; BMWI Dörr-Voß, Claudia; BMBF Drechsler, Andreas; BMFSFJ Elping, Nicole; BMU Ernstberger, Christian; BK Felsheim, Georg; GII2_; BMWI Gerling, Katja; Gorecki-Schöberl (BKM), Elisabeth; BMZ Gruschinski, Bernd; AA Sautter, Günter; BPA Köhn, Ulrich; BMU Kracht, Eva; BMZ Kreipe, Nils; Cornelia.Kuckuck@bmf.bund.de; BPA Lamberty, Karl-Heinz; BMG Langbein, Birte; AA Langhals, Werner; AA Leben, Wilfried; BMWI Leier, Klaus-Peter; BMWI Lepers, Rudolf; susanne.lietz@bmas.bund.de; BK Morgenstern, Albrecht; BMF Müller, Ralph; BMBF Müller-Roosen, Ingrid;

e-vz1@diplo.de; BMWI Obersteller, Andreas; BMWI Plessing, Wolf-Dieter; BMF Pohnert, Jürgen; BK Röhr, Ellen; BMWI Rüger, Andreas; EKR-L@auswaertiges-amt.de; e-vz2@diplo.de; BMFSFJ Simon, Roland; BMAS Strahl, Gabriela; Treber, Petra; AA Vossenkuhl, Ursula; BMFSFJ Walz, Christiane; BMU Werner, Julia; BMAS Winkler, Holger; AA Dieter, Robert; BMWI Drascher, Franziska

Betreff: (PT)_Einladung EU-AL-Sitzung am 12.12.2013 im BMWi

Sehr geehrte Damen und Herren,

anbei erhalten Sie die Einladung für die nächste Sitzung der Europa-Abteilungsleiter am 12.12.2013 im BMWi.

Mit freundlichen Grüßen
im Auftrag

Julia Grzondziel

Julia Grzondziel, LL.M. (London)
Referentin

Referat EA1; Grundsatzfragen EU-Politik, Koordinierung, Weisungsgebung
Bundesministerium für Wirtschaft und Technologie

Scharnhorststr. 34 - 37

10115 Berlin

Tel.: +49-(0)3018-615-6915

Fax: +49-(0)3018-615-50-6915

Email: Julia.Grzondziel@bmwi.bund.de

Homepage: <http://www.bmwi.de>



Bundesministerium
für Wirtschaft
und Technologie

Ministerialdirektorin
Claudia Dörr-Voß
-Leiterin der Europaabteilung-

Scharnhorststr. 34-37
11015 Berlin
Telefon Sekretariat: (03018) 615-7721
Telefax Sekretariat: (03018) 615-5481
E-Mail: claudia.doerr@bmwi.bund.de



Auswärtiges Amt

Ministerialdirigent
Arndt Freytag von Loringhoven
-Stellvertretender Leiter der
Europaabteilung-

Werderscher Markt 1
10113 Berlin
Telefon Sekretariat: (03018) 17-2336
Telefax Sekretariat: (03018) 17-4175
E-Mail: E-D@auswaertiges-amt.de

Berlin, den 29.11.2013

nur per E-Mail

Herrn MDg Dr. Neueder, Abtlg. 5, ChBK
Herrn MD Thomas Westphal, Leiter Abtlg. E, BMF
Herrn MD Dr. Bentmann, Leiter Abtlg. G, BMI
Herrn MDg Meyer-Cabri van Amelrode, Leiter EU-Koordination, BMJ
Herrn MD Koller, Leiter Abtlg. VI, BMAS
Herrn MD Dr. Guth, Leiter Abtlg. 6, BMELV
Herrn VA Scholten, Leiter Unterabtlg. Z3, BMG
Herrn MD Dr. Rid, Leiter Abtlg. E, BMU
Herrn Dr. Veit Steinle, Leiter Abtlg. UI, BMVBS
Herrn MD Rieke, Leiter Abtlg. 2, BMBF
Frau Dr. Böllhoff, Leiterin Abtlg. 4, BMZ
Herrn MD Spindeldreier, Leiter Abtlg. 3, BPA
Herrn MDg Linzbach, Leiter Unterabtlg. 31, BMFSFJ
Herrn Dr. Schlie, AL Pol, BMVg
Herrn MD Winands, BKM
Herrn Botschafter Tempel, StV Brüssel
Herrn Botschafter Dr. Peruzzo, StV Brüssel

nachrichtlich:

ChBK	z.Hd. Herrn VLR I Felsheim
AA	z.Hd. Herrn VLR I Schieb
BMWi	z.Hd. Herrn MR Leier
BMF	z.Hd. Herrn MR Müller
BMI	z.Hd. Herrn RD Dr. Christoph Hübner
BMAS	z.Hd. Herrn MR Winkler
BMELV	z.Hd. Herrn MR Burbach
BMVg	z.Hd. Herrn KzS Deertz
BMFSFJ	z.Hd. Frau Elping
BMG	z.Hd. Frau Langbein
BMVBS	z.Hd. Frau RDir'in Seefried
BMU	z.Hd. Frau RD'in Dr. Kracht
BMBF	z.Hd. Herrn MR Drechsler
BMZ	z.Hd. Herrn RD Gruschinski
BKM	z.Hd. Frau MR'in Gorecki-Schöberl

Seite 2 von 3 BPA z.Hd. Herrn MR Köhn
StV z.Hd. Herrn BR I Dieter
z.Hd. Herrn OAR Langhals

Betr.: Koordinierung der Europapolitik innerhalb der Bundesregierung

Sehr geehrte Kolleginnen und Kollegen,

wir laden Sie hiermit zu einer weiteren Besprechung zur Koordinierung der Europapolitik ein am

Donnerstag, den 12. Dezember 2013

um 8.30 Uhr

im BMWi, Saal 3 (Raum G 3.011, Gebäude G).

Für die **Bonner Ressorts** besteht die Möglichkeit, per Videokonferenz im **BMBF** Dienstsitz Bonn, Heinemannstraße 2, 53175 Bonn, Raum A2/1329, an der Besprechung teilzunehmen.

Folgende Themen sind bisher vorgesehen:

TOP 1: Ausblick auf den Europäischen Rat am 19./20. Dezember 2013

Ziel: Austausch über die Schwerpunkte des ER, ggf. Identifizierung von Nachsteuerungsbedarf.
Einführung durch AA, Ressorts werden gebeten zu ergänzen.

TOP 2: Bankenunion

Ziel: Information über den aktuellen Sachstand (auch zum weiteren Verfahren im EP bis zum Ende der Legislaturperiode).
BMF wird gebeten vorzutragen.

TOP 3: Ausblick auf die griechische EU-Ratspräsidentschaft im 1. Hj 2014

Ziel: Information über die Planungen der GRC-Präsidentschaft (auch zu Fragen betr. Dolmetschung bei informellen Ministertreffen), über evtl. Maßnahmen der BReg zur Unterstützung der GRC-Präsidentschaft sowie Identifizierung von möglichem Koordinierungsbedarf der BReg.
AA führt ein, Ressorts werden gebeten zu ergänzen.

TOP 4: Jugendbeschäftigung, KMU-Finanzierung

Ziel: Information über den Stand der Arbeiten auf EU-Ebene; Austausch über bilaterale Initiativen der Ressorts, insbes. auch für die Euro-Krisenländer.
BMAS und BMF werden gebeten einzuführen, Ressorts werden gebeten zu ergänzen.

Seite 3 von 3

TOP 5: Post-Stockholm-Programm

Ziel: Information zum Stand der Abstimmung einer DEU-Position und Austausch zum weiteren Vorgehen nach der Befassung des J/I-Rats.

BMI und **BMJ** werden gebeten, über das weitere Vorgehen nach dem J/I-Rat zu informieren.

Top 6: Datenschutz

Ziel: Erste inhaltliche Bewertung der am 27.11.2013 vorgelegten KOM-Mitteilungen und Austausch über das weitere Vorgehen.

BMI wird gebeten einzuführen.

Top 7: Monitoring Vertragsverletzungsverfahren

Ziel: Übersicht über aktuelle Vertragsverletzungsverfahren wegen Nichtmitteilung der Richtlinienumsetzung mit Zwangsgeldrisiko

BMWi trägt vor; **betroffene Ressorts** werden gebeten zu ergänzen, insbes. **BMJ** zur Nichtmitteilung der Umsetzungen von RL 2011/7 - Zahlungsverzugs-RL und von RL 2011/36 – Menschenhandels-RL.

TOP 8: Verschiedenes

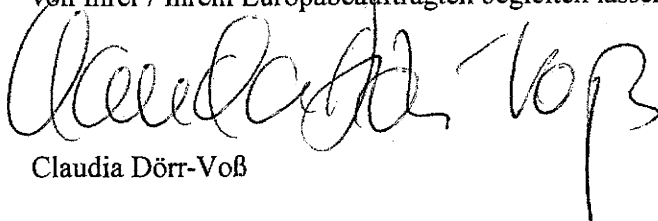
- **Europawahlgesetz:** **BMI** wird gebeten, über das Verfahren vor dem BVerfG und Auswirkungen auf die Vorbereitung der Wahl in DEU vorzutragen.
- **Europäisches Semester:** **BMWi** informiert über den Vorbereitungsprozess für das NRP 2014.
- **ETS/Luftverkehr:** **BMU** und **BMVBS** werden gebeten über den aktuellen Stand und die Position DEU-GBR-FRA zu berichten.

Sofern aus Sicht der Ressorts dringender Gesprächsbedarf zu weiteren Themen besteht, bitten wir Sie, diese bis

Montag, den 9. Dezember 2013, Dienstschluss

an das **AA, Referat E-KR** (LR I Sebastian Brökelmann, E-Mail: ekr-4@diplo.de, Tel. 030-1817 3945), und **BMWi, Referat E A 1** (ORR'in Julia Grzondziel, Tel. 615-6915, Fax: 615-7061, e-mail: Julia.Grzondziel@bmwi.bund.de) zu melden und mit **kurzen schriftlichen Angaben** zum Sachstand zu ergänzen.

Für die persönliche Wahrnehmung des Termins wären wir Ihnen dankbar. Wir schlagen vor, dass Sie sich von Ihrer / Ihrem Europabeauftragten begleiten lassen.



Claudia Dörr-Voß

gez.

Arndt Freytag von Loringhoven

Abteilungsleiterrunde zur Koordinierung der Europapolitik
am Donnerstag, dem 12. Dezember 2013 um 08.30 Uhr im BMWi

AG ÖS I 3 /PGDS
bearbeitet von: RR'n Elena Bratanova
RR Dr. Spitzer

Berlin, den 06.12.2013
HR: 45530
HR: 1390

TOP 6 Datenschutz

Anlagen: 6

Federführendes Ressort: BMI

I. **Gesprächsziel:**

Information über die am 27.11. durch KOM veröffentlichten Berichte.

II. **Sachverhalt/Sprechpunkte**

1 **Allgemein**

aktiv

- Am 27. November 2013 hat KOM folgende Berichte vorgelegt:
 - Feststellungen der "ad hoc EU-US working group on data protection" (Anlage 1); hierauf aufbauend wurde ein „Empfehlungspapier“ zur Einbringung in die laufende US-interne Evaluierung der Überwachungsprogramme auf EU-Ebene abgestimmt (Anlage 2);
 - **Strategiepapier über transatlantische Datenströme** (Anlage 3);
 - **Analyse des Funktionierens des Safe-Harbor-Abkommens** (Anlage 4);
 - **Bericht über das TFTP-Abkommen** (auch SWIFT-Abkommen genannt; Anlage 5)
- Darüber hinaus hat KOM am 27. November 2013 ihren Bericht über die **1. turnusmäßige Überprüfung der Durchführung des geltenden PNR-Abkommens zwischen der EU und den USA (Anlage 6)** vorgelegt, das am 1. Juli 2012 in Kraft getreten war (gem. Art. 23 des Abkommens überprüfen die Parteien die Durchführung des Abkommens ein Jahr nach Inkrafttreten und danach regelmäßig).

2. Abschlussbericht der „ad hoc EU-US working group on data protection“ und Empfehlungen für die US-interne Evaluierung der Überwachungsprogramme

aktiv

- Die „ad hoc EU US working group on data protection“ der KOM (DEU-Vertreter: UAL ÖS I Peters; „Working Group“) wurde **im Juli 2013 eingerichtet**, um „datenschutzrechtliche Fragestellungen im Hinblick auf personenbezogene Daten von EU-Bürgern, die von den US-Überwachungsprogrammen betroffen sind“, zu erörtern. Sie hat sich von **Juli bis November 2013 insgesamt vier Mal in Brüssel und in Washington** getroffen.
- Der **Abschlussbericht der KOM** (Anlage 1) beschränkt sich iW auf die **Darstellung der US-Rechtslage** (insbes. sec. 702 FISA, sec. 215 Patriot Act).
- Nachdem die **US-Seite im Rahmen der Working Group angeregt** hatte, eine EU-Position für den laufenden Prozess der US-internen Evaluierung der Überwachungsprogramme einzubringen, hat PRÄS ein **Papier mit Empfehlungen** vorgelegt (Anlage 2), das am 3. Dezember 2013 durch den AStV verabschiedet wurde und an die USA weitergegeben werden soll.
- Zentrale Forderungen des Papiers sind die **„Gleichbehandlung von US- und EU-Bürgern“**, **„Wahrung des Verhältnismäßigkeitsprinzips“** sowie **Stärkung des Rechtsschutzes** (für von Überwachungsmaßnahmen betroffene EU-Bürger). **DEU hat die Erarbeitung der Empfehlungen unterstützt.**

Inhaltliche Kurzbewertung:

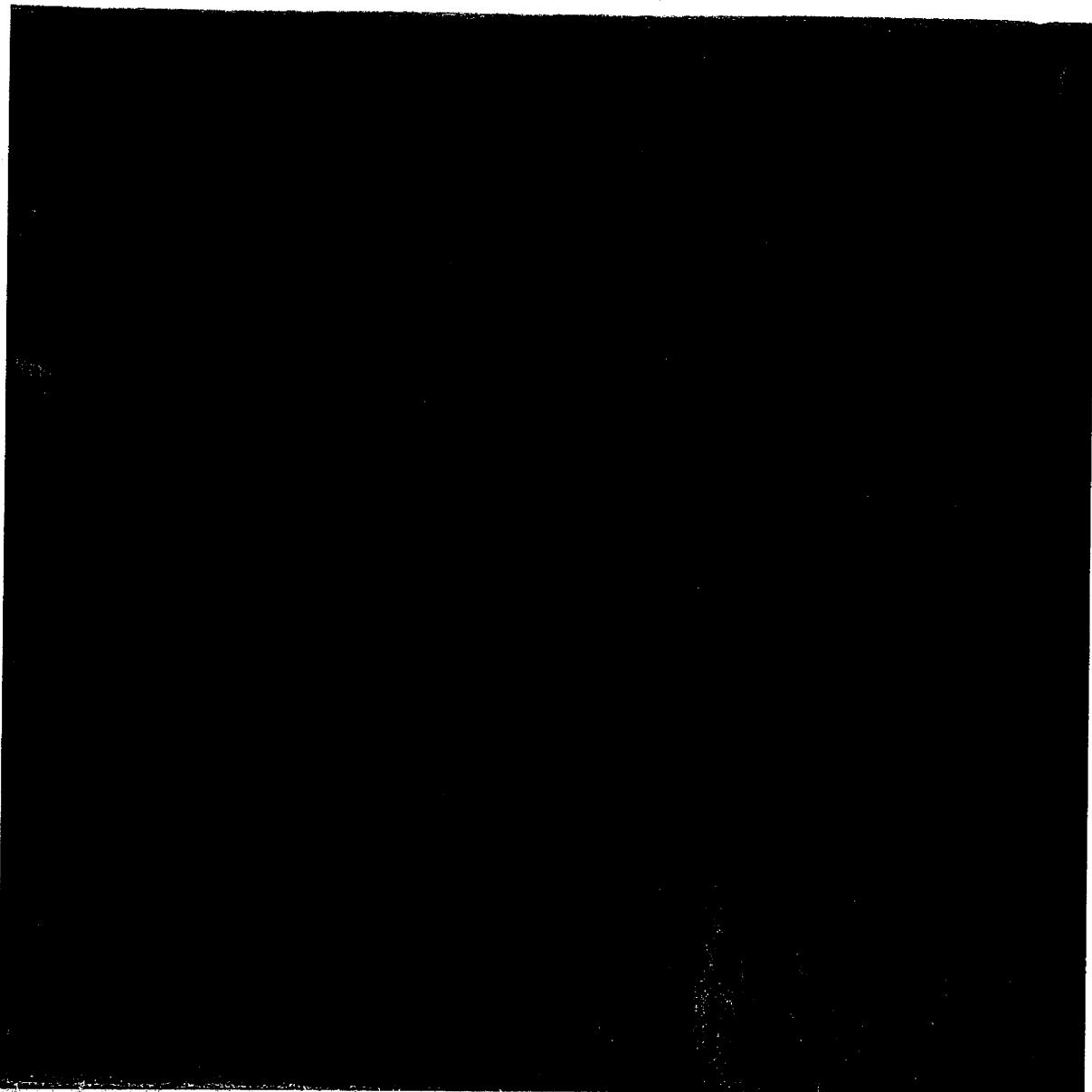
aktiv:

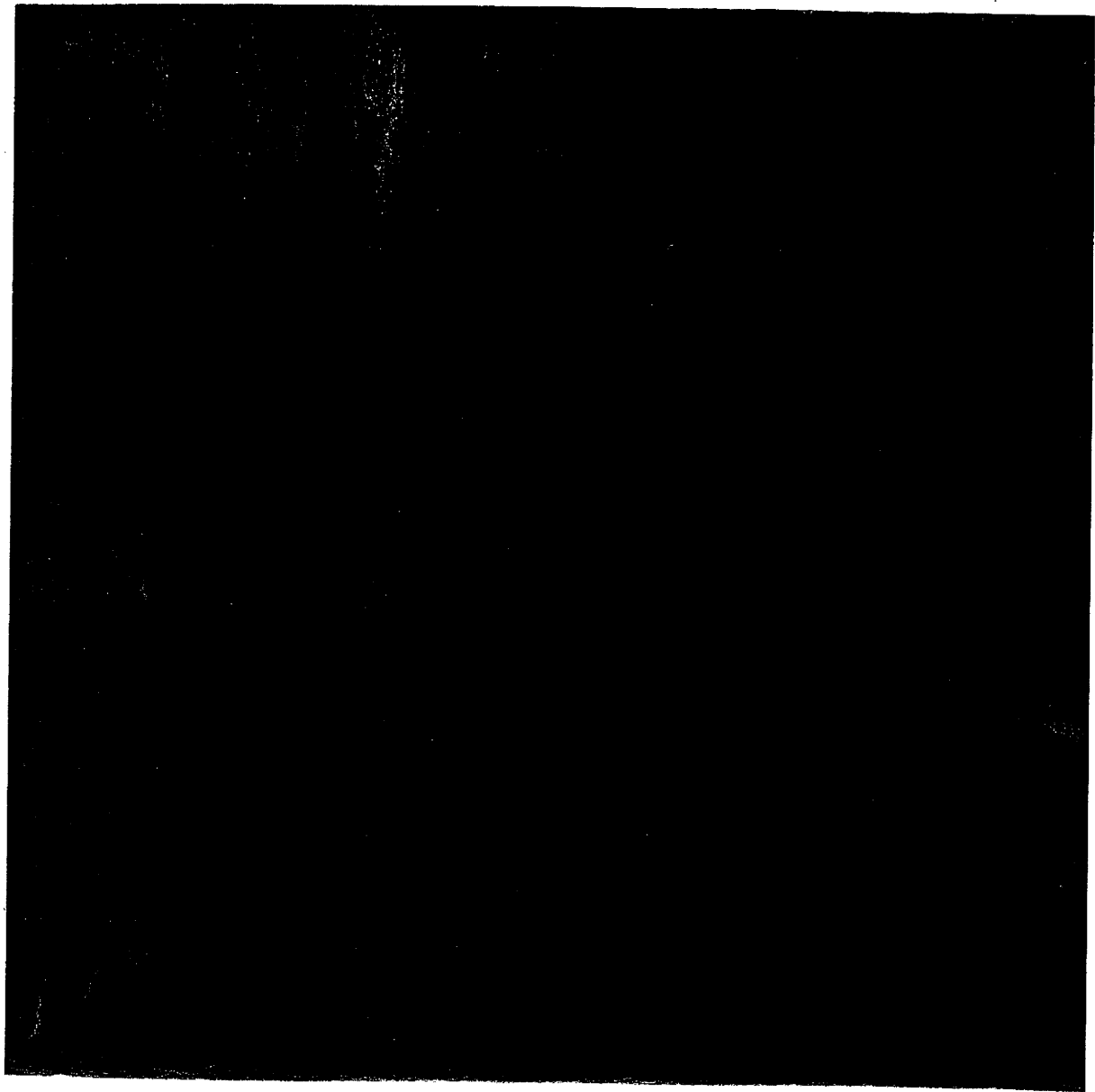
- Die vorliegenden Papiere sind **inhaltlich wenig überraschend** und vertretbar. Die Details zu den US-Rechtsgrundlagen sind im Wesentlichen bekannt. Die hieraus abgeleiteten Empfehlungen für eine (rechtliche) Neuaufstellung der US-Überwachungsprogramme sind grundsätzlich zu begrüßen.
- In **kompetenzieller Hinsicht** sind allerdings beide Papiere umstritten. Die EU hat ausdrücklich **keine Kompetenz zur Regelung der Tätigkeit der nationalen Nachrichtendienste.**

- Deshalb hat DEU gefordert, das Papier auch im **Namen der Mitgliedstaaten** veröffentlichen zu lassen.

reaktiv:

- Es lässt sich auch keine Zuständigkeit für ausländische Nachrichtendienste ableiten, soweit die EU auf dem Gebiet der Außenbeziehungen oder des Datenschutzrechts tätig wird (**keine „Annexregelung“**). Allenfalls soweit auf US-Seite das FBI (zwar nur als Antragsteller) in das Verfahren nach sec. 215 Patriot Act eingebunden ist, besteht eine EU-Kompetenz.





5. Bericht über das TFTP-Abkommen (Anlage 5)

Sachverhalt

aktiv

- Im Zusammenhang mit der Veröffentlichung der Snowden-Dokumente wurde in der Presse der Vorwurf erhoben, die NSA habe unter Umgehung des TFTP-Abkommens, das die Weiterleitungsmöglichkeiten von Daten des Finanzdienstleisters SWIFT aus der EU an die USA regelt und begrenzt, direkten Zugriff auf die SWIFT-Server genommen.
- Am 23. Oktober 2013 hat das EP in einer Entschließung KOM aufgefordert, das zwischen der EU und den USA geschlossene Abkommen auszusetzen. KOM'n Malmström hat nach Bekanntwerden der Vorwürfe Konsultationen mit den USA eingeleitet. Diese sind zwischenzeitlich abgeschlossen worden. KOM ist zu dem Schluss gelangt, dass keine Anhaltspunkte für einen Verstoß gegen das Abkommen vorliegen.
- Parallel dazu hat die KOM (wie in Art. 6 Abs. 6 des Abkommens vorgesehen) drei Jahre nach Inkrafttreten des Abkommens (Stichtag:

1. August 2013) gemeinsam mit den USA den Nutzen der bereitgestellten TFTP-Daten evaluiert und den betreffenden Bericht (Anlage 6) am 27. November 2013 veröffentlicht.

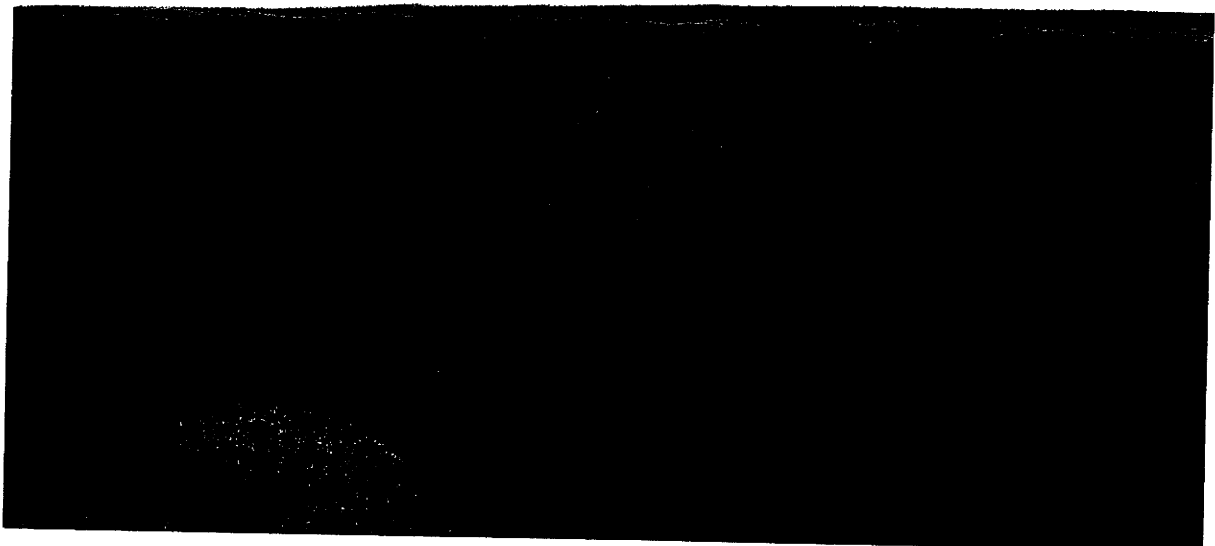
- KOM und USA kommen darin zu dem Schluss, dass die generierten Daten einen signifikanten Beitrag zur Bekämpfung der Terrorismusfinanzierung leisten. Durch die Rekonstruktion von Finanzgeflechten könnten Informationen über Organisationen und Einzelpersonen generiert werden. Auch wird auf die Bedeutung der fünfjährigen Speicherdauer hingewiesen, die keinesfalls verkürzt werden sollte.

Inhaltliche Kurzbewertung:

- Da Vertragsparteien des TFTP-Abkommens die EU und die USA sind, war es Aufgabe der KOM, die gegen die USA erhobenen Vorwürfe aufzuklären. Erst danach konnte über eine Suspendierung oder Kündigung nachgedacht werden.
- BMI ist nicht bekannt, dass die NSA unter Umgehung des Abkommens Zugriff auf SWIFT -Daten zugreift. Mit Vorliegen des Untersuchungsergebnisses der KOM, dass kein Verstoß gegen das Abkommen vorliegt, besteht derzeit kein Anlass, das Abkommen auszusetzen.

⇒ *Hintergrundinformation: Der **Koalitionsvertrag** sieht vor, dass die neue Bundesregierung in der EU auf Nachverhandlungen mit den USA dringen wird, um die im Abkommen enthaltenen Datenschutzregelungen zu verbessern.*

- Das Ergebnis des Evaluierungsberichts war aus hiesiger Sicht zu erwarten. Auch BKA und BfV haben bestätigt, dass die von den USA weitergegebenen TFTP-Daten hilfreich waren, da vorhandene Kenntnisse angereichert und/oder bestätigt werden konnten.



Bl. 243

Entnahme wegen fehlenden Bezugs zum
Untersuchungsgegenstand

Dokument 2014/0067402

Von: Weinbrenner, Ulrich
Gesendet: Dienstag, 17. Dezember 2013 16:41
An: PGNSA; Jergl, Johann; Stöber, Karlheinz, Dr.; Taube, Matthias
Betreff: : LIBE-Agenda mit Glenn Greenwold
Anlagen: Agenda 17-18 December 2013.pdf

zKts.

Mit freundlichem Gruß

Ulrich Weinbrenner

Bundesministerium des Innern
Leiter der Arbeitsgruppe ÖS I 3
Polizeiliches Informationswesen, BKA-Gesetz,
Datenschutz im Sicherheitsbereich
Tel.: + 49 30 3981 1301
Fax.: + 49 30 3981 1438
PC-Fax.: 01888 681 51301
Ulrich.Weinbrenner@bmi.bund.de

Von: .BRUEEU POL-IN2-2-EU Eickelpasch, Joerg [mailto:pol-in2-2-eu@brue.auswaertiges-amt.de]
Gesendet: Dienstag, 17. Dezember 2013 16:26
An: Weinbrenner, Ulrich
Betreff: LIBE-Agenda

Lieber Herr Weinbrenner,

wie besprochen.

Mit freundlichen Grüßen,
Jörg Eickelpasch



EUROPEAN PARLIAMENT

2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens

Draft programme

Tuesday, 17 December, 17.00 - 18.30 (JAN 6Q2)
Wednesday, 18 December 2013, 9:00 - 13:00 (JAN 2Q2)

Brussels

Meeting room: JAN 2Q2

17 December 2013, room 6Q2

17:00 Introductory remarks by Mr Claude MORAES, Rapporteur for the LIBE Committee Inquiry on Mass surveillance.

<p style="text-align: center;">SESSION I Parliamentary Committee of Inquiry on Espionage of the Brazilian Senate (Videoconference)</p>

- | | |
|---------------|---|
| 17:15 – 17:35 | Statement by <ul style="list-style-type: none">• Ms Vanessa GRAZZIOTIN, Chair of the Parliamentary Committee of Inquiry on Espionage• Mr Ricardo DE REZENDE FERRAÇO, Rapporteur of the Parliamentary Committee of Inquiry on Espionage |
| 17:35 – 18:20 | Questions & Answers |
| 18:20 – 18:30 | Concluding remarks and follow-up |

18 December 2013, room 2Q2

9:00 Introductory remarks by Ms Sophie IN'T VELD, Vice-Chair of the LIBE Committee

SESSION II IT Means of protecting privacy
--

- 09:05 – 09:25 Statement by
- Mr Bart PRENEEL, Professor in Computer Security and Industrial Cryptography in the University KU Leuven, Belgium
 - Mr Stephan LECHNER, Director, Institute for the Protection and Security of the Citizen (IPSC), - Joint Research Centre(JRC), European Commission
- 09:25 – 10:00 Questions & Answers
- 10:00 – 10:20 Statement by
- Dr. Christopher SOGHOIAN, Principal Technologist, Speech, Privacy & Technology Project, American Civil Liberties Union
 - Christian HORCHERT, IT-Security Consultant, Germany
- 10:20 – 11:00 Questions & Answers

SESSION III Presentation of Working Documents (Part III) (tbc)

- 11:00 – 11:10 Presentation of the Working Document on "Scope of International, European and national security in the EU perspective" co-authored by the Rapporteur, Mr Moraes and by Mr. Kirkhope, Shadow Rapporteur
- 11.10 – 11.25 Questions & Answers

SESSION IV Exchange of views with the journalist having made public the facts (Part II)(Videoconference)

- 11:30 – 12:00 Statement by
- Mr Glenn GREENWALD, Author and columnist with a focus on national security and civil liberties, formerly of the Guardian
- 12:00 – 12:30 Questions & Answers

SESSION V
Presentation of the Draft Report

- | | |
|---------------|--|
| 12:30 - 12:55 | Presentation of the Draft Report by the Rapporteur, Mr Claude Moraes |
| 12:55 - 13:00 | Concluding remarks and follow-up |

Dokument 2014/0067398

Von: Weinbrenner, Ulrich
Gesendet: Mittwoch, 18. Dezember 2013 15:08
An: PGNSA; Jergl, Johann; Schäfer, Ulrike; Richter, Annegret; Stöber, Karlheinz, Dr.
Cc: Spitzer, Patrick, Dr.
Betreff: WG: 1. EU-Datenschutzreform und 2. EP-Untersuchungsausschuss zu Überwachungssystemen

zKts.

Mit freundlichem Gruß

Ulrich Weinbrenner

Bundesministerium des Innern
 Leiter der Arbeitsgruppe ÖS I 3
 Polizeiliches Informationswesen, BKA-Gesetz,
 Datenschutz im Sicherheitsbereich
 Tel.: + 49 30 3981 1301
 Fax.: + 49 30 3981 1438
 PC-Fax.: 01888 681 51301
 Ulrich.Weinbrenner@bmi.bund.de

Von: .BRUEEU POL-IN2-2-EU Eickelpasch, Joerg [mailto:pol-in2-2-eu@brue.auswaertiges-amt.de]
Gesendet: Mittwoch, 18. Dezember 2013 14:47
An: Stentzel, Rainer, Dr.; PGDS_; IT1_; OESI3AG_; Binder, Thomas; Spitzer, Patrick, Dr.; Lesser, Ralf; Mammen, Lars, Dr.; Knobloch, Hans-Heinrich von; Weinbrenner, Ulrich; BK Hornung, Ulrike; Hübner, Christoph, Dr.; Franßen-Sanchez de la Cerda, Boris; Kuczynski, Alexandra; Peters, Reinhard; Scheuring, Michael; Korff, Annegret
Cc: Thomas Pohl (t.pohl@diplo.de)
Betreff: 1. EU-Datenschutzreform und 2. EP-Untersuchungsausschuss zu Überwachungssystemen

Liebe Kolleginnen und Kollegen,

noch einige Information.....

1. EU-Datenschutzreform

Der zuständige JI-Referent GRC teilte mir heute (bestätigend) mit, dass sich die Dapix vom 8. - 10. Januar 2014 mit dem Kapitel 9 der Grundverordnung und mit ausgewählten Themen aus den ersten vier Kapiteln befassen werde. Er nannte konkret die Themen Profilbildung und pseudonyme Daten. Ferner plant GRC-Vorsitz beim informellen Rat das Thema Drittstaatstransfer (Kapitel V der Verordnung) zu behandeln. Zur Vorbereitung soll sich die RAG Dapix am 20./21. Januar 2014 hiermit befassen.

2. EP-Untersuchungsausschuss zu Überwachungssystemen

Der Berichterstatter des LIBE-Untersuchungsausschusses (MdEP Moraes, S & D) versprach in der heutigen Sitzung des LIBE, bis Ende dieser Woche einen Berichtsentwurf an die Schattenberichterstatter (u.a. MdEP Voss, Albrecht, Kirkhope) senden zu wollen. Er wolle noch das Urteil des US-Richters (siehe insofern gestrige Pressemeldungen) zur Verfassungswidrigkeit der NSA-Praxis, umfassend und anlasslos Metadaten zu verarbeiten, berücksichtigen. Über Weihnachten könnten die „Shadows“ dann den Bericht prüfen, anschließend solle er am 9. Januar 2014 im LIBE beraten werden. Frist zur Abgabe von Änderungsanträgen sei schließlich der 13. Januar 2013.

Für Rückfragen stehe ich gerne zur Verfügung und wünsche Ihnen/Euch bereits auf diesem Wege ein frohes Fest!

Jörg Eickelpasch

Jörg Eickelpasch

Ständige Vertretung der Bundesrepublik Deutschland bei der Europäischen Union

EU-Datenschutzreform/Schengenangelegenheiten

8-14, rue Jacques de Lalaing
B-1040 Brüssel

Tel: 0032-(0)2-787-1051

Fax: 0032-(0)2-787-2051

Mobile: 0032-(0)476-760868

e-mail: pol-in2-2-eu@brue.auswaertiges-amt.de

INVALID HTML

Kuczynski, Alexandra

Von: PStSchröder_
Gesendet: Freitag, 10. Januar 2014 11:14
An: ALOES_
Cc: StFritsche_; UALOESI_; StabOESI_; UALGII_; OESI3AG_; MB_; Baum, Michael, Dr.; PStSchröder_; AA Eickelpasch, Jörg
Betreff: LIBE Berichtsentwurf NSA mdB um Stellungnahme bis 17.1.
Anlagen: moraes_1014703_en.pdf

Vg. 13/14

Sehr geehrter Herr Kaller,

Herr PStS hat den beigefügten Berichtsentwurf von Herrn Voss, MdEP, erhalten. Dies war verbunden mit dem Angebot, Anregungen für Änderungsvorschläge einzubringen, die MdEP Voss bis 22.1. ggü. LIBE-Ausschuss einbringen könnte.

Vor diesem Hintergrund bittet Herr PStS um Prüfung, Stellungnahme und ggf. weitergabefähige Vorschläge für Änderungsanträge bis **Freitag, den 17.1. DS** (Eingang Büro PStS).

Zum Verfahren waren folgende Informationen beigefügt:

Es handelt sich um den Berichtsentwurf von Berichterstatter Claude Moraes (S&D, UK) der NSA-Arbeitsgruppe zum Thema "US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs". Der Berichtsentwurf stellt das Abschlussdokument der NSA-Arbeitsgruppe dar. Diese wurde per Entschließungsantrag am 4. Juli 2013 im Rahmen des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) eingerichtet, um den Sachverhalt um die mutmaßliche Internetüberwachung durch die NSA zu untersuchen und dem LIBE-Ausschuss seine Erkenntnisse in Form eines Endberichts vorzulegen. Nach 15 Anhörungen liegt dieser Bericht nun zur Prüfung vor und kann nun durch Änderungsanträge abgeändert werden.

Frist für Änderungsanträge ist der 22. Januar. Der weitere Zeitplan sieht eine Abstimmung im LIBE-Ausschuss im Februar und anschließend eine Abstimmung im Plenum im März vor.

Mit freundlichen Grüßen

Im Auftrag

Alexandra Kuczynski

Bundesministerium des Innern
Persönliche Referentin des
Parlamentarischen Staatssekretärs Dr. Ole Schröder
Alt-Moabit 101 D, 10559 Berlin

Telefon: +49 (0)30 18 681 1056
Fax: +49 (0)30 18 681 1137
E-Mail: alexandra.kuczynski@bmi.bund.de

Prinz, Judith-Petra

Von: VOSS Axel [axel.voss@europarl.europa.eu]
Gesendet: Donnerstag, 9. Januar 2014 18:19
An: PStSchröder_
Betreff: Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA
Anlagen: moraes_1014703_en.pdf

Sehr geehrter Herr Dr. Schröder,

anbei sende ich Ihnen im Auftrag von Herrn Voss (MdEP) den Berichtsentwurf von Berichterstatter Claude Moraes (S&D, UK) der NSA-Arbeitsgruppe zum Thema "US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs". Der Berichtsentwurf stellt das Abschlussdokument der NSA-Arbeitsgruppe dar. Diese wurde per Entschließungsantrag am 4. Juli 2013 im Rahmen des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) eingerichtet, um den Sachverhalt um die mutmaßliche Internetüberwachung durch die NSA zu untersuchen und dem LIBE-Ausschuss seine Erkenntnisse in Form eines Endberichts vorzulegen. Nach 15 Anhörungen liegt dieser Bericht nun zur Prüfung vor und kann nun durch Änderungsanträge abgeändert werden.

Sollten Sie Ideen oder Anregungen für Änderungsvorschläge haben, sind diese gerne willkommen. Frist für Änderungsanträge ist der 22. Januar. Der weitere Zeitplan sieht eine Abstimmung im LIBE-Ausschuss im Februar und anschließend eine Abstimmung im Plenum im März vor.

Falls Sie Fragen haben sollten oder weiter Informationen benötigen, stehe ich Ihnen gerne zur Verfügung.

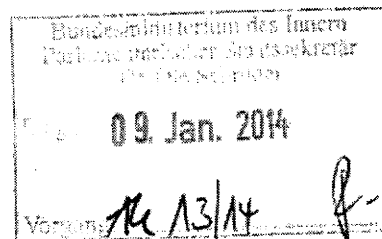
Mit freundlichen Grüßen,

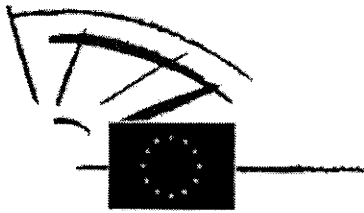
Selma Toporan

Selma Toporan
 (Parlamentarische Referentin)

Büro Axel Voss, MdEP
 Europäisches Parlament
 ASP 15 E 150
 Rue Wiertz
 B-1047 Brüssel

Tel.: +32-2-28 47302
 Fax: +32-2-28 49302
 Email: selma.toporan@europarl.europa.eu





EUROPEAN PARLIAMENT

2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

2013/2188(INI)

8.1.2014

DRAFT REPORT

on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs

(2013/2188(INI))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Claude Moraes

PR_INI

CONTENTS

	Page
MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION.....	3
EXPLANATORY STATEMENT.....	35
ANNEX I: LIST OF WORKING DOCUMENTS.....	42
ANNEX II: LIST OF HEARINGS AND EXPERTS.....	43
ANNEX III: LIST OF EXPERTS WHO DECLINED PARTICIPATING IN THE LIBE INQUIRY PUBLIC HEARINGS.....	51

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs
(2013/2188(INI))

The European Parliament,

- having regard to the Treaty on European Union (TEU), in particular Articles 2, 3, 4, 5, 6, 7, 10, 11 and 21 thereof,
- having regard to the Treaty on the Functioning of the European Union (TFEU), in particular Articles 15, 16 and 218 and Title V thereof,
- having regard to Protocol 36 on transitional provisions and Article 10 thereof and to Declaration 50 concerning this protocol,
- having regard to the Charter on Fundamental Rights of the European Union, in particular Articles 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 and 52 thereof,
- having regard to the European Convention on Human Rights, notably its Articles 6, 8, 9, 10 and 13, and the protocols thereto,
- having regard to the Universal Declaration of Human Rights, notably its Articles 7, 8, 10, 11, 12 and 14¹,
- having regard to the International Covenant on Civil and Political Rights, notably its Articles 14, 17, 18 and 19,
- having regard to the Council of Europe Convention on Data Protection (ETS No 108) and its Additional Protocol of 8 November 2001 to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No 181),
- having regard to the Council of Europe Convention on Cybercrime (ETS No 185),
- having regard to the Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, submitted on 17 May 2010²,
- having regard to the Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, submitted on 17 April 2013³,
- having regard to the Guidelines on human rights and the fight against terrorism

¹ <http://www.un.org/en/documents/udhr/>

² <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement>

³ http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

adopted by the Committee of Ministers of the Council of Europe on 11 July 2002,

- having regard to the Declaration of Brussels of 1 October 2010, adopted at the 6th Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States,
- having regard to Council of Europe Parliamentary Assembly Resolution No 1954 (2013) on national security and access to information,
- having regard to the report on the democratic oversight of the security services adopted by the Venice Commission on 11 June 2007¹, and expecting with great interest the update thereof, due in spring 2014,
- having regard to the testimonies of the representatives of the oversight committees on intelligence of Belgium, the Netherlands, Denmark and Norway,
- having regard to the cases lodged before the French², Polish and British³ courts, as well as before the European Court of Human Rights⁴, in relation to systems of mass surveillance,
- having regard to the Convention established by the Council in accordance with Article 34 of the Treaty on European Union on Mutual Assistance in Criminal Matters between the Member States of the European Union, and in particular to Title III thereof⁵,
- having regard to Commission Decision 520/2000 of 26 July 2000 on the adequacy of the protection provided by the Safe Harbour privacy principles and the related frequently asked questions (FAQs) issued by the US Department of Commerce,
- having regard to the Commission assessment reports on the implementation of the Safe Harbour privacy principles of 13 February 2002 (SEC(2002)196) and of 20 October 2004 (SEC(2004)1323),
- having regard to the Commission Communication of 27 November 2013 (COM(2013)847) on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU and the Commission Communication of 27 November 2013 on rebuilding trust in EU-US data flows (COM(2013)846),
- having regard to the European Parliament resolution of 5 July 2000 on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, which took the view that the adequacy of the system could not be

¹ [http://www.venice.coe.int/webforms/documents/CDL-AD\(2007\)016.aspx](http://www.venice.coe.int/webforms/documents/CDL-AD(2007)016.aspx)

² La Fédération Internationale des Ligues des Droits de l'Homme and La Ligue française pour la défense des droits de l'Homme et du Citoyen against X; Tribunal de Grande Instance of Paris.

³ Cases by Privacy International and Liberty in the Investigatory Powers Tribunal.

⁴ Joint Application Under Article 34 of Big Brother Watch, Open Rights Group, English Pen Dr Constanze Kurz (Applicants) - v - United Kingdom (Respondent).

⁵ OJ C 197, 12.7.2000, p. 1.

confirmed¹, and to the Opinions of the Article 29 Working Party, more particularly Opinion 4/2000 of 16 May 2000²,

- having regard to the agreements between the United States of America and the European Union on the use and transfer of passenger name records (PNR agreement) of 2004, 2007³ and 2012⁴,
- having regard to the Joint Review of the implementation of the Agreement between the EU and the USA on the processing and transfer of passenger name records to the US Department of Homeland Security⁵, accompanying the report from the Commission to the European Parliament and to the Council on the joint review (COM(2013)844),
- having regard to the opinion of Advocate-General Cruz Villalón concluding that Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks is as a whole incompatible with Article 52(1) of the Charter of Fundamental Rights of the European Union and that Article 6 thereof is incompatible with Articles 7 and 52(1) of the Charter⁶,
- having regard to Council Decision 2010/412/EU of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (TFTP)⁷ and the accompanying declarations by the Commission and the Council,
- having regard to the Agreement on mutual legal assistance between the European Union and the United States of America⁸,
- having regard to the ongoing negotiations on an EU-US framework agreement on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters (the 'Umbrella agreement'),
- having regard to Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom⁹,
- having regard to the statement by the President of the Federative Republic of Brazil at

¹ OJ C 121, 24.4.2001, p. 152.

² <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf>

³ OJ L 204, 4.8.2007, p. 18.

⁴ OJ L 215, 11.8.2012, p. 5.

⁵ SEC(2013)630, 27.11.2013.

⁶ Opinion of Advocate General Cruz Villalón, 12 December 2013, Case C-293/12.

⁷ OJ L 195, 27.7.2010, p. 3.

⁸ OJ L 181, 19.7.2003, p. 34.

⁹ OJ L 309, 29.11.1996, p.1.

the opening of the 68th session of the UN General Assembly on 24 September 2013 and to the work carried out by the Parliamentary Committee of Inquiry on Espionage established by the Federal Senate of Brazil,

- having regard to the US PATRIOT Act signed by President George W. Bush on 26 October 2001,
- having regard to the Foreign Intelligence Surveillance Act (FISA) of 1978 and the FISA Amendments Act of 2008,
- having regard to Executive Order No 12333, issued by the US President in 1981 and amended in 2008,
- having regard to legislative proposals currently under examination in the US Congress, in particular the draft US Freedom Act,
- having regard to the reviews conducted by the Privacy and Civil Liberties Oversight Board, the US National Security Council and the President's Review Group on Intelligence and Communications Technology, particularly the report by the latter of 12 December 2013 entitled 'Liberty and Security in a Changing World',
- having regard to the ruling of the United States District Court for the District of Columbia, *Klayman et al. v Obama et al.*, Civil Action No 13-0851 of 16 December 2013,
- having regard to the report on the findings by the EU Co-Chairs of the ad hoc EU-US Working Group on data protection of 27 November 2013¹,
- having regard to its resolutions of 5 September 2001 and 7 November 2002 on the existence of a global system for the interception of private and commercial communications (ECHELON interception system),
- having regard to its resolution of 21 May 2013 on the EU Charter: standard settings for media freedom across the EU²,
- having regard to its resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens, whereby it instructed its Committee on Civil Liberties, Justice and Home Affairs to conduct an in-depth inquiry into the matter³,
- having regard to its resolution of 23 October 2013 on organised crime, corruption and money laundering: recommendations on action and initiatives to be taken⁴,
- having regard to its resolution of 23 October 2013 on the suspension of the TFTP

¹ Council document 16987/13.

² Texts adopted, P7_TA(2013)0203.

³ Texts adopted, P7_TA-(2013)0322.

⁴ Texts adopted, P7_TA(2013)0444.

- agreement as a result of US National Security Agency surveillance¹,
- having regard to its resolution of 10 December 2013 on unleashing the potential of cloud computing²,
 - having regard to the interinstitutional agreement between the European Parliament and the Council concerning the forwarding to and handling by the European Parliament of classified information held by the Council on matters other than those in the area of the common foreign and security policy³,
 - having regard to Annex VIII of its Rules of Procedure,
 - having regard to Rule 48 of its Rules of Procedure,
 - having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs (A70000/2013),

The impact of mass surveillance

- A. whereas the ties between Europe and the United States of America are based on the spirit and principles of democracy, liberty, justice and solidarity;
- B. whereas mutual trust and understanding are key factors in the transatlantic dialogue;
- C. whereas in September 2001 the world entered a new phase which resulted in the fight against terrorism being listed among the top priorities of most governments; whereas the revelations based on leaked documents from Edward Snowden, former NSA contractor, put democratically elected leaders under an obligation to address the challenges of the increasing capabilities of intelligence agencies in surveillance activities and their implications for the rule of law in a democratic society;
- D. whereas the revelations since June 2013 have caused numerous concerns within the EU as to:
 - the extent of the surveillance systems revealed both in the US and in EU Member States;
 - the high risk of violation of EU legal standards, fundamental rights and data protection standards;
 - the degree of trust between EU and US transatlantic partners;
 - the degree of cooperation and involvement of certain EU Member States with US surveillance programmes or equivalent programmes at national level as unveiled by the media;
 - the degree of control and effective oversight by the US political authorities and certain EU Member States over their intelligence communities;

¹ Texts adopted, P7_TA(2013)0449.

² Texts adopted, P7_TA(2013)0535.

³ OJ C 353 E, 3.12.2013, p.156-167.

- the possibility of these mass surveillance operations being used for reasons other than national security and the strict fight against terrorism, for example economic and industrial espionage or profiling on political grounds;
 - the respective roles and degree of involvement of intelligence agencies and private IT and telecom companies;
 - the increasingly blurred boundaries between law enforcement and intelligence activities, leading to every citizen being treated as a suspect;
 - the threats to privacy in a digital era;
- E. whereas the unprecedented magnitude of the espionage revealed requires full investigation by the US authorities, the European Institutions and Members States' governments and national parliaments;
- F. whereas the US authorities have denied some of the information revealed but not contested the vast majority of it; whereas the public debate has developed on a large scale in the US and in a limited number of EU Member States; whereas EU governments too often remain silent and fail to launch adequate investigations;
- G. whereas it is the duty of the European Institutions to ensure that EU law is fully implemented for the benefit of European citizens and that the legal force of EU Treaties is not undermined by a dismissive acceptance of extraterritorial effects of third countries' standards or actions;

Developments in the US on reform of intelligence

- H. whereas the District Court for the District of Columbia, in its Decision of 16 December 2013, has ruled that the bulk collection of metadata by the NSA is in breach of the Fourth Amendment to the US Constitution¹;
- I. whereas a Decision of the District Court for the Eastern District of Michigan has ruled that the Fourth Amendment requires reasonableness in all searches, prior warrants for any reasonable search, warrants based upon prior-existing probable cause, as well as particularity as to persons, place and things and the interposition of a neutral magistrate between Executive branch enforcement officers and citizens²;
- J. whereas in its report of 12 December 2013, the President's Review Group on Intelligence and Communication Technology proposes 45 recommendations to the President of the US; whereas the recommendations stress the need simultaneously to protect national security and personal privacy and civil liberties; whereas in this regard it invites the US Government to end bulk collection of phone records of US persons under Section 215 of the Patriot Act as soon as practicable, to undertake a thorough review of the NSA and the US intelligence legal framework in order to ensure respect for the right to privacy, to end efforts to subvert or make vulnerable commercial software (backdoors and malware), to increase the use of encryption, particularly in

¹ Klayman et al. v Obama et al., Civil Action No 13-0851, 16 December 2013.

² ACLU v: NSA No 06-CV-10204, 17 August 2006.

the case of data in transit, and not to undermine efforts to create encryption standards, to create a Public Interest Advocate to represent privacy and civil liberties before the Foreign Intelligence Surveillance Court, to confer on the Privacy and Civil Liberties Oversight Board the power to oversee Intelligence Community activities for foreign intelligence purposes, and not only for counterterrorism purposes, and to receive whistleblowers' complaints, to use Mutual Legal Assistance Treaties to obtain electronic communications, and not to use surveillance to steal industry or trade secrets;

- K. whereas in respect of intelligence activities about non-US persons under Section 702 of FISA, the Recommendations to the President of the USA recognise the fundamental issue of respect for privacy and human dignity enshrined in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights; whereas they do not recommend granting non-US persons the same rights and protections as US persons;

Legal framework

Fundamental rights

- L. whereas the report on the findings by the EU Co-Chairs of the ad hoc EU-US Working Group on data protection provides for an overview of the legal situation in the US but has not helped sufficiently with establishing the facts about US surveillance programmes; whereas no information has been made available about the so-called 'second track' Working Group, under which Member States discuss bilaterally with the US authorities matters related to national security;
- M. whereas fundamental rights, notably freedom of expression, of the press, of thought, of conscience, of religion and of association, private life, data protection, as well as the right to an effective remedy, the presumption of innocence and the right to a fair trial and non-discrimination, as enshrined in the Charter on Fundamental Rights of the European Union and in the European Convention on Human Rights, are cornerstones of democracy;

Union competences in the field of security

- N. whereas according to Article 67(3) TFEU the EU 'shall endeavour to ensure a high level of security'; whereas the provisions of the Treaty (in particular Article 4(2) TEU, Article 72 TFEU and Article 73 TFEU) imply that the EU disposes of certain competences on matters relating to the collective security of the Union; whereas the EU has exercised competence in matters of internal security by deciding on a number of legislative instruments and concluding international agreements (PNR, TFTP) aimed at fighting serious crime and terrorism and by setting up an internal security strategy and agencies working in this field;
- O. whereas the concepts of 'national security', 'internal security', 'internal security of the EU' and 'international security' overlap; whereas the Vienna Convention on the Law of Treaties, the principle of sincere cooperation among EU Member States and the human rights law principle of interpreting any exemptions narrowly point towards a

restrictive interpretation of the notion of 'national security' and require that Member States refrain from encroaching upon EU competences;

- P. whereas, under the ECHR, Member States' agencies and even private parties acting in the field of national security also have to respect the rights enshrined therein, be they of their own citizens or of citizens of other States; whereas this also goes for cooperation with other States' authorities in the field of national security;

Extra-territoriality

- Q. whereas the extra-territorial application by a third country of its laws, regulations and other legislative or executive instruments in situations falling under the jurisdiction of the EU or its Member States may impact on the established legal order and the rule of law, or even violate international or EU law, including the rights of natural and legal persons, taking into account the extent and the declared or actual aim of such an application; whereas, in these exceptional circumstances, it is necessary to take action at the EU level to ensure that the rule of law, and the rights of natural and legal persons are respected within the EU, in particular by removing, neutralising, blocking or otherwise countering the effects of the foreign legislation concerned;

International transfers of data

- R. whereas the transfer of personal data by EU institutions, bodies, offices or agencies or by the Member States to the US for law enforcement purposes in the absence of adequate safeguards and protections for the respect of fundamental rights of EU citizens, in particular the rights to privacy and the protection of personal data, would make that EU institution, body, office or agency or that Member State liable, under Article 340 TFEU or the established case law of the CJEU¹, for breach of EU law – which includes any violation of the fundamental rights enshrined in the EU Charter;

Transfers to the US based on the US Safe Harbour

- S. whereas the US data protection legal framework does not ensure an adequate level of protection for EU citizens;
- T. whereas, in order to enable EU data controllers to transfer personal data to an entity in the US, the Commission, in its Decision 520/2000, has declared the adequacy of the protection provided by the Safe Harbour privacy principles and the related FAQs issued by the US Department of Commerce for personal data transferred from the Union to organisations established in the United States that have joined the Safe Harbour;
- U. whereas in its resolution of 5 July 2000 the European Parliament expressed doubts and concerns as to the adequacy of the Safe Harbour and called on the Commission to review the decision in good time in the light of experience and of any legislative developments;

¹ See notably Joined Cases C-6/90 and C-9/90, *Francovich and others v. Italy*, judgment of 28 May 1991.

- V. whereas Commission Decision 520/2000 stipulates that the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Safe Harbour principles, in order to protect individuals with regard to the processing of their personal data in cases where there is a substantial likelihood that the Safe Harbour principles are being violated or that the continuing transfer would create an imminent risk of grave harm to data subjects;
- W. whereas Commission Decision 520/2000 also states that when evidence has been provided that anybody responsible for ensuring compliance with the principles is not effectively fulfilling their role, the Commission must inform the US Department of Commerce and, if necessary, present measures with a view to reversing or suspending the said Decision or limiting its scope;
- X. whereas in its first two reports on the implementation of the Safe Harbour, of 2002 and 2004, the Commission identified several deficiencies as regards the proper implementation of the Safe Harbour and made several recommendations to the US authorities with a view to rectifying them;
- Y. whereas in its third implementation report, of 27 November 2013, nine years after the second report and without any of the deficiencies recognised in that report having been rectified, the Commission identified further wide-ranging weaknesses and shortcomings in the Safe Harbour and concluded that the current implementation could not be maintained; whereas the Commission has stressed that wide-ranging access by US intelligence agencies to data transferred to the US by Safe-Harbour-certified entities raises additional serious questions as to the continuity of protection of the data of EU data subjects; whereas the Commission addressed 13 recommendations to the US authorities and undertook to identify by summer 2014, together with the US authorities, remedies to be implemented as soon as possible, forming the basis for a full review of the functioning of the Safe Harbour principles;
- Z. whereas on 28-31 October 2013 the delegation of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) to Washington D.C. met with the US Department of Commerce and the US Federal Trade Commission; whereas the Department of Commerce acknowledged the existence of organisations having self-certified adherence to Safe Harbour Principles but clearly showing a 'not-current status', meaning that the company does not fulfil Safe Harbour requirements although continuing to receive personal data from the EU; whereas the Federal Trade Commission admitted that the Safe Harbour should be reviewed in order to improve it, particularly with regard to complaints and alternative dispute resolution systems;
- AA. whereas Safe Harbour Principles may be limited 'to the extent necessary to meet national security, public interest, or law enforcement requirements'; whereas, as an exception to a fundamental right, such an exception must always be interpreted restrictively and be limited to what is necessary and proportionate in a democratic society, and the law must clearly establish the conditions and safeguards to make this limitation legitimate; whereas such an exception should not be used in a way that

undermines the protection afforded by EU data protection law and the Safe Harbour principles;

- AB. whereas large-scale access by US intelligence agencies has seriously eroded transatlantic trust and negatively impacted on the trust for US organisations acting in the EU; whereas this is further exacerbated by the lack of judicial and administrative redress for EU citizens under US law, particularly in cases of surveillance activities for intelligence purposes;

Transfers to third countries with the adequacy decision

- AC. whereas according to the information revealed and to the findings of the inquiry conducted by the LIBE Committee, the national security agencies of New Zealand and Canada have been involved on a large scale in mass surveillance of electronic communications and have actively cooperated with the US under the so called 'Five eyes' programme, and may have exchanged with each other personal data of EU citizens transferred from the EU;
- AD. whereas Commission Decisions 2013/65¹ and 2/2002 of 20 December 2001² have declared the adequate level of protection ensured by the New Zealand and the Canadian Personal Information Protection and Electronic Documents Act; whereas the aforementioned revelations also seriously affect trust in the legal systems of these countries as regards the continuity of protection afforded to EU citizens; whereas the Commission has not examined this aspect;

Transfers based on contractual clauses and other instruments

- AE. whereas Directive 95/46/EC provides that international transfers to a third country may also take place by means of specific instruments whereby the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights;
- AF. whereas such safeguards may in particular result from appropriate contractual clauses;
- AG. whereas Directive 95/46/EC empowers the Commission to decide that specific standard contractual clauses offer sufficient safeguards required by the Directive and whereas on this basis the Commission has adopted three models of standard contractual clauses for transfers to controllers and processors (and sub-processors) in third countries;
- AH. whereas the Commission Decisions establishing the standard contractual clauses stipulate that the competent authorities in Member States may exercise their existing powers to suspend data flows when it is established that the law to which the data importer or a sub-processor is subject imposes upon them requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in

¹ OJ L 28, 30.1.2013, p. 12.

² OJ L 2, 4.1.2002, p. 13.

a democratic society as provided for in Article 13 of Directive 95/46/EC, where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses, or where there is a substantial likelihood that the standard contractual clauses in the annex are not being or will not be complied with and the continuing transfer would create an imminent risk of grave harm to the data subjects;

- AI. whereas national data protection authorities have developed binding corporate rules (BCRs) in order to facilitate international transfers within a multinational corporation with adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; whereas before being used, BCRs need to be authorised by the Member States' competent authorities after the latter have assessed compliance with Union data protection law;

Transfers based on TFTP and PNR agreements

- AJ. whereas in its resolution of 23 October 2013 the European Parliament expressed serious concerns about the revelations concerning the NSA's activities as regards direct access to financial payments messages and related data, which would constitute a clear breach of the Agreement, in particular Article 1 thereof;
- AK. whereas the European Parliament asked the Commission to suspend the Agreement and requested that all relevant information and documents be made available immediately for Parliament's deliberations;
- AL. whereas following the allegations published by the media, the Commission decided to open consultations with the US pursuant to Article 19 of the TFTP Agreement; whereas on 27 November 2013 Commissioner Malmström informed the LIBE Committee that, after meeting US authorities and in view of the replies given by the US authorities in their letters and during their meetings, the Commission had decided not to pursue the consultations on the grounds that there were no elements showing that the US Government has acted in a manner contrary to the provisions of the Agreement, and that the US has provided written assurance that no direct data collection has taken place contrary to the provisions of the TFTP agreement;
- AM. whereas during the LIBE delegation to Washington of 28-31 October 2013 the delegation met with the US Department of the Treasury; whereas the US Treasury stated that since the entry into force of the TFTP Agreement it had not had access to data from SWIFT in the EU except within the framework of the TFTP; whereas the US Treasury refused to comment on whether SWIFT data would have been accessed outside TFTP by any other US government body or department or whether the US administration was aware of NSA mass surveillance activities; whereas on 18 December 2013 Mr Glenn Greenwald stated before the LIBE Committee inquiry that the NSA and GCHQ had targeted SWIFT networks;
- AN. whereas the Belgian and Dutch Data Protection authorities decided on 13 November 2013 to conduct a joint investigation into the security of SWIFT's payment networks in order to ascertain whether third parties could gain unauthorised or unlawful access

to European citizens' bank data¹;

- AO. whereas according to the Joint Review of the EU-US PNR agreement, the United States Department of Homeland Security (DHS) made 23 disclosures of PNR data to the NSA on a case-by-case basis in support of counterterrorism cases, in a manner consistent with the specific terms of the Agreement;
- AP. whereas the Joint Review fails to mention the fact that in the case of processing of personal data for intelligence purposes, under US law, non-US citizens do not enjoy any judicial or administrative avenue to protect their rights, and constitutional protections are only granted to US persons; whereas this lack of judicial or administrative rights nullifies the protections for EU citizens laid down in the existing PNR agreement;

Transfers based on the EU-US Mutual Legal Assistance Agreement in criminal matters.

- AQ. whereas the EU-US Agreement on mutual legal assistance in criminal matters of 6 June 2003² entered into force on 1 February 2010 and is intended to facilitate cooperation between the EU and US to combat crime in a more effective way, having due regard for the rights of individuals and the rule of law;

Framework agreement on data protection in the field of police and judicial cooperation ('umbrella agreement')

- AR. whereas the purpose of this general agreement is to establish the legal framework for all transfers of personal data between the EU and US for the sole purposes of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters; whereas negotiations were authorised by the Council on 2 December 2010;
- AS. whereas this agreement should provide for clear and precise legally binding data-processing principles and should in particular recognise EU citizens' right to access, rectification and erasure of their personal data in the US, as well as the right to an efficient administrative and judicial redress mechanism for EU citizens and independent oversight of the data-processing activities;
- AT. whereas in its Communication of 27 November 2013 the Commission indicated that the 'umbrella agreement' should result in a high level of protection for citizens on both sides of the Atlantic and should strengthen the trust of Europeans in EU-US data exchanges, providing a basis on which to develop EU-US security cooperation and partnership further;
- AU. whereas negotiations on the agreement have not progressed because of the US Government's persistent position of refusing recognition of effective rights of administrative and judicial redress to EU citizens and because of the intention of providing broad derogations to the data protection principles contained in the

¹ <http://www.privacycommission.be/fr/news/les-instances-europ%C3%A9ennes-charg%C3%A9es-de-contr%C3%B4ler-le-respect-de-la-vie-priv%C3%A9e-examinent-la>

² OJ L 181, 19.7.2003, p. 25

agreement, such as purpose limitation, data retention or onward transfers either domestically or abroad;

Data Protection Reform

- AV. whereas the EU data protection legal framework is currently being reviewed in order to establish a comprehensive, consistent, modern and robust system for all data-processing activities in the Union; whereas in January 2012 the Commission presented a package of legislative proposals: a General Data Protection Regulation¹, which will replace Directive 95/46/EC and establish a uniform law throughout the EU, and a Directive² which will lay down a harmonised framework for all data processing activities by law enforcement authorities for law enforcement purposes and will reduce the current divergences among national laws;
- AW. whereas on 21 October 2013 the LIBE Committee adopted its legislative reports on the two proposals and a decision on the opening of negotiations with the Council with a view to having the legal instruments adopted during this legislative term;
- AX. whereas, although the European Council of 24/25 October 2013 called for the timely adoption of a strong EU General Data Protection framework in order to foster the trust of citizens and businesses in the digital economy, the Council has been unable to arrive at a general approach on the General Data Protection Regulation and the Directive³;

IT security and cloud computing

- AY. whereas the resolution of 10 December⁴ emphasises the economic potential of 'cloud computing' business for growth and employment;
- AZ. whereas the level of data protection in a cloud computing environment must not be inferior to that required in any other data-processing context; whereas Union data protection law, since it is technologically neutral, already applies fully to cloud computing services operating in the EU;
- BA. whereas mass surveillance activities give intelligence agencies access to personal data stored by EU individuals under cloud services agreements with major US cloud providers; whereas the US intelligence authorities have accessed personal data stored in servers located on EU soil by tapping into the internal networks of Yahoo and Google⁵; whereas such activities constitute a violation of international obligations; whereas it is not excluded that information stored in cloud services by Member States' public authorities or undertakings and institutions has also been accessed by intelligence authorities;

Democratic oversight of intelligence services

¹ COM(2012) 11, 25.1.2012.

² COM(2012) 10, 25.1.2012.

³ http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf

⁴ AT-0353/2013 PE506.114V2.00.

⁵ The Washington Post, 31 October 2013.

- BB. whereas intelligence services perform an important function in protecting democratic society against internal and external threats; whereas they are given special powers and capabilities to this end; whereas these powers are to be used within the rule of law, as otherwise they risk losing legitimacy and eroding the democratic nature of society;
- BC. whereas the high level of secrecy that is intrinsic to the intelligence services in order to avoid endangering ongoing operations, revealing *modi operandi* or putting at risk the lives of agents impedes full transparency, public scrutiny and normal democratic or judicial examination;
- BD. whereas technological developments have led to increased international intelligence cooperation, also involving the exchange of personal data, and often blurring the line between intelligence and law enforcement activities;
- BE. whereas most of existing national oversight mechanisms and bodies were set up or revamped in the 1990s and have not necessarily been adapted to the rapid technological developments over the last decade;
- BF. whereas democratic oversight of intelligence activities is still conducted at national level, despite the increase in exchange of information between EU Member States and between Member States and third countries; whereas there is an increasing gap between the level of international cooperation on the one hand and oversight capacities limited to the national level on the other, which results in insufficient and ineffective democratic scrutiny;

Main findings

1. Considers that recent revelations in the press by whistleblowers and journalists, together with the expert evidence given during this inquiry, have resulted in compelling evidence of the existence of far-reaching, complex and highly technologically advanced systems designed by US and some Member States' intelligence services to collect, store and analyse communication and location data and metadata of all citizens around the world on an unprecedented scale and in an indiscriminate and non-suspicion-based manner;
2. Points specifically to US NSA intelligence programmes allowing for the mass surveillance of EU citizens through direct access to the central servers of leading US internet companies (PRISM programme), the analysis of content and metadata (Xkeyscore programme), the circumvention of online encryption (BULLRUN), access to computer and telephone networks and access to location data, as well as to systems of the UK intelligence agency GCHQ such as its upstream-surveillance activity (Tempora programme) and decryption programme (Edgehill); believes that the existence of programmes of a similar nature, even if on a more limited scale, is likely in other EU countries such as France (DGSE), Germany (BND) and Sweden (FRA);
3. Notes the allegations of 'hacking' or tapping into the Belgacom systems by the UK intelligence agency GCHQ; reiterates the indication by Belgacom that it could not confirm that EU institutions were targeted or affected, and that the malware used was extremely complex and required the use of extensive financial and staffing resources

- for its development and use that would not be available to private entities or hackers;
4. States that trust has been profoundly shaken: trust between the two transatlantic partners, trust among EU Member States, trust between citizens and their governments, trust in the respect of the rule of law, and trust in the security of IT services; believes that in order to rebuild trust in all these dimensions a comprehensive plan is urgently needed;
 5. Notes that several governments claim that these mass surveillance programmes are necessary to combat terrorism; wholeheartedly supports the fight against terrorism, but strongly believes that it can never in itself be a justification for untargeted, secret and sometimes even illegal mass surveillance programmes; expresses concerns, therefore, regarding the legality, necessity and proportionality of these programmes;
 6. Considers it very doubtful that data collection of such magnitude is only guided by the fight against terrorism, as it involves the collection of all possible data of all citizens; points therefore to the possible existence of other power motives such as political and economic espionage;
 7. Questions the compatibility of some Member States' massive economic espionage activities with the EU internal market and competition law as enshrined in Title I and Title VII of the Treaty on the Functioning of the European Union; reaffirms the principle of sincere cooperation as enshrined in Article 4 paragraph 3 of the Treaty on European Union and the principle that the Member States shall 'refrain from any measures which could jeopardise the attainment of the Union's objectives';
 8. Notes that international treaties and EU and US legislation, as well as national oversight mechanisms, have failed to provide for the necessary checks and balances and for democratic accountability;
 9. Condemns in the strongest possible terms the vast, systemic, blanket collection of the personal data of innocent people, often comprising intimate personal information; emphasises that the systems of mass, indiscriminate surveillance by intelligence services constitute a serious interference with the fundamental rights of citizens; stresses that privacy is not a luxury right, but that it is the foundation stone of a free and democratic society; points out, furthermore, that mass surveillance has potentially severe effects on the freedom of the press, thought and speech, as well as a significant potential for abuse of the information gathered against political adversaries; emphasises that these mass surveillance activities appear also to entail illegal actions by intelligence services and raise questions regarding the extra-territoriality of national laws;
 10. Sees the surveillance programmes as yet another step towards the establishment of a fully fledged preventive state, changing the established paradigm of criminal law in democratic societies, promoting instead a mix of law enforcement and intelligence activities with blurred legal safeguards, often not in line with democratic checks and balances and fundamental rights, especially the presumption of innocence; recalls in

that regard the decision of the German Federal Constitutional Court¹ on the prohibition of the use of preventive dragnets ('präventive Rasterfahndung') unless there is proof of a concrete danger to other high-ranking legally protected rights, whereby a general threat situation or international tensions do not suffice to justify such measures;

11. Is adamant that secret laws, treaties and courts violate the rule of law; points out that any judgment of a court or tribunal and any decision of an administrative authority of a non-EU state authorising, directly or indirectly, surveillance activities such as those examined by this inquiry may not be automatically recognised or enforced, but must be submitted individually to the appropriate national procedures on mutual recognition and legal assistance, including rules imposed by bilateral agreements;
12. Points out that the abovementioned concerns are exacerbated by rapid technological and societal developments; considers that, since internet and mobile devices are everywhere in modern daily life ('ubiquitous computing') and the business model of most internet companies is based on the processing of personal data of all kinds that puts at risk the integrity of the person, the scale of this problem is unprecedented;
13. Regards it as a clear finding, as emphasised by the technology experts who testified before the inquiry, that at the current stage of technological development there is no guarantee, either for EU public institutions or for citizens, that their IT security or privacy can be protected from intrusion by well-equipped third countries or EU intelligence agencies ('no 100% IT security'); notes that this alarming situation can only be remedied if Europeans are willing to dedicate sufficient resources, both human and financial, to preserving Europe's independence and self-reliance;
14. Strongly rejects the notion that these issues are purely a matter of national security and therefore the sole competence of Member States; recalls a recent ruling of the Court of Justice according to which 'although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision concerns State security cannot result in European Union law being inapplicable'²; recalls further that the protection of the privacy of all EU citizens is at stake, as are the security and reliability of all EU communication networks; believes therefore that discussion and action at EU level is not only legitimate, but also a matter of EU autonomy and sovereignty;
15. Commends the current discussions, inquiries and reviews concerning the subject of this inquiry in several parts of the world; points to the Global Government Surveillance Reform signed up to by the world's leading technology companies, which calls for sweeping changes to national surveillance laws, including an international ban on bulk collection of data to help preserve the public's trust in the internet; notes with great interest the recommendations published recently by the US President's Review Group on Intelligence and Communications Technologies; strongly urges governments to take these calls and recommendations fully into account and to overhaul their national frameworks for the intelligence services in order to implement appropriate safeguards and oversight;

¹ No I BvR 518/02 of 4 April 2006.

² No I BvR 518/02 of 4 April 2006.

16. Commends the institutions and experts who have contributed to this inquiry; deplores the fact that several Member States' authorities have declined to cooperate with the inquiry the European Parliament has been conducting on behalf of citizens; welcomes the openness of several Members of Congress and of national parliaments;
17. Is aware that in such a limited timeframe it has been possible to conduct only a preliminary investigation of all the issues at stake since July 2013; recognises both the scale of the revelations involved and their ongoing nature; adopts, therefore, a forward-planning approach consisting in a set of specific proposals and a mechanism for follow-up action in the next parliamentary term, ensuring the findings remain high on the EU political agenda;
18. Intends to request strong political undertakings from the European Commission to be designated after the May 2014 elections to implement the proposals and recommendations of this Inquiry; expects adequate commitment from the candidates in the upcoming parliamentary hearings for the new Commissioners;

Recommendations

19. Calls on the US authorities and the EU Member States to prohibit blanket mass surveillance activities and bulk processing of personal data;
20. Calls on certain EU Member States, including the UK, Germany, France, Sweden and the Netherlands, to revise where necessary their national legislation and practices governing the activities of intelligence services so as to ensure that they are in line with the standards of the European Convention on Human Rights and comply with their fundamental rights obligations as regards data protection, privacy and presumption of innocence; in particular, given the extensive media reports referring to mass surveillance in the UK, would emphasise that the current legal framework which is made up of a 'complex interaction' between three separate pieces of legislation – the Human Rights Act 1998, the Intelligence Services Act 1994 and the Regulation of Investigatory Powers Act 2000 – should be revised;
21. Calls on the Member States to refrain from accepting data from third states which have been collected unlawfully and from allowing surveillance activities on their territory by third states' governments or agencies which are unlawful under national law or do not meet the legal safeguards enshrined in international or EU instruments, including the protection of Human Rights under the TEU, the ECHR and the EU Charter of Fundamental Rights;
22. Calls on the Member States immediately to fulfil their positive obligation under the European Convention on Human Rights to protect their citizens from surveillance contrary to its requirements, including when the aim thereof is to safeguard national security, undertaken by third states and to ensure that the rule of law is not weakened as a result of extraterritorial application of a third country's law;
23. Invites the Secretary-General of the Council of Europe to launch the Article 52 procedure according to which 'on receipt of a request from the Secretary General of the Council of Europe any High Contracting Party shall furnish an explanation of the

manner in which its internal law ensures the effective implementation of any of the provisions of the Convention’;

24. Calls on Member States to take appropriate action immediately, including court action, against the breach of their sovereignty, and thereby the violation of general public international law, perpetrated through the mass surveillance programmes; calls further on EU Member States to make use of all available international measures to defend EU citizens’ fundamental rights, notably by triggering the inter-state complaint procedure under Article 41 of the International Covenant on Civil and Political Rights (ICCPR);
25. Calls on the US to revise its legislation without delay in order to bring it into line with international law, to recognise the privacy and other rights of EU citizens, to provide for judicial redress for EU citizens and to sign the Additional Protocol allowing for complaints by individuals under the ICCPR;
26. Strongly opposes any conclusion of an additional protocol or guidance to the Council of Europe Cybercrime Convention (Budapest Convention) on transborder access to stored computer data which could provide for a legitimisation of intelligence services’ access to data stored in another jurisdiction without its authorisation and without the use of existing mutual legal assistance instruments, since this could result in unfettered remote access by law enforcement authorities to servers and computers located in other jurisdictions and would be in conflict with Council of Europe Convention 108;
27. Calls on the Commission to carry out, before July 2014, an assessment of the applicability of Regulation EC No 2271/96 to cases of conflict of laws for transfers of personal data;

International transfers of data

US data protection legal framework and US Safe Harbour

28. Notes that the companies identified by media revelations as being involved in the large-scale mass surveillance of EU data subjects by US NSA are companies that have self-certified their adherence to the Safe Harbour, and that the Safe Harbour is the legal instrument used for the transfer of EU personal data to the US (Google, Microsoft, Yahoo!, Facebook, Apple, LinkedIn); expresses its concerns on the fact that these organisations admitted that they do not encrypt information and communications flowing between their data centres, thereby enabling intelligence services to intercept information’;
29. Considers that large-scale access by US intelligence agencies to EU personal data processed by Safe Harbour does not per se meet the criteria for derogation under ‘national security’;
30. Takes the view that, as under the current circumstances the Safe Harbour principles do not provide adequate protection for EU citizens, these transfers should be carried out

¹ The Washington Post, 31 October 2013.

under other instruments, such as contractual clauses or BCRs setting out specific safeguards and protections;

31. Calls on the Commission to present measures providing for the immediate suspension of Commission Decision 520/2000, which declared the adequacy of the Safe Harbour privacy principles, and of the related FAQs issued by the US Department of Commerce;
32. Calls on Member States' competent authorities, namely the data protection authorities, to make use of their existing powers and immediately suspend data flows to any organisation that has self-certified its adherence to the US Safe Harbour Principles and to require that such data flows are only carried out under other instruments, provided they contain the necessary safeguards and protections with respect to the protection of the privacy and fundamental rights and freedoms of individuals;
33. Calls on the Commission to present by June 2014 a comprehensive assessment of the US privacy framework covering commercial, law enforcement and intelligence activities in response to the fact that the EU and the US legal systems for protecting personal data are drifting apart;

Transfers to other third countries with adequacy decision

34. Recalls that Directive 95/46/EC stipulates that transfers of personal data to a third country may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of the Directive, the third country in question ensures an adequate level of protection, the purpose of this provision being to ensure the continuity of the protection afforded by EU data protection law where personal data are transferred outside the EU;
35. Recalls that Directive 95/46/EC provides that the adequacy of the level of protection afforded by a third country is to be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; likewise recalls that the said Directive also equips the Commission with implementing powers to declare that a third country ensures an adequate level of protection in the light of the criteria laid down by Directive 95/46/EC; whereas Directive 95/46/EC also empowers the Commission to declare that a third country does not ensure an adequate level of protection;
36. Recalls that in the latter case Member States must take the measures necessary to prevent any transfer of data of the same type to the third country in question, and that the Commission should enter into negotiations with a view to remedying the situation;
37. Calls on the Commission and the Member States to assess without delay whether the adequate level of protection of the New Zealand and of the Canadian Personal Information Protection and Electronic Documents Act, as declared by Commission Decisions 2013/651 and 2/2002 of 20 December 2001, have been affected by the involvement of their national intelligence agencies in the mass surveillance of EU

¹ OJ L 28, 30.1.2013, p. 12.

citizens and, if necessary, to take appropriate measures to suspend or reverse the adequacy decisions; expects the Commission to report to the European Parliament on its findings on the abovementioned countries by December 2014 at the latest;

Transfers based on contractual clauses and other instruments

38. Recalls that national data protection authorities have indicated that neither standard contractual clauses nor BCRs were written with situations of access to personal data for mass surveillance purposes in mind, and that such access would not be in line with the derogation clauses of the contractual clauses or BCRs which refer to exceptional derogations for a legitimate interest in a democratic society and where necessary and proportionate;
39. Calls on the Member States to prohibit or suspend data flows to third countries based on the standard contractual clauses, contractual clauses or BCRs authorised by the national competent authorities where it is established that the law to which the data importer is subject imposes upon him requirements which go beyond the restrictions necessary in a democratic society and which are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses, or because continuing transfer would create an imminent risk of grave harm to the data subjects;
40. Calls on the Article 29 Working Party to issue guidelines and recommendations on the safeguards and protections that contractual instruments for international transfers of EU personal data should contain in order to ensure the protection of the privacy, fundamental rights and freedoms of individuals, taking particular account of the third-country laws on intelligence and national security and the involvement of the companies receiving the data in a third country in mass surveillance activities by a third country's intelligence agencies;
41. Calls on the Commission to examine the standard contractual clauses it has established in order to assess whether they provide the necessary protection as regards access to personal data transferred under the clauses for intelligence purposes and, if appropriate, to review them;

Transfers based on the Mutual Legal Assistance Agreement

42. Calls on the Commission to conduct before the end 2014 an in-depth assessment of the existing Mutual Legal Assistance Agreement, pursuant to its Article 17, in order to verify its practical implementation and, in particular, whether the US has made effective use of it for obtaining information or evidence in the EU and whether the Agreement has been circumvented to acquire the information directly in the EU, and to assess the impact on the fundamental rights of individuals; such an assessment should not only refer to US official statements as a sufficient basis for the analysis but be based on specific EU evaluations; this in-depth review should also address the consequences of the application of the Union's constitutional architecture to this instrument in order to bring it into line with Union law, taking account in particular of Protocol 36 and Article 10 thereof and Declaration 50 concerning this protocol;

EU mutual assistance in criminal matters

43. Asks the Council and the Commission to inform Parliament about the actual use by Member States of the Convention on Mutual Assistance in Criminal Matters between the Member States, in particular Title III on interception of telecommunications; calls on the Commission to put forward a proposal, in accordance with Declaration 50, concerning Protocol 36, as requested, before the end of 2014 in order to adapt it to the Lisbon Treaty framework;

Transfers based on the TFTP and PNR agreements

44. Takes the view that the information provided by the European Commission and the US Treasury does not clarify whether US intelligence agencies have access to SWIFT financial messages in the EU by intercepting SWIFT networks or banks' operating systems or communication networks, alone or in cooperation with EU national intelligence agencies and without having recourse to existing bilateral channels for mutual legal assistance and judicial cooperation;
45. Reiterates its resolution of 23 October 2013 and asks the Commission for the suspension of the TFTP Agreement;
46. Calls on the European Commission to react to concerns that three of the major computerised reservation systems used by airlines worldwide are based in the US and that PNR data are saved in cloud systems operating on US soil under US law, which lacks data protection adequacy;

Framework agreement on data protection in the field of police and judicial cooperation ('Umbrella agreement')

47. Considers that a satisfactory solution under the 'Umbrella agreement' is a pre-condition for the full restoration of trust between the transatlantic partners;
48. Asks for an immediate resumption of the negotiations with the US on the 'Umbrella Agreement', which should provide for clear rights for EU citizens and effective and enforceable administrative and judicial remedies in the US without any discrimination;
49. Asks the Commission and the Council not to initiate any new sectorial agreements or arrangements for the transfer of personal data for law enforcement purposes as long as the 'Umbrella Agreement' has not entered into force;
50. Urges the Commission to report in detail on the various points of the negotiating mandate and the latest state of play by April 2014;

Data protection reform

51. Calls on the Council Presidency and the majority of Member States who support a high level of data protection to show a sense of leadership and responsibility and accelerate their work on the whole Data Protection Package to allow for adoption in 2014, so that EU citizens will be able to enjoy better protection in the very near future;

52. Stresses that both the Data Protection Regulation and the Data Protection Directive are necessary to protect the fundamental rights of individuals and therefore must be treated as a package to be adopted simultaneously, in order to ensure that all data-processing activities in the EU provide a high level of protection in all circumstances;

Cloud computing

53. Notes that trust in US cloud computing and cloud providers has been negatively affected by the abovementioned practices; emphasises, therefore, the development of European clouds as an essential element for growth and employment and trust in cloud computing services and providers and for ensuring a high level of personal data protection;
54. Reiterates its serious concerns about the compulsory direct disclosure of EU personal data and information processed under cloud agreements to third-country authorities by cloud providers subject to third-country laws or using storage servers located in third countries, and about direct remote access to personal data and information processed by third-country law enforcement authorities and intelligence services;
55. Regrets the fact that such access is usually attained by means of direct enforcement by third-country authorities of their own legal rules, without recourse to international instruments established for legal cooperation such as mutual legal assistance (MLA) agreements or other forms of judicial cooperation;
56. Calls on the Commission and the Member States to speed up the work of establishing a European Cloud Partnership;
57. Recalls that all companies providing services in the EU must, without exception, comply with EU law and are liable for any breaches;

Transatlantic Trade and Investment Partnership Agreement (TTIP)

58. Recognises that the EU and the US are pursuing negotiations for a Transatlantic Trade and Investment Partnership, which is of major strategic importance for creating further economic growth and for the ability of both the EU and the US to set future global regulatory standards;
59. Strongly emphasises, given the importance of the digital economy in the relationship and in the cause of rebuilding EU-US trust, that the European Parliament will only consent to the final TTIP agreement provided the agreement fully respects fundamental rights recognised by the EU Charter, and that the protection of the privacy of individuals in relation to the processing and dissemination of personal data must continue to be governed by Article XIV of the GATS;

Democratic oversight of intelligence services

60. Stresses that, despite the fact that oversight of intelligence services' activities should be based on both democratic legitimacy (strong legal framework, ex ante authorisation and ex post verification) and an adequate technical capability and expertise, the

majority of current EU and US oversight bodies dramatically lack both, in particular the technical capabilities;

61. Invites, as it has done in the case of Echelon, all national parliaments which have not yet done so to install meaningful oversight of intelligence activities by parliamentarians or expert bodies with legal powers to investigate; calls on national parliaments to ensure that such oversight committees/bodies have sufficient resources, technical expertise and legal means to be able to effectively control intelligence services;
62. Calls for the setting up of a high-level group to strengthen cooperation in the field of intelligence at EU level, combined with a proper oversight mechanism ensuring both democratic legitimacy and adequate technical capacity; stresses that the high-level group should cooperate closely with national parliaments in order to propose further steps to be taken for increased oversight collaboration in the EU;
63. Calls on this high-level group to define minimum European standards or guidelines on the (ex ante and ex post) oversight of intelligence services on the basis of existing best practices and recommendations by international bodies (UN, Council of Europe);
64. Calls on the high-level group to set strict limits on the duration of any surveillance ordered unless its continuation is duly justified by the authorising/oversight authority;
65. Calls on the high-level group to develop criteria on enhanced transparency, built on the general principle of access to information and the so-called 'Tshwane Principles'¹;
66. Intends to organise a conference with national oversight bodies, whether parliamentary or independent, by the end of 2014;
67. Calls on the Member States to draw on best practices so as to improve access by their oversight bodies to information on intelligence activities (including classified information and information from other services) and establish the power to conduct on-site visits, a robust set of powers of interrogation, adequate resources and technical expertise, strict independence vis-à-vis their respective governments, and a reporting obligation to their respective parliaments;
68. Calls on the Member States to develop cooperation among oversight bodies, in particular within the European Network of National Intelligence Reviewers (ENNIR);
69. Urges the Commission to present, by September 2014, a proposal for a legal basis for the activities of the EU Intelligence Analysis Centre (IntCen), as well as a proper oversight mechanism adapted to its activities, including regular reporting to the European Parliament;
70. Calls on the Commission to present, by September 2014, a proposal for an EU security clearance procedure for all EU office holders, as the current system, which relies on the security clearance undertaken by the Member State of citizenship, provides for

¹ The Global Principles on National Security and the Right to Information, June 2013.

different requirements and lengths of procedures within national systems, thus leading to differing treatment of Members of Parliament and their staff depending on their nationality;

71. Recalls the provisions of the interinstitutional agreement between the European Parliament and the Council concerning the forwarding to and handling by the European Parliament of classified information held by the Council on matters other than those in the area of the common foreign and security policy that should be used to improve oversight at EU level;

EU agencies

72. Calls on the Europol Joint Supervisory Body, together with national data protection authorities, to conduct a joint inspection before the end of 2014 in order to ascertain whether information and personal data shared with Europol has been lawfully acquired by national authorities, particularly if the information or data was initially acquired by intelligence services in the EU or a third country, and whether appropriate measures are in place to prevent the use and further dissemination of such information or data;
73. Calls on Europol to ask the competent authorities of the Member States, in line with its competences, to initiate investigations with regard to possible cybercrimes and cyber attacks committed by governments or private actors in the course of the activities under scrutiny;

Freedom of expression

74. Expresses deep concern about the developing threats to the freedom of the press and the chilling effect on journalists of intimidation by state authorities, in particular as regards the protection of confidentiality of journalistic sources; reiterates the calls expressed in its resolution of 21 May 2013 on 'the EU Charter: standard settings for media freedom across the EU';
75. Considers that the detention of Mr Miranda and the seizure of the material in his possession under Schedule 7 of the Terrorism Act 2000 (and also the request to *The Guardian* to destroy or hand over the material) constitutes an interference with the right of freedom of expression as recognised by Article 10 of the ECHR and Article 11 of the EU Charter;
76. Calls on the Commission to put forward a proposal for a comprehensive framework for the protection of whistleblowers in the EU, with particular attention to the specificities of whistleblowing in the field of intelligence, for which provisions relating to whistleblowing in the financial field may prove insufficient, and including strong guarantees of immunity;

EU IT security

77. Points out that recent incidents clearly demonstrate the acute vulnerability of the EU, and in particular the EU institutions, national governments and parliaments, major European companies, European IT infrastructures and networks, to sophisticated

attacks using complex software; notes that these attacks require such financial and human resources that they are likely to originate from state entities acting on behalf of foreign governments or even from certain EU national governments that support them; in this context, regards the case of the hacking or tapping of the telecommunications company Belgacom as a worrying example of an attack against the EU's IT capacity;

78. Takes the view that the mass surveillance revelations that have initiated this crisis can be used as an opportunity for Europe to take the initiative and build up an autonomous IT key-resource capability for the mid term; calls on the Commission and the Member States to use public procurement as leverage to support such resource capability in the EU by making EU security and privacy standards a key requirement in the public procurement of IT goods and services;
79. Is highly concerned by indications that foreign intelligence services sought to lower IT security standards and to install backdoors in a broad range of IT systems;
80. Calls on all the Members States, the Commission, the Council and the European Council to address the EU's dangerous lack of autonomy in terms of IT tools, companies and providers (hardware, software, services and network), and encryption and cryptographic capabilities;
81. Calls on the Commission, standardisation bodies and ENISA to develop, by September 2014, minimum security and privacy standards and guidelines for IT systems, networks and services, including cloud computing services, in order to better protect EU citizens' personal data; believes that such standards should be set in an open and democratic process, not driven by a single country, entity or multinational company; takes the view that, while legitimate law enforcement and intelligence concerns need to be taken into account in order to support the fight against terrorism, they should not lead to a general undermining of the dependability of all IT systems;
82. Points out that both telecom companies and the EU and national telecom regulators have clearly neglected the IT security of their users and clients; calls on the Commission to make full use of its existing powers under the ePrivacy and Telecommunication Framework Directive to strengthen the protection of confidentiality of communication by adopting measures to ensure that terminal equipment is compatible with the right of users to control and protect their personal data, and to ensure a high level of security of telecommunication networks and services, including by way of requiring state-of-the-art encryption of communications;
83. Supports the EU cyber strategy but considers that it does not cover all possible threats and should be extended to cover malicious state behaviours;
84. Calls on the Commission, by January 2015 at the latest, to present an Action Plan to develop more EU independence in the IT sector, including a more coherent approach to boosting European IT technological capabilities (including IT systems, equipment, services, cloud computing, encryption and anonymisation) and to the protection of critical IT infrastructure (including in terms of ownership and vulnerability);
85. Calls on the Commission, in the framework of the next Work Programme of the

- Horizon 2020 Programme, to assess whether more resources should be directed towards boosting European research, development, innovation and training in the field of IT technologies, in particular privacy-enhancing technologies and infrastructures, cryptology, secure computing, open-source security solutions and the Information Society;
86. Asks the Commission to map out current responsibilities and to review, by June 2014 at the latest, the need for a broader mandate, better coordination and/or additional resources and technical capabilities for Europol's CyberCrime Centre, ENISA, CERT-EU and the EDPS in order to enable them to be more effective in investigating major IT breaches in the EU and in performing (or assisting Member States and EU bodies to perform) on-site technical investigations regarding major IT breaches;
87. Deems it necessary for the EU to be supported by an EU IT Academy that brings together the best European experts in all related fields, tasked with providing all relevant EU Institutions and bodies with scientific advice on IT technologies, including security-related strategies; as a first step asks the Commission to set up an independent scientific expert panel;
88. Calls on the European Parliament's Secretariat to carry out, by September 2014 at the latest, a thorough review and assessment of the European Parliament's IT security dependability focused on: budgetary means, staff resources, technical capabilities, internal organisation and all relevant elements, in order to achieve a high level of security for the EP's IT systems; believes that such an assessment should at the least provide information analysis and recommendations on:
- the need for regular, rigorous, independent security audits and penetration tests, with the selection of outside security experts ensuring transparency and guarantees of their credentials vis-à-vis third countries or any types of vested interest;
 - the inclusion in tender procedures for new IT systems of specific IT security/privacy requirements, including the possibility of a requirement for Open Source Software as a condition of purchase;
 - the list of US companies under contract with the European Parliament in the IT and telecom fields, taking into account revelations about NSA contracts with a company such as RSA, whose products the European Parliament is using to supposedly protect remote access to their data by its Members and staff;
 - the reliability and resilience of third-party commercial software used by the EU institutions in their IT systems with regard to penetrations and intrusions by EU or third-country law enforcement and intelligence authorities;
 - the use of more open-source systems and fewer off-the-shelf commercial systems;
 - the impact of the increased use of mobile tools (smartphones, tablets, whether professional or personal) and its effects on the IT security of the system;

- the security of the communications between different workplaces of the European Parliament and of the IT systems used at the European Parliament;
 - the use and location of servers and IT centres for the EP's IT systems and the implications for the security and integrity of the systems;
 - the implementation in reality of the existing rules on security breaches and prompt notification of the competent authorities by the providers of publicly available telecommunication networks;
 - the use of cloud storage by the EP, including what kind of data is stored on the cloud, how the content and access to it is protected and where the cloud is located, clarifying the applicable data protection legal regime;
 - a plan allowing for the use of more cryptographic technologies, in particular end-to-end authenticated encryption for all IT and communications services such as cloud computing, email, instant messaging and telephony;
 - the use of electronic signature in email;
 - an analysis of the benefits of using the GNU Privacy Guard as a default encryption standard for emails which would at the same time allow for the use of digital signatures;
 - the possibility of setting up a secure Instant Messaging service within the European Parliament allowing secure communication, with the server only seeing encrypted content;
89. Calls on all the EU Institutions and agencies to perform a similar exercise, by December 2014 at the latest, in particular the European Council, the Council, the External Action Service (including EU delegations), the Commission, the Court of Justice and the European Central Bank; invites the Member States to conduct similar assessments;
90. Stresses that as far as the external action of the EU is concerned, assessments of related budgetary needs should be carried out and first measures taken without delay in the case of the European External Action Service (EEAS) and that appropriate funds need to be allocated in the 2015 Draft Budget;
91. Takes the view that the large-scale IT systems used in the area of freedom, security and justice, such as the Schengen Information System II, the Visa Information System, Eurodac and possible future systems, should be developed and operated in such a way as to ensure that data is not compromised as a result of US requests under the Patriot Act; asks eu-LISA to report back to Parliament on the reliability of the systems in place by the end of 2014;
92. Calls on the Commission and the EEAS to take action at the international level, with the UN in particular, and in cooperation with interested partners (such as Brazil), and to implement an EU strategy for democratic governance of the internet in order to

prevent undue influence over ICANN's and IANA's activities by any individual entity, company or country by ensuring appropriate representation of all interested parties in these bodies;

93. Calls for the overall architecture of the internet in terms of data flows and storage to be reconsidered, striving for more data minimisation and transparency and less centralised mass storage of raw data, as well as avoiding unnecessary routing of traffic through the territory of countries that do not meet basic standards on fundamental rights, data protection and privacy;
94. Calls on the Member States, in cooperation with ENISA, Europol's CyberCrime Centre, CERTs and national data protection authorities and cybercrime units, to start an education and awareness-raising campaign in order to enable citizens to make a more informed choice regarding what personal data to put on line and how better to protect them, including through 'digital hygiene', encryption and safe cloud computing, making full use of the public interest information platform provided for in the Universal Service Directive;
95. Calls on the Commission, by September 2014, to evaluate the possibilities of encouraging software and hardware manufacturers to introduce more security and privacy through default features in their products, including the possibility of introducing legal liability on the part of manufacturers for unpatched known vulnerabilities or the installation of secret backdoors, and disincentives for the undue and disproportionate collection of mass personal data, and if appropriate to come forward with legislative proposals;

Rebuilding trust

96. Believes that the inquiry has shown the need for the US to restore trust with its partners, as US intelligence agencies' activities are primarily at stake;
97. Points out that the crisis of confidence generated extends to:
- the spirit of cooperation within the EU, as some national intelligence activities may jeopardise the attainment of the Union's objectives;
 - citizens, who realise that not only third countries or multinational companies, but also their own government, may be spying on them;
 - respect for the rule of law and the credibility of democratic safeguards in a digital society;

Between the EU and the US

98. Recalls the important historical and strategic partnership between the EU Member States and the US, based on a common belief in democracy, the rule of law and fundamental rights;
99. Believes that the mass surveillance of citizens and the spying on political leaders by

the US have caused serious damage to relations between the EU and the US and negatively impacted on trust in US organisations acting in the EU; this is further exacerbated by the lack of judicial and administrative remedies for redress under US law for EU citizens, particularly in cases of surveillance activities for intelligence purposes;

100. Recognises, in light of the global challenges facing the EU and the US, that the transatlantic partnership needs to be further strengthened, and that it is vital that transatlantic cooperation in counter-terrorism continues; insists, however, that clear measures need to be taken by the US to re-establish trust and re-emphasise the shared basic values underlying the partnership;
101. Is ready actively to engage in a dialogue with US counterparts so that, in the ongoing American public and congressional debate on reforming surveillance and reviewing intelligence oversight, the privacy rights of EU citizens are addressed, equal information rights and privacy protection in US courts guaranteed and the current discrimination not perpetuated;
102. Insists that necessary reforms be undertaken and effective guarantees given to Europeans to ensure that the use of surveillance and data processing for foreign intelligence purposes is limited by clearly specified conditions and related to reasonable suspicion or probable cause of terrorist or criminal activity; stresses that this purpose must be subject to transparent judicial oversight;
103. Considers that clear political signals are needed from our American partners to demonstrate that the US distinguishes between allies and adversaries;
104. Urges the EU Commission and the US Administration to address, in the context of the ongoing negotiations on an EU-US umbrella agreement on data transfer for law enforcement purposes, the information and judicial redress rights of EU citizens, and to conclude these negotiations, in line with the commitment made at the EU-US Justice and Home Affairs Ministerial Meeting of 18 November 2013, before summer 2014;
105. Encourages the US to accede to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), as it acceded to the 2001 Convention on Cybercrime, thus strengthening the shared legal basis among the transatlantic allies;
106. Calls on the EU institutions to explore the possibilities for establishing with the US a code of conduct which would guarantee that no US espionage is pursued against EU institutions and facilities;

Within the European Union

107. Also believes that that the involvement and activities of EU Members States has led to a loss of trust; is of the opinion that only full clarity as to purposes and means of surveillance, public debate and, ultimately, revision of legislation, including a strengthening of the system of judicial and parliamentary oversight, will be able to

re-establish the trust lost;

108. Is aware that some EU Member States are pursuing bilateral communication with the US authorities on spying allegations, and that some of them have concluded (United Kingdom) or envisage concluding (Germany, France) so-called 'anti-spying' arrangements; underlines that these Member States need to observe fully the interests of the EU as a whole;
109. Considers that such arrangements should not breach European Treaties, especially the principle of sincere cooperation (under Article 4 paragraph 3 TEU), or undermine EU policies in general and, more specifically, the internal market, fair competition and economic, industrial and social development; reserves its right to activate Treaty procedures in the event of such arrangements being proved to contradict the Union's cohesion or the fundamental principles on which it is based;

Internationally

110. Calls on the Commission to present, in January 2015 at the latest, an EU strategy for democratic governance of the internet;
111. Calls on the Member States to follow the call of the 35th International Conference of Data Protection and Privacy Commissioners 'to advocate the adoption of an additional protocol to Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which should be based on the standards that have been developed and endorsed by the International Conference and the provisions in General Comment No 16 to the Covenant in order to create globally applicable standards for data protection and the protection of privacy in accordance with the rule of law'; asks the High Representative/Vice-President of the Commission and the External Action Service to take a proactive stance;
112. Calls on the Member States to develop a coherent and strong strategy within the United Nations, supporting in particular the resolution on 'The right to privacy in the digital age' initiated by Brazil and Germany, as adopted by the third UN General Assembly Committee (Human Rights Committee) on 27 November 2013;

Priority Plan: A European Digital Habeas Corpus

113. Decides to submit to EU citizens, Institutions and Member States the abovementioned recommendations as a Priority Plan for the next legislature;
114. Decides to launch *A European Digital Habeas Corpus for protecting privacy* based on the following 7 actions with a European Parliament watchdog:

Action 1: Adopt the Data Protection Package in 2014;

Action 2: Conclude the EU-US Umbrella Agreement ensuring proper redress mechanisms for EU citizens in the event of data transfers from the EU to the US for law-enforcement purposes;

Action 3: Suspend Safe Harbour until a full review has been conducted and current loopholes are remedied, making sure that transfers of personal data for commercial purposes from the Union to the US can only take place in compliance with highest EU standards;

Action 4: Suspend the TFTP agreement until (i) the Umbrella Agreement negotiations have been concluded; (ii) a thorough investigation has been concluded on the basis of an EU analysis, and all concerns raised by Parliament in its resolution of 23 October have been properly addressed;

Action 5: Protect the rule of law and the fundamental rights of EU citizens, with a particular focus on threats to the freedom of the press and professional confidentiality (including lawyer-client relations) as well as enhanced protection for whistleblowers;

Action 6: Develop a European strategy for IT independence (at national and EU level);

Action 7: Develop the EU as a reference player for a democratic and neutral governance of the internet;

115. Calls on the EU Institutions and the Member States to support and promote the European Digital Habeas Corpus; undertakes to act as the EU citizens' rights watchdog, with the following timetable to monitor implementation:

- April-July 2014: a monitoring group based on the LIBE inquiry team responsible for monitoring any new revelations in the media concerning the inquiry's mandate and scrutinising the implementation of this resolution;
- July 2014 onwards: a standing oversight mechanism for data transfers and judicial remedies within the competent committee;
- Spring 2014: a formal call on the European Council to include the European Digital Habeas Corpus in the guidelines to be adopted under Article 68 TFEU;
- Autumn 2014: a commitment that the European Digital Habeas Corpus and related recommendations will serve as key criteria for the approval of the next Commission;
- 2014-2015: a Trust/Data/Citizens' Rights group to be convened on a regular basis between the European Parliament and the US Congress, as well as with other committed third-country parliaments, including Brazil;
- 2014-2015: a conference with the intelligence oversight bodies of European national parliaments;
- 2015: a conference bringing together high-level European experts in the various fields conducive to IT security (including mathematics, cryptography and privacy-enhancing technologies) to help foster an EU IT strategy for the

next legislature;

116. Instructs its President to forward this resolution to the European Council, the Council, the Commission, the parliaments and governments of the Member States, national data protection authorities, the EDPS, eu-LISA, ENISA, the Fundamental Rights Agency, the Article 29 Working Party, the Council of Europe, the Congress of the United States of America, the US Administration, the President, the Government and the Parliament of the Federative Republic of Brazil, and the United Nations Secretary-General.

EXPLANATORY STATEMENT

*'The office of the sovereign, be it a monarch or an assembly, consisteth in the end, for which he was trusted with the sovereign power, namely the procuration of the safety of people'
Hobbes, Leviathan (chapter XXX)*

*'We cannot commend our society to others by departing from the fundamental standards which make it worthy of commendation'
Lord Bingham of Cornhill,
Former Lord Chief Justice of England and Wales*

Methodology

From July 2013, the LIBE Committee of Inquiry was responsible for the extremely challenging task of fulfilling the mandate¹ of the Plenary on the investigation into the electronic mass surveillance of EU citizens in a very short timeframe, less than 6 months.

During that period it held over 15 hearings covering each of the specific cluster issues prescribed in the 4 July resolution, drawing on the submissions of both EU and US experts representing a wide range of knowledge and backgrounds: EU institutions, national parliaments, US congress, academics, journalists, civil society, security and technology specialists and private business. In addition, a delegation of the LIBE Committee visited Washington on 28-30 October 2013 to meet with representatives of both the executive and the legislative branch (academics, lawyers, security experts, business representatives)². A delegation of the Committee on Foreign Affairs (AFET) was also in town at the same time. A few meetings were held together.

A series of working documents³ have been co-authored by the rapporteur, the shadow-rapporteurs⁴ from the various political groups and 3 Members from the AFET Committee⁵ enabling a presentation of the main findings of the Inquiry. The rapporteur would like to thank all shadow rapporteurs and AFET Members for their close cooperation and high-level commitment throughout this demanding process.

Scale of the problem

An increasing focus on security combined with developments in technology has enabled States to know more about citizens than ever before. By being able to collect data

¹ [http://www.europarl.europa.eu/meetdocs/2009_2014/documents/ta/04/07/2013%20-%200322/p7_taprov\(2013\)0322_en.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/ta/04/07/2013%20-%200322/p7_taprov(2013)0322_en.pdf)

² See Washington delegation report.

³ See Annex I.

⁴ List of shadow rapporteurs: Axel Voss (EPP), Sophia in't Veld (ALDE), Jan Philipp Albrecht (GREENS/ALE), Timothy Kirkhope (EFD), Cornelia Ernst (GUE).

⁵ List of AFET Members: José Ignacio Salafranca Sánchez-Neyra (EPP), Ana Gomes (S&D), Annemie Neyts-Uyttebroeck (ALDE).

regarding the content of communications, as well as metadata, and by following citizens' electronic activities, in particular their use of smartphones and tablet computers, intelligence services are de facto able to know almost everything about a person. This has contributed to a fundamental shift in the work and practices of intelligence agencies, away from the traditional concept of targeted surveillance as a necessary and proportional counter-terrorism measure, towards systems of mass surveillance.

This process of increasing mass surveillance has not been subject to any prior public debate or democratic decision-making. Discussion is needed on the purpose and scale of surveillance and its place in a democratic society. Is the situation created by Edward Snowden's revelations an indication of a general societal turn towards the acceptance of the death of privacy in return for security? Do we face a breach of privacy and intimacy so great that it is possible not only for criminals but for IT companies and intelligence agencies to know every detail of the life of a citizen? Is it a fact to be accepted without further discussion? Or is the responsibility of the legislator to adapt the policy and legal tools at hand to limit the risks and prevent further damages in case less democratic forces would come to power?

Reactions to mass surveillance and a public debate

The debate on mass surveillance does not take place in an even manner inside the EU. In fact in many Member States there is hardly any public debate and media attention varies. Germany seems to be the country where reactions to the revelations have been strongest and public discussions as to their consequences have been widespread. In the United Kingdom and France, in spite of investigations by The Guardian and Le Monde, reactions seem more limited, a fact that has been linked to the alleged involvement of their national intelligence services in activities with the NSA. The LIBE Committee Inquiry has been in a position to hear valuable contributions from the parliamentary oversight bodies of Belgian, the Netherlands, Denmark and even Norway; however the British and French Parliament have declined participation. These differences show again the uneven degree of checks and balances within the EU on these issues and that more cooperation is needed between parliamentary bodies in charge of oversight.

Following the disclosures of Edward Snowden in the mass media, public debate has been based on two main types of reactions. On the one hand, there are those who deny the legitimacy of the information published on the grounds that most of the media reports are based on misinterpretation; in addition many argue, while not having refuted the disclosures, the validity of the disclosures made due to allegations of security risks they cause for national security and the fight against terrorism.

On the other hand, there are those who consider the information provided requires an informed, public debate because of the magnitude of the problems it raises to issues key to a democracy including: the rule of law, fundamental rights, citizens' privacy, public accountability of law-enforcement and intelligence services, etc. This is certainly the case for the journalists and editors of the world's biggest press outlets who are privy to the disclosures including The Guardian, Le Monde, Der Spiegel, The Washington Post and Glenn Greenwald.

The two types of reactions outlined above are based on a set of reasons which, if followed,

may lead to quite opposed decisions as to how the EU should or should not react.

5 reasons not to act

– *The 'Intelligence/national security argument': no EU competence*

Edward Snowden's revelations relate to US and some Member States' intelligence activities, but national security is a national competence, the EU has no competence in such matters (except on EU internal security) and therefore no action is possible at EU level.

– *The 'Terrorism argument': danger of the whistleblower*

Any follow up to these revelations, or their mere consideration, further weakens the security of the US as well as the EU as it does not condemn the publication of documents the content of which even if redacted as involved media players explain may give valuable information to terrorist groups.

– *The 'Treason argument': no legitimacy for the whistleblower*

As mainly put forward by some in the US and in the United Kingdom, any debate launched or action envisaged further to E. Snowden's revelations is intrinsically biased and irrelevant as they would be based on an initial act of treason.

– *The 'realism argument': general strategic interests*

Even if some mistakes and illegal activities were to be confirmed, they should be balanced against the need to maintain the special relationship between the US and Europe to preserve shared economic, business and foreign policy interests.

– *The 'Good government argument': trust your government*

US and EU Governments are democratically elected. In the field of security, and even when intelligence activities are conducted in order to fight against terrorism, they comply with democratic standards as a matter of principle. This 'presumption of good and lawful governance' rests not only on the goodwill of the holders of the executive powers in these states but also on the checks and balances mechanism enshrined in their constitutional systems.

As one can see reasons not to act are numerous and powerful. This may explain why most EU governments, after some initial strong reactions, have preferred not to act. The main action by the Council of Ministers has been to set up a 'transatlantic group of experts on data protection' which has met 3 times and put forward a final report. A second group is supposed to have met on intelligence related issues between US authorities and Member States' ones but no information is available. The European Council has addressed the surveillance problem in a mere statement of Heads of state or government¹, Up until now only a few national

¹ European Council Conclusions of 24-25 October 2013, in particular: 'The Heads of State or Government took note of the intention of France and Germany to seek bilateral talks with the USA with the aim of finding before

parliaments have launched inquiries.

5 reasons to act

- *The 'mass surveillance argument': in which society do we want to live?*

Since the very first disclosure in June 2013, consistent references have been made to George's Orwell novel '1984'. Since 9/11 attacks, a focus on security and a shift towards targeted and specific surveillance has seriously damaged and undermined the concept of privacy. The history of both Europe and the US shows us the dangers of mass surveillance and the graduation towards societies without privacy.

- *The 'fundamental rights argument':*

Mass and indiscriminate surveillance threaten citizens' fundamental rights including right to privacy, data protection, freedom of press, fair trial which are all enshrined in the EU Treaties, the Charter of fundamental rights and the ECHR. These rights cannot be circumvented nor be negotiated against any benefit expected in exchange unless duly provided for in legal instruments and in full compliance with the treaties.

- *The 'EU internal security argument':*

National competence on intelligence and national security matters does not exclude a parallel EU competence. The EU has exercised the competences conferred upon it by the EU Treaties in matters of internal security by deciding on a number of legislative instruments and international agreements aimed at fighting serious crime and terrorism, on setting-up an internal security strategy and agencies working in this field. In addition, other services have been developed reflecting the need for increased cooperation at EU level on intelligence-related matters: INTCEN (placed within EEAS) and the Anti-terrorism Coordinator (placed within the Council general secretariat), neither of them with a legal basis.

- *The 'deficient oversight argument'*

While intelligence services perform an indispensable function in protecting against internal and external threats, they have to operate within the rule of law and to do so must be subject to a stringent and thorough oversight mechanism. The democratic oversight of intelligence activities is conducted at national level but due to the international nature of security threats there is now a huge exchange of information between Member States and with third countries like the US; improvements in oversight mechanisms are needed both at national and at EU level if traditional oversight mechanisms are not to become ineffective and outdated.

- *The 'chilling effect on media' and the protection of whistleblowers*

The disclosures of Edward Snowden and the subsequent media reports have highlighted the

the end of the year an understanding on mutual relations in that field. They noted that other EU countries are welcome to join this initiative. They also pointed to the existing Working Group between the EU and the USA on the related issue of data protection and called for rapid and constructive progress in that respect'.

pivotal role of the media in a democracy to ensure accountability of Governments. When supervisory mechanisms fail to prevent or rectify mass surveillance, the role of media and whistleblowers in unveiling eventual illegalities or misuses of power is extremely important. Reactions from the US and UK authorities to the media have shown the vulnerability of both the press and whistleblowers and the urgent need to do more to protect them.

The European Union is called on to choose between a 'business as usual' policy (sufficient reasons not to act, wait and see) and a 'reality check' policy (surveillance is not new, but there is enough evidence of an unprecedented magnitude of the scope and capacities of intelligence agencies requiring the EU to act).

Habeas Corpus in a Surveillance Society

In 1679 the British parliament adopted the Habeas Corpus Act as a major step forward in securing the right to a judge in times of rival jurisdictions and conflicts of laws. Nowadays our democracies ensure proper rights for a convicted or detainee who is in person physically subject to a criminal proceeding or deferred to a court. But his or her data, as posted, processed, stored and tracked on digital networks form a 'body of personal data', a kind of digital body specific to every individual and enabling to reveal much of his or her identity, habits and preferences of all types.

Habeas Corpus is recognised as a fundamental legal instrument to safeguarding individual freedom against arbitrary state action. What is needed today is an extension of Habeas Corpus to the digital era. Right to privacy, respect of the integrity and the dignity of the individual are at stake. Mass collections of data with no respect for EU data protection rules and specific violations of the proportionality principle in the data management run counter to the constitutional traditions of the Member States and the fundamentals of the European constitutional order.

The main novelty today is these risks do not only originate in criminal activities (against which the EU legislator has adopted a series of instruments) or from possible cyber-attacks from governments of countries with a lower democratic record. There is a realisation that such risks may also come from law-enforcement and intelligence services of democratic countries putting EU citizens or companies under conflicts of laws resulting in a lesser legal certainty, with possible violations of rights without proper redress mechanisms.

Governance of networks is needed to ensure the safety of personal data. Before modern states developed, no safety on roads or city streets could be guaranteed and physical integrity was at risk. Nowadays, despite dominating everyday life, information highways are not secure. Integrity of digital data must be secured, against criminals of course but also against possible abuse of power by state authorities or contractors and private companies under secret judicial warrants.

LIBE Committee Inquiry Recommendations

Many of the problems raised today are extremely similar to those revealed by the European Parliament Inquiry on the Echelon programme in 2001. The impossibility for the previous legislature to follow up on the findings and recommendations of the Echelon Inquiry should serve as a key lesson to this Inquiry. It is for this reason that this Resolution, recognising both

the magnitude of the revelations involved and their ongoing nature, is forward planning and ensures that there are specific proposals on the table for follow up action in the next Parliamentary mandate ensuring the findings remain high on the EU political agenda.

Based on this assessment, the rapporteur would like to submit to the vote of the Parliament the following measures:

A European Digital Habeas corpus for protecting privacy based on 7 actions:

Action 1: Adopt the Data Protection Package in 2014;

Action 2: Conclude the EU-US Umbrella agreement ensuring proper redress mechanisms for EU citizens in case of data transfers from the EU to the US for law-enforcement purposes;

Action 3: Suspend Safe Harbour until a full review is conducted and current loopholes are remedied making sure that transfers of personal data for commercial purposes from the Union to the US can only take place in compliance with EU highest standards;

Action 4: Suspend the TFTP agreement until i) the Umbrella agreement negotiations have been concluded; ii) a thorough investigation has been concluded based on EU analysis and all concerns raised by the Parliament in its resolution of 23 October have been properly addressed;

Action 5: Protect the rule of law and the fundamental rights of EU citizens, with a particular focus on threats to the freedom of the press and professional confidentiality (including lawyer-client relations) as well as enhanced protection for whistleblowers;

Action 6: Develop a European strategy for IT independence (at national and EU level);

Action 7: Develop the EU as a reference player for a democratic and neutral governance of Internet;

After the conclusion of the Inquiry the European Parliament should continue acting as EU citizens' rights watchdog with the following timetable to monitor implementations:

- April-July 2014: a monitoring group based on the LIBE Inquiry team responsible for monitoring any new revelations in the media concerning the Inquiries mandate and scrutinising the implementation of this resolution;
- July 2014 onwards: a standing oversight mechanism for data transfers and judicial remedies within the competent committee;
- Spring 2014: a formal call on the European Council to include the European Digital Habeas Corpus in the guidelines to be adopted under Article 68 TFEU;

- Autumn 2014: a commitment that the European Digital Habeas Corpus and related recommendations will serve as key criteria for the approval of the next Commission;
- 2014-2015: a Trust/Data/Citizens' rights group to be convened on a regular basis between the European Parliament and the US Congress as well as with other committed third-country parliaments including Brazil;
- 2014-2015: a conference with European intelligence oversight bodies of European national parliaments;
- 2015: a conference gathering high-level European experts in the various fields conducive to IT security (including mathematics, cryptography, privacy enhancing technologies, ...) to help foster an EU IT strategy for the next legislature;

ANNEX I: LIST OF WORKING DOCUMENTS**LIBE Committee Inquiry**

Rapporteur & Shadows as co-authors	Issues	EP resolution of 4 July 2013 (see paragraphs 15-16)
Mr Moraes (S&D)	US and EU Member Surveillance programmes and their impact on EU citizens fundamental rights	16 (a) (b) (c) (d)
Mr Voss (EPP)	US surveillance activities with respect to EU data and its possible legal implications on transatlantic agreements and cooperation	16 (a) (b) (c)
Mrs. In't Veld (ALDE) & Mrs. Ernst (GUE)	Democratic oversight of Member State intelligence services and of EU intelligence bodies.	15, 16 (a) (c) (e)
Mr Albrecht (GREENS/EF A)	The relation between the surveillance practices in the EU and the US and the EU data protection provisions	16 (c) (e) (f)
Mr Kirkhope (ECR)	Scope of International, European and national security in the EU perspective	16 (a) (b)
AFET 3 Members	Foreign Policy Aspects of the Inquiry on Electronic Mass Surveillance of EU Citizens	16 (a) (b) (f)

ANNEX II: LIST OF HEARINGS AND EXPERTS**LIBE COMMITTEE INQUIRY
ON US NSA SURVEILLANCE PROGRAMME,
SURVEILLANCE BODIES IN VARIOUS MEMBER STATES
AND THEIR IMPACT ON EU CITIZENS' FUNDAMENTAL RIGHTS AND ON
TRANSATLANTIC COOPERATION IN JUSTICE AND HOME AFFAIRS**

Following the European Parliament resolution of 4th July 2013 (para. 16), the LIBE Committee has held a series of hearings to gather information relating the different aspects at stake, assess the impact of the surveillance activities covered, notably on fundamental rights and data protection rules, explore redress mechanisms and put forward recommendations to protect EU citizens' rights, as well as to strengthen IT security of EU Institutions.

Bl. 269-304

Entnahme wegen Schutz Persönlichkeitsrechte Dritter

Dokument 2014/0067340

Von: .BRUEEU POL-IN2-2 Eickelpasch, Joerg <pol-in2-2-eu@brue.auswaertiges-
amt.de>
Gesendet: Freitag, 21. Juni 2013 09:10
An: Weinbrenner, Ulrich; Jergl, Johann; Stentzel, Rainer, Dr.; Mammen, Lars, Dr.
Cc: t.pohl@diplo.de
Betreff: KOM-Interna zu PRISM
Anlagen: Speaking Note Reding for LIBE.DOCX

Anbei vertraulich aus KOM erhaltene speaking note -daraus wird u.a.
ersichtlich, dass KOM noch nicht weiss, wie Expertengruppe arbeiten soll:

. [If asked on how this Transatlantic group of experts will
materialise/other details] We are currently in the process of preparing
the set-up of this Group, and we will keep the European Parliament fully
informed.

Na ja, vielleicht erfahren wir am Montag mehr....

Viele Grüße,
Jörg Eickelpasch

Defensives on data protection: Verizon/PRISM, 'umbrella' negotiations, Convention 108

- At the Justice Ministerial in Dublin last week (14 June), AG Holder and I had an open exchange on the concrete issues that arose following the recent press revelations.
- The discussion in Dublin was a constructive first exchange. We expect this meeting to be followed up by more detailed answers in writing from the US to the concrete and elaborative questions I raised in the letter to AG Holder.

What will the European Commission do concretely to protect the EU individuals' rights? The US is invoking 'national security' to spy ordinary EU citizens.

- I asked Mr Holder seven questions, on which I am waiting for the answers. In particular, I would also like to know how many Europeans are targeted, to have an idea of what the impact is in concrete terms.

I heard that these are matters of security. Indeed, national security is competence of the Member States and the US respectively. However, what I clearly stated to Mr Holder is that national security is not a broadly defined concept, which can be used at the expense of fundamental rights of Europeans.

- As the European Court of Justice explained in a recent judgement¹, although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision concerns State security cannot result in European Union law being inapplicable.
- I also explained to Mr Holder that in Europe, also in cases of national security, every individual – irrespective of their nationality – benefits from protection and can go to Court if they believe that their fundamental rights have been infringed. This is a basic principle in European and Member State law.

¹ Judgment of the European Court of Justice (Grand Chamber) of 4 June 2013, case C-300/1, *ZZ v Secretary of State for the Home Department*, para. 38 –cf. Background.

- Respect for fundamental rights and the rule of law are the foundations of the EU-US relationship. This common understanding has been the basis of cooperation between us, also when it comes to law enforcement co-operation in the fight against terrorism and serious crime.
- We put forward a concrete solution to address this issue: We will convene a Transatlantic group of experts from the field of data protection and security from the European Commission, the Member States and the US administration to clarify these matters further.
- *[If asked on how this Transatlantic group of experts will materialise/other details]* We are currently in the process of preparing the set-up of this Group, and we will keep the European Parliament fully informed.

How does PRISM affect law enforcement cooperation? In any case, the 'umbrella agreement' cannot provide any solutions in this respect.

- While it is correct that national security and intelligence activities are outside the scope of the umbrella agreement, since this is not an EU competence I consider that this agreement has the potential to provide guarantees that will help address some of our concerns.
- A strong umbrella agreement will provide a solid legal framework on both sides of the Atlantic that will promote trust in day-to-day law enforcement cooperation under concrete conditions for law enforcement authorities and with concrete guarantees for individuals' rights.
- A strong umbrella will also promote the use of formal channels of cooperation, such as Mutual Legal Assistance agreements, which are the appropriate, lawful means for data transfers by providing guarantees ensuring individuals' rights. The "umbrella agreement" will ensure that these safeguards are present in every specific agreement.
- It is against this background that I explained to AG Holder that national security is designed to address specific needs. The interpretation of national security cannot be used to undermine

the established channels of law enforcement co-operation and empty our co-operation agreements of the protections guaranteed for individuals.

- If there is a need for EU citizens' data held by private companies to be accessed by a third country, this must take place through formal channels of cooperation. Any exceptional cases should be limited, clearly defined and judicially reviewable.
- This will help to restore trust which is:
 - the basis for our cooperation in the field of law enforcement;
 - essential to the stability and growth of the digital economy, and
 - of paramount importance for individuals and companies alike.
- In Dublin, we committed to advance with the negotiations for an Umbrella Agreement on data protection in the area of law enforcement. This is important. Some progress has been made, including in recent months, but more needs to be done.
- Time has come now to address key issues like equal treatment of EU and US citizens and effective judicial redress. Now is the right time to address this cornerstone issue, which is a key EU concern.

The EU Data Protection Reform cannot help prevent PRISM-type scandals in any way.

- In the proposed General Data Protection Regulation, which you are currently negotiating, there are key building blocks for a system of strong data protection. By adopting our Reform, we can ensure that certain important data protection components - from a European perspective - will be 'written in stone' when we engage with our US counterparts in deliberations on PRISM-type issues.
- The first one is a clear provision on the territory where the rules apply. It has to be made certain that companies from outside Europe abide by E.U. data protection laws when they offer and sell products and services to consumers in the

Union. If you want to play in our backyard, you have to play by our rules.

- Secondly, I propose a broad definition of personal data. This should include not just the content of e-mails and phone calls, for example, but related traffic data ("meta-data") as well, such as information on where something was sent from or which individual was calling whom. The perception that people's "meta-data" is not protected is at the core of the Verizon-scandal and we should take a clear stance on this issue when negotiating the Data Protection Reform.
- Thirdly, we must not limit the rules to those companies that collect people's data. Rather, we have to include processors of those data as well — such as cloud providers — because, as the Prism scandal shows, cloud providers also present an avenue for those who want to access data.
- And finally we must have strong rules on international transfers to shield our citizens from PRISM-type phenomena. I said it before, I will repeat it now: The avenues to be used for data exchange in the law enforcement sector are formal channels of cooperation, such as Mutual Legal Assistance Agreements etc. Outside such formal channels of cooperation, the personal data of European individuals may only be transferred to non-European law enforcement authorities in exceptional situations that are limited, clearly-defined and subject to judicial review.

Will data protection be included in the negotiations for a Transatlantic Trade and Investment Partnership (TTIP)?

- The TTIP is not going to negotiate privacy standards and data protection. The EU is not going to discuss citizens' fundamental rights within the context of a trade negotiation.
- The differences on how the EU and the US regulate data protection have been recognised for a long time. The TTIP negotiations will not be the right forum to address these differences. Last year we have seen some moves in the direction of increased consumer privacy in the US, with the adoption of the Consumer Privacy Blueprint by the Obama administration. But there is clearly some considerable way to go. So the TTIP, with its ambitious timescale, is not the place

to discuss how to change the US standards. Data protection is outside of the scope of the trade negotiations.

- The correct forum for these discussions is the on-going 'umbrella' negotiations between the EU and the US on the specific issue of access to data by law enforcement and judicial authorities and the new group on privacy and security to be set up in that context, agreed at the Ministerial last week.

Will the Commission revoke Safe Harbour?

- The Commission is awaiting clarification from the United States authorities on some remaining issues. I cannot say anything about potential implications for Safe Harbour until I am in possession of all the facts.

[Background on Safe Harbour: In 2000, the Commission declared that transfers by US organizations having joined the Safe Harbour scheme, which is enforced by the US Federal Trade Commission, offer an adequate level of protection. This so-called "partial adequacy" allows over 3.000 companies registered in Safe Harbour to freely exchange data across the Atlantic. The Commission periodically evaluates the functioning of Safe Harbour. Several amendments to the DP Regulation call for the abolition of Safe Harbour.]

Does the EU-US PNR agreement facilitate access by US authorities to communications data?

- The EU-US PNR agreement is concerned with the transfer of PNR data, which are booking data for air travel, including such data as the travel date, travel agent, ticket number, seat number, billing address.
- A PNR may also include a contact telephone number if that number has been provided by the traveller. However, this data type does not include information about telecommunications data like the ones dealt with under the Prism case, such as 'metadata' or traffic data (data necessary to identify for example the date of a call, time and duration) generated by telecommunications service providers.

Are the companies that are allowing access to the NSA through PRISM acting in breach of EU law? Will the Commission bring infringement proceedings against the UK in respect of use by its intelligence services of data obtained through PRISM?

- I requested further clarifications from the US Attorney-General in order to establish the scope of the PRISM programme.
- Under the Treaty, national security is a matter for Member States and falls outside the scope of EU legislation. However, national security is not a broadly defined concept, which can be used at the expense of fundamental rights of Europeans.
- As the European Court of Justice explained in a recent judgement², although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision concerns State security cannot result in European Union law being inapplicable.
- Furthermore, we should not forget that in Europe, also in cases of national security, every individual – irrespective of their nationality – benefits from protection and can go to Court if they believe that their fundamental rights have been infringed. This is a basic principle of European and Member State law.
- It should also be recalled that all Member States are Parties to the European Convention on Human Rights which also ensures the protection of fundamental rights.
- Of course, we also have to consider European business interests, and the proper functioning of the internal market, which may be put at risk if information should happen to be accessed or disclosed.

² Judgment of the European Court of Justice (Grand Chamber) of 4 June 2013, case C-300/1, *ZZ v Secretary of State for the Home Department*, para. 38 –cf. Background.

On Patriot Act/FISA – third countries' laws providing for direct access to data (extraterritorial effect)

- I have repeated this many times: data protection is a fundamental right, enshrined in the EU Charter of fundamental rights and the European Convention on Human rights. Our constitutional Courts, as well as the European Court of Human Rights have the competence to address possible violations of these rights in specific cases.
- As mentioned in replies to several questions from Members of this House, the Commission is concerned about some third countries' laws and other legislative instruments which purport directly to regulate data processing activities of natural and legal persons under the jurisdiction of the Member States.
- Let me say again: The extraterritorial application of such legislation may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union. Transfers should only be allowed where the conditions of European law for a transfer to third countries are met.
- This point is made both to our counterparts as well as in multilateral fora. We need to ensure that official channels of cooperation, such as international agreements, are used to exchange personal information of our individuals.
- In this respect, I reiterate the importance of EU-US Mutual Legal Assistance and Extradition agreements, which should be implemented with efficiency and full respect for fundamental rights.
- A political solution to this issue has to be found. I said and reiterated this to my counterparts in the framework of the on-going dialogue we have with them on the issue of data protection, in particular in the negotiations on an EU-US data protection agreement for the law enforcement sector ("umbrella" agreement).

The US has a mandate for an executive agreement, which limits very much the outcome of the agreement (i.e. will not change US legislation). What are you planning to do to stop US secret services conducting surveillance over Europeans' data?

- The European Commission is closely monitoring these developments, which reflect the growing importance and awareness when it comes to data protection for people in the digital world.
- Last Friday I spoke to my counterpart, Justice Minister Holder, in Dublin. I explicitly expressed concerns regarding this issue, in particular regarding the direct access of law enforcement authorities in the US to personal data held by companies in the EU.
- The umbrella agreement between the US and the EU can become an incentive for the US to review its laws and practices and ratify this agreement.
- As to judicial redress in particular, I made the point that EU citizens should have this right in the US, in the same way that US citizens have right to judicial redress in all EU Member States.

Why did the EP not receive the copy of the mandate to accede to Council of Europe ("Convention 108") in time?

- The draft document was submitted to the European Parliament in April.
- The mandate was recently approved by Council with limited changes.
- The main goal of the European Commission during these negotiations is to ensure a high level of data protection for individuals. The other core (and strictly related) objective of these negotiations is to ensure compatibility between the negotiated modernised text and the Data Protection Reform, which we are currently negotiating here and at the Council. This two-fold objective is expressly reflected in the mandate.
- For example, the mandate requires that in the context of the negotiations of the modernized convention the Commission

shall seek consistency between the EU data protection *acquis* and the Convention 108 rules governing trans-border data flows in order to ensure the effective application of EU rules on international transfers.

- As in other on-going negotiations, the Commission will keep the European Parliament and this committee fully informed of all stages of the negotiation. These regular exchanges are very useful for the Commission.

BACKGROUND

(1) Difference between “national security” and “law enforcement”

On the one hand, law enforcement cooperation falls, broadly speaking, in the former “3rd pillar” of EU law. After the entry into force of the Lisbon Treaty and the abolition of the pillar structure, Chapter 4 and Chapter 5 of the TFEU lay down rules relevant to judicial and police cooperation in criminal matters. Law enforcement refers to the prevention, detection, investigation and punishment of criminal offences. This term encompasses the activities of a wide range of entities, ranging from police to courts and prisons.

On the other hand, national security falls under the responsibility of Member States (art. 4(2) TUE: “national security remains the sole responsibility of each member State”). Even though there is no single universally accepted definition of national security, what is generally accepted as pertaining to national security are issues relating to defence and protection of the safety and sovereign interests of a State. These matters are typically dealt with by intelligence services which can be of civilian and/or military nature.

ECJ case-law repeatedly stated that, even within the system of the Treaty's national security clause, this remains a qualified exception: national security has to be strictly interpreted and invoked only if there are duly justified and proportionate reasons thereto.

(2) ECJ: “National security cannot result in European Union law being inapplicable”

Recent ECJ case C-300/11 - Judgment of the Court (Grand Chamber) of 4 June 2013 - ZZ v Secretary of State for the Home Department:
<http://curia.europa.eu/juris/liste.jsf?num=C-300/11#>

Facts of the case: ZZ denied entry to the UK on the basis of information whose disclosure would be liable to prejudice national security. ZZ appealed to Special Immigration Appeals Commission ('SIAC'). Neither he nor his own lawyers had access to the information upon which the decision was based (disclosure contrary to the public interest). SIAC dismissed ZZ's appeal, and gave a 'closed judgment' with exhaustive grounds and an 'open judgment' with summary grounds. Only the 'open judgment' was provided to ZZ. It is apparent from the 'open judgment' that SIAC was satisfied, for reasons explained in the 'closed judgment', that ZZ was involved in activities of the Armed Islamic Group (GIA) network and in terrorist activities in 1995 and 1996. Court of Appeal asked ECJ to what extent SIAC obliged to inform the person concerned of the public security grounds which constitute the basis of a decision refusing entry.

Before the ECJ it was argued: it is clear from Article 4(2) TEU and Article 346(1)(a) TFEU that State security remains the responsibility of solely the Member States. The question referred thus relates to an area governed by national law and, for that reason, does not fall within European Union competence.

Relevant parts of the judgement (paras 36-38):

"In that regard, the Court's settled case-law should be recalled according to which, in proceedings under Article 267 TFEU, which are based on a clear separation of functions between the national courts and the Court of Justice, the national court alone

has jurisdiction to find and assess the facts in the case before it and to interpret and apply national law. Similarly, it is solely for the national court, before which the dispute has been brought and which must assume responsibility for the judicial decision to be made, to determine, in the light of the particular circumstances of the case, both the need for and the relevance of the questions that it submits to the Court. Consequently, **where the questions submitted concern the interpretation of European Union law, the Court is in principle bound to give a ruling** (Case C-553/11 Rintisch [2012] ECR I-0000, paragraph 15 and the case-law cited).

The Court may refuse to rule on a question referred by a national court only where it is quite obvious that the interpretation of **European Union law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical**, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (Joined Cases C-188/10 and C-189/10 Melki and Abdeli [2010] ECR I-5667, paragraph 27 and the case-law cited).

That is not the case here. First, the question referred relates to the **interpretation of Article 30(2) of Directive 2004/38, read in the light, in particular, of Article 47 of the Charter**. Second, that question arises in the context of a genuine dispute relating to the legality of a decision refusing entry taken, pursuant to the directive, by the Secretary of State against ZZ. **Furthermore, although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision concerns State security cannot result in European Union law being inapplicable** (see, to this effect, Case C-387/05 Commission v Italy [2009] ECR I-11831, paragraph 45). "

Other interesting parts of the judgement:

- No presumption that the reasons invoked by a national authority in order to refuse [disclosure of those grounds] exist and are valid.
- If it turns out that State security does stand in the way of disclosure of the grounds to the person concerned, **judicial review of the legality of the decision** refusing entry must be carried out in a **procedure which strikes an appropriate balance between the requirements flowing from State security and the requirements of the right to effective judicial protection whilst limiting any interference with the exercise of that right to that which is strictly necessary**.

(2) Important abstracts from mandate to the European Commission to negotiate and adhere to the Council of Europe Convention for the protection of individuals with regard to processing of personal data ("Convention 108")

- "The modernised Convention 108 shall ensure a high level of protection of fundamental rights and freedoms with respect to the processing of personal data."
- "The Convention 108 shall remain comprehensive and wide in scope and general in nature."
- "The essential nature of the system of Convention 108, including its rules on exceptions and restrictions, shall not be altered. The rules shall when

necessary, be updated while maintaining the general nature and technological neutrality of the Convention. This should include inter alia provisions addressing quality and legitimacy of data processing, proportionality, special categories of data and supervisory authorities."

- "The consistency of Convention 108 with the EU data protection acquis shall be ensured taking duly into account the on-going reform of the data protection legislation. The Commission shall conduct negotiations in accordance with relevant Union legislation and coordinated positions of the Union established specifically for the purpose of those negotiations".
- "In particular, the Commission shall seek consistency between the EU data protection acquis and the Convention 108 rules governing trans-border data flows in order to ensure the effective application of EU rules on transborder data flows."

(3) State of Play of the modernisation of Convention 108

- On 27-29 November 2012 took place in Strasbourg the 29th plenary meeting of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("T-DP"), which is the Committee responsible for the modernisation of the Convention. The discussions finalised the work at technical level and presented a technical text of modernised Convention 108. Following active participation by the European Commission representatives (who participate as observers to the discussions), the outcome is coherent with the present EU acquis and leaves sufficient margin to adapt it, at a later stage, to the future acquis.
- The European Commission together with the Cypriot Presidency held a co-ordination meeting prior to the beginning of the CoE Committee's plenary session. MS representatives were reminded of their duty of loyal co-operation, which includes the duty not to negotiate or take commitments that are not compatible with the EU *acquis*.
- During the T-DP Plenary, the European Commission intervened on several occasions in order to ensure compatibility of the text to be adopted at technical level against the evolving EU *acquis*. This included the following interventions:
 - the text of certain provisions was kept rather general (e.g. household exception);
 - the text of certain provisions was bracketed and left open for further consideration at a later stage (e.g. precise qualification of consent as "explicit" or "unambiguous", which could be revisited by the "ad hoc Committee", ideally when we will know the final outcome of the negotiations on this issue at EU co-legislators' level);
 - deletion of ambiguous notion of "making available of data" as qualification for trans-border data flows which would have raised both legal (compatibility with ECJ case-law) and practical (an almost open-ended concept of the notion of "data transfer") issues;

- clarification and fine-tuning regarding the wording of two provisions that were brought in line with the EU *acquis*, namely:
 - o the provision on sensitive data (proposed redrafting by the EC according to structure and rationale of corresponding Directive 95/46/EC and proposed Regulation was taken on board); and
 - o the provision on trans-border data flows which allows the EU MS to derogate from the Convention's rules on free flow of data and apply higher standards to international transfers (proposed redrafting by the EC along the lines agreed with the LS and modelled after similar WTO provisions on regional custom unions). The inclusion of such a provision in the draft convention solves the most problematic issue in terms of articulation between the EU and CoE regimes.
- The Committee of Ministers adopted this month a mandate for an "ad hoc Committee" that will look at the technical text with a view to finalising the text prepared at technical level for adoption. Present in this "ad hoc Committee" will be the Member States, other Members of the Council of Europe, the European Commission as well as participants of third countries (as observers with no right to vote).
- **Next steps:** November 2013: The technical text will be transmitted to the "ad hoc Committee on data protection" (CAHDATA), bringing together representatives of all Council of Europe member States, other Parties to the Convention as well as other non-European States, before being submitted for formal endorsement by the Committee of Ministers.

Contact point: Katerina Dimitrakopoulou
DG JUSTICE/C.3 ☐ 91818

Director: Paul NEMITZ

0513

319

5200014#1

Glaser, Anika

Von: Dimroth, Johannes, Dr.
Gesendet: Freitag, 17. Januar 2014 18:09
An: Weinbrenner, Ulrich; Peters, Reinhard
Cc: PStSchröder_; Kutzschbach, Gregor, Dr.; OESI3AG_; ALOES_; Glaser, Anika
Betreff: AW: Eilt sehr: LIBE Berichtsentwurf NSA

Frau Stn H hat gebilligt.

Herzliche Grüße

Dr. Johannes Dimroth

Bundesministerium des Innern
Persönlicher Referent der
Staatssekretärin Dr. Emily Haber
Alt-Moabit 101 D, 10559 Berlin
Telefon: +49 30 18681-1116
E-Mail: johannes.dimroth@bmi.bund.de

2 d A
603717
Bundesministerium des Innern,
Parlamentarischer Staatssekretär
Dr. Ole Sebastian
Eing.: 20. Jan. 2014
Vorgang: AW 13/14 JF

Von: Weinbrenner, Ulrich
Gesendet: Freitag, 17. Januar 2014 16:26
An: Peters, Reinhard
Cc: PStSchröder_; Kutzschbach, Gregor, Dr.; OESI3AG_; StHaber_; ALOES_; Glaser, Anika
Betreff: Eilt sehr: LIBE Berichtsentwurf NSA
Wichtigkeit: Hoch

Herrn PStS

über

Frau Stn Haber (mdB um Billigung auch zur Weiterleitung an St Fritsche)

Herrn AL ÖS
Herrn UAL ÖS I

- wegen Eilbedürftigkeit nur per Email -

(Anlage)
1) Paralelles Modell
über informelle
Kommunikation Abt. I
2) Herr PStS ist
einverstanden
3) Versand am
20.1. (Anlage)
AW 2014

I. Votum

Es wird die Übersendung der unten stehenden Anregungen für Änderungen am LIBE-Berichtsentwurf vorgeschlagen.

II. Sachverhalt/Stellungnahme

Der LIBE-Ausschuss hat auf Grundlage von Expertenbefragungen, Gesprächen mit US- und EU-Behörden sowie Zeitungsartikeln einen Bericht zur NSA-Überwachungsprogrammen verfasst. Dieser kommt zu dem Schluss, dass die NSA z.T. gemeinsam mit Behörden in UK, Kanada und Neuseeland eine massenhafte Überwachung der elektronischen Kommunikation durchführt und dadurch vermutlich auch Rechte von EU-Bürgern und Mitgliedstaaten verletzt. Er schlägt ein breites Maßnahmenbündel vor: Überprüfung und Anpassung von Abkommen mit den USA, Stärkung von ENISA, dem Europol-Cybercrime-Center und dem EDPS und diversen Appellen an die Kommission und die Mitgliedstaaten. Schwerpunkt ist eine „Digitaler Habeas Corpus“, der 7 Punkte beinhaltet:

- 1. Abschluss des Datenschutzpakets in 2014

Stellungnahme: Grds. möglich. Allerdings sind noch eine Vielzahl bedeutender Frage zu klären. Gründlichkeit muss deshalb vor Schnelligkeit gehen.

2. Abschluss des EU-US-Datenschutzabkommens
Stellungnahme: Keine Bedenken. Zuständig ist EU –KOM.
3. Aussetzung des Safe-Harbour-Abkommens
Stellungnahme: Die Bundesregierung hat sich dafür eingesetzt, zur Verbesserung von Safe Harbor in der Datenschutz-Grundverordnung einen rechtlichen Rahmen zu schaffen. Falls die Datenschutz-Grundverordnung nicht bis 2015 verabschiedet werden kann, kann Safe Harbor auch unter der Richtlinie 95/46 überarbeitet und verbessert werden. Die Frage, ob eine Aussetzung des Safe-Harbor-Abkommen in Betracht kommt, wird gemeinsam mit unseren europäischen Partner in Brüssel erörtert.
4. Aussetzung des TFTP-Abkommens (betr. Zugang zu SWIFT-Daten zur Terrorismusbekämpfung) bis zum Abschluss des Datenschutzabkommens
Stellungnahme: Angesichts der Tatsache, dass die Kommission nach Abschluss ihrer Konsultationen zu den Vorwürfen, die USA hätten unter Umgehung des TFTP-Abkommens direkten Zugriff auf den SWIFT-Server genommen, keine Anhaltspunkte für einen Verstoß feststellen konnte, besteht aus unserer Sicht derzeit kein Anlass, das Abkommen auszusetzen.
5. Besserer Schutz der Rechte von EU-Bürgern (ohne Konkretisierung)
Stellungnahme: Keine Bedenken.
6. Entwicklung einer Strategie für eine Europäische (unabhängige) IT-Industrie
Stellungnahme: Zustimmung. Entspricht einer Forderung aus dem Koalitionsvertrag: „Um Freiheit und Sicherheit im Internet zu schützen, stärken und gestalten wir die Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum. Dazu treten wir für eine europäische Cybersicherheitsstrategie ein, ergreifen Maßnahmen zur Rückgewinnung der technologischen Souveränität, unterstützen die Entwicklung Moderner Staat, innere Sicherheit und Bürgerrechte vertrauenswürdiger IT- und Netz-Infrastruktur sowie die Entwicklung sicherer Soft- und Hardware und sicherer Cloud-Technologie und begrüßen auch Angebote eines nationalen bzw. europäischen Routings.“
7. EU-Politik als Referenz für demokratische und neutrale Internet-Governance
Stellungnahme: Keine Bedenken.

III. Stellungnahme im Übrigen:

Die Schlussfolgerungen überraschen wenig, auch wenn sie teilweise nicht belegt werden können, sondern nur auf Vermutungen oder Presseberichte zurückgreifen. Einige Punkte sind aus deutscher Sicht jedoch kritisch und sollten daher gestrichen werden. Im Einzelnen:

1) S. 16 (Main findings Nr. 2): Der Ausschuss glaubt, dass (neben Frankreich und Schweden) **auch Deutschland ähnliche Überwachungsprogramme wie PRISM betreibt**. Diesem ist entschieden entgegenzutreten. Deutsche Behörden dürfen Kommunikationsdaten nur im Einzelfall, auf gesetzlicher Grundlage und einer förmlichen Anordnung erheben. Auch die strategische Fernmeldeaufklärung nach § 5 Artikel 10 Gesetz ist nur in eng begrenzten Fällen aufgrund in der Anordnung vorab festgelegter und nach Anordnung der G10-Kommission unter der Kontrolle durch das parlamentarische Kontrollgremium, dass die betroffenen TK-Beziehungen zu bestätigen hat, zulässig. Zudem sieht § 10 Abs. 4 S. 4 G 10 eine Beschränkung auf 20 % des möglichen Aufkommens vor.

2) S. 19 (Recommendations Nr. 20): Dementsprechend ist auch die **Aufforderung an Deutschland** (neben UK, Frankreich, Schweden und den Niederlanden), **seine Gesetzgebung zu überprüfen bzw. zu überarbeiten**, zu streichen. Die hier einschlägigen Vorschriften entsprechend den Vorgaben aus den entsprechenden Urteilen des

Bundesverfassungsgerichts und sind mit den Grundrechten vereinbar. Unabhängig davon liegt die nationale Sicherheitsgesetzgebung außerhalb der Zuständigkeit der EU und damit auch des EP.

3) S. 24 (Recommendations Nr. 24): Problematisch ist auch die Aufforderung an alle Mitgliedstaaten, die unterstellten Verletzungen ihrer Souveränität auch gerichtlich geltend zu machen. Es obliegt alleine der Entscheidung des Mitgliedstaats, ob er seine Souveränität verletzt sieht und auf welchem Wege er dagegen ggf. vorgehen will.

Weinbrenner

Dr. Kutzschbach

Von: PStSchröder_

Gesendet: Freitag, 10. Januar 2014 11:14

An: ALOES_

Cc: StFritsche_; UALOESI_; StabOESII_; UALGII_; OESI3AG_; MB_; Baum, Michael, Dr.; PStSchröder_; AA Eickelpasch, Jörg

Betreff: LIBE Berichtsentwurf NSA mdB um Stellungnahme bis 17.1.

g. 13/14

sehr geehrter Herr Kaller,

Herr PStS hat den beigefügten Berichtsentwurf von Herrn Voss, MdEP, erhalten. Dies war verbunden mit dem Angebot, Anregungen für Änderungsvorschläge einzubringen, die MdEP Voss bis 22.1. ggü. LIBE-Ausschuss einbringen könnte.

Vor diesem Hintergrund bittet Herr PStS um Prüfung, Stellungnahme und ggf. weitergabefähige Vorschläge für Änderungsanträge bis **Freitag, den 17.1. DS** (Eingang Büro PStS).

Zum Verfahren waren folgende Informationen beigefügt:

Es handelt sich um den Berichtsentwurf von Berichterstatter Claudé Moraes (S&D, UK) der NSA-Arbeitsgruppe zum Thema "US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs". Der Berichtsentwurf stellt das Abschlussdokument der NSA-Arbeitsgruppe dar. Diese wurde per Entschließungsantrag am 4. Juli 2013 im Rahmen des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) eingerichtet, um den Sachverhalt um die mutmaßliche Internetüberwachung durch die NSA zu untersuchen und dem LIBE-Ausschuss seine Erkenntnisse in Form eines Endberichts vorzulegen. Nach 15 Anhörungen liegt dieser Bericht nun zur Prüfung vor und kann nun durch Änderungsanträge abgeändert werden.

Frist für Änderungsanträge ist der 22. Januar. Der weitere Zeitplan sieht eine Abstimmung im LIBE-Ausschuss im Februar und anschließend eine Abstimmung im Plenum im März vor.

Mit freundlichen Grüßen

Im Auftrag

Alexandra Kuczynski

Bundesministerium des Innern
 Persönliche Referentin des
 Parlamentarischen Staatssekretärs Dr. Ole Schröder
 Alt-Moabit 101 D, 10559 Berlin

Telefon: +49 (0)30 18 681 1056
 Fax: +49 (0)30 18 681 1137

OSI3 -

Herrn PStS mdB
322
neu Bkupp vor

Kuczynski, Alexandra

An: VOSS Axel
Cc: AA Eickelpasch, Jörg
Betreff: Anmerkungen zum LIBE-Berichtsentwurf NSA
Anlagen: 131223 draft report.doc

52000 14111

Abganz

Au 2011

en-Au 2011

Sehr geehrte Frau Toporan,

im Auftrag von Herrn PStS darf ich Ihnen folgende Stellungnahme für Herrn Voss, MdEP zukommen lassen. Diese gliedert sich in einen allgemeinen Sachverhalt / Stellungnahme (I.) und einen Teil mit konkreten Änderungsvorschlägen (II). Schließlich ist darüber hinaus (!) ein Dokument einigen Anmerkungen/ Kommentierungen beigelegt, die eventl. für die weitere Diskussion hilfreich sind.

I. Sachverhalt/Stellungnahme

Der LIBE-Ausschuss hat auf Grundlage von Expertenbefragungen, Gesprächen mit US- und EU-Behörden sowie Zeitungsartikeln einen Bericht zur NSA-Überwachungsprogrammen verfasst. Dieser kommt zu dem Schluss, dass die NSA z.T. gemeinsam mit Behörden in UK, Kanada und Neuseeland eine massenhafte Überwachung der elektronischen Kommunikation durchführt und dadurch vermutlich auch Rechte von EU-Bürgern und Mitgliedstaaten verletzt. Er schlägt ein breites Maßnahmenbündel vor: Überprüfung und Anpassung von Abkommen mit den USA, Stärkung von ENISA, dem Europol-Cybercrime-Center und dem EDPS und diversen Appellen an die Kommission und die Mitgliedstaaten. Schwerpunkt ist eine „Digitaler Habeas Corpus“, der 7 Punkte beinhaltet:

1. Abschluss des Datenschutzpakets in 2014
Stellungnahme: Grds. möglich. Allerdings sind noch eine Vielzahl bedeutender Frage zu klären. Gründlichkeit muss deshalb vor Schnelligkeit gehen.
2. Abschluss des EU-US-Datenschutzabkommens
Stellungnahme: Keine Bedenken. Zuständig ist EU-KOM.
3. Aussetzung des Safe-Harbour-Abkommens
Stellungnahme: Die Bundesregierung hat sich dafür eingesetzt, zur Verbesserung von Safe Harbor in der Datenschutz-Grundverordnung einen rechtlichen Rahmen zu schaffen. Falls die Datenschutz-Grundverordnung nicht bis 2015 verabschiedet werden kann, kann Safe Harbor auch unter der Richtlinie 95/46 überarbeitet und verbessert werden. Die Frage, ob eine Aussetzung des Safe-Harbour-Abkommen in Betracht kommt, wird gemeinsam mit unseren europäischen Partner in Brüssel erörtert.
4. Aussetzung des TFTP-Abkommens (betr. Zugang zu SWIFT-Daten zur Terrorismusbekämpfung) bis zum Abschluss des Datenschutzabkommens
Stellungnahme: Angesichts der Tatsache, dass die Kommission nach Abschluss ihrer Konsultationen zu den Vorwürfen, die USA hätten unter Umgehung des TFTP-Abkommens direkten Zugriff auf den SWIFT-Server genommen, keine Anhaltspunkte für einen Verstoß feststellen konnte, besteht aus unserer Sicht derzeit kein Anlass, das Abkommen auszusetzen.
5. Besserer Schutz der Rechte von EU-Bürgern (ohne Konkretisierung)
Stellungnahme: Keine Bedenken.
6. Entwicklung einer Strategie für eine Europäische (unabhängige) IT-Industrie
Stellungnahme: Zustimmung. Entspricht einer Forderung aus dem Koalitionsvertrag: „Um Freiheit und Sicherheit im Internet zu schützen, stärken und gestalten wir die Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum. Dazu treten

wir für eine europäische Cybersicherheitsstrategie ein, ergreifen Maßnahmen zur Rückgewinnung der technologischen Souveränität, unterstützen die Entwicklung Moderner Staat, innere Sicherheit und Bürgerrechte vertrauenswürdiger IT- und Netz-Infrastruktur sowie die Entwicklung sicherer Soft- und Hardware und sicherer Cloud-Technologie und begrüßen auch Angebote eines nationalen bzw. europäischen Routings.“

7. EU-Politik als Referenz für demokratische und neutrale Internet-Governance
Stellungnahme: Keine Bedenken.

II. Änderungsvorschläge:

Die Schlussfolgerungen überraschen wenig, auch wenn sie teilweise nicht belegt werden können, sondern nur auf Vermutungen oder Presseberichte zurückgreifen. Einige Punkte sind aus deutscher Sicht jedoch kritisch und sollten daher gestrichen werden. Im Einzelnen:

1) S. 16 (Main findings Nr. 2): Der Ausschuss glaubt, dass (neben Frankreich und Schweden) **auch Deutschland ähnliche Überwachungsprogramme wie PRISM** betreibt. Diesem ist entschieden entgegenzutreten. Deutsche Behörden dürfen Kommunikationsdaten nur im Einzelfall, auf gesetzlicher Grundlage und einer förmlichen Anordnung erheben. Auch die strategische Fernmeldeaufklärung nach § 5 Artikel 10 Gesetz ist nur in eng begrenzten Fällen aufgrund in der Anordnung vorab festgelegter und nach Anordnung der G10-Kommission unter der Kontrolle durch das parlamentarische Kontrollgremium, dass die betroffenen TK-Beziehungen zu bestätigen hat, zulässig. Zudem sieht § 10 Abs. 4 S. 4 G 10 eine Beschränkung auf 20 % des möglichen Aufkommens vor.

2) S. 19 (Recommendations Nr. 20): Dementsprechend ist auch die **Aufforderung an Deutschland** (neben UK, Frankreich, Schweden und den Niederlanden), **seine Gesetzgebung zu überprüfen bzw. zu überarbeiten**, zu streichen. Die hier einschlägigen Vorschriften entsprechend den Vorgaben aus den entsprechenden Urteilen des Bundesverfassungsgerichts und sind mit den Grundrechten vereinbar. Unabhängig davon liegt die nationale Sicherheitsgesetzgebung außerhalb der Zuständigkeit der EU und damit auch des EP.

3) S. 24 (Recommendations Nr. 24): Problematisch ist auch die Aufforderung an alle Mitgliedstaaten, die unterstellten Verletzungen ihrer Souveränität auch gerichtlich geltend zu machen. Es obliegt alleine der Entscheidung des Mitgliedstaats, ob er seine Souveränität verletzt sieht und auf welchem Wege er dagegen ggf. vorgehen will.

Mit freundlichen Grüßen

Im Auftrag

Alexandra Kuczynski

Bundesministerium des Innern
 Persönliche Referentin des
 Parlamentarischen Staatssekretärs Dr. Ole Schröder
 Alt-Moabit 101 D, 10559 Berlin

Telefon: +49 (0)30 18 681 1056
 Fax: +49 (0)30 18 681 1137
 E-Mail: alexandra.kuczynski@bmi.bund.de

Von: Kuczynski, Alexandra
Gesendet: Freitag, 10. Januar 2014 11:23
An: 'VOSS Axel'
Betreff: AW/ Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrte Frau Toporan,

vielen Dank für die Übersendung des Entwurfs verbunden mit der Möglichkeit, Änderungsvorschläge zu übermitteln. BMI prüft und Herr Voss erhält eine Rückmeldung von Herrn Schröder.

Viele Grüße von der Spree,

Alexandra Kuczynski
 PR'n PStS.

P.S. Bitte übermitteln Sie Herrn Voss auch herzliche Grüße von Herrn Schröder.

Von: VOSS Axel [<mailto:axel.voss@europarl.europa.eu>]
Gesendet: Donnerstag, 9. Januar 2014 18:19
An: PStSchröder_
Betreff: JP/ Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrter Herr Dr. Schröder,

anbei sende ich Ihnen im Auftrag von Herrn Voss (MdEP) den Berichtsentwurf von Berichterstatter Claude Moraes (S&D, UK) der NSA-Arbeitsgruppe zum Thema "US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs". Der Berichtsentwurf stellt das Abschlussdokument der NSA-Arbeitsgruppe dar. Diese wurde per Entschließungsantrag am 4. Juli 2013 im Rahmen des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) eingerichtet, um den Sachverhalt um die mutmaßliche Internetüberwachung durch die NSA zu untersuchen und dem LIBE-Ausschuss seine Erkenntnisse in Form eines Endberichts vorzulegen. Nach 15 Anhörungen liegt dieser Bericht nun zur Prüfung vor und kann nun durch Änderungsanträge abgeändert werden.

Sollten Sie Ideen oder Anregungen für Änderungsvorschläge haben, sind diese gerne willkommen. Frist für Änderungsanträge ist der 22. Januar. Der weitere Zeitplan sieht eine Abstimmung im LIBE-Ausschuss im Februar und anschließend eine Abstimmung im Plenum im März vor.

Falls Sie Fragen haben sollten oder weiter Informationen benötigen, stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen,

Selma Toporan

Selma Toporan
 (Parlamentarische Referentin)

Büro Axel Voss, MdEP
 Europäisches Parlament
 ASP 15 E 150
 Rue Wiertz
 B-1047 Brüssel

Tel.: +32-2-28 47302

Fax: +32-2-28 49302

Email: selma.toporan@europarl.europa.eu

Kuczynski, Alexandra

Von: PStSchröder_
Gesendet: Montag, 20. Januar 2014 11:57
An: 'VOSS Axel'
Cc: AA Eickelpasch, Jörg; Weinbrenner, Ulrich; PStSchröder_
Betreff: Anmerkungen zum LIBE-Berichtsentwurf NSA
Anlagen: 131223 draft report.doc

Sehr geehrte Frau Toporan,

im Auftrag von Herrn PStS darf ich Ihnen folgende Stellungnahme für Herrn Voss, MdEP zukommen lassen. Diese gliedert sich in einen allgemeinen Sachverhalt / Stellungnahme (I.) und einen Teil mit konkreten Änderungsvorschlägen (II). Schließlich ist darüber hinaus (!) ein Dokument einigen Anmerkungen/ Kommentierungen beigelegt, die eventl. für die weitere Diskussion hilfreich sind.

I. Sachverhalt/Stellungnahme

Der LIBE-Ausschuss hat auf Grundlage von Expertenbefragungen, Gesprächen mit US- und EU-Behörden sowie Zeitungsartikeln einen Bericht zur NSA-Überwachungsprogrammen verfasst. Dieser kommt zu dem Schluss, dass die NSA z.T. gemeinsam mit Behörden in UK, Kanada und Neuseeland eine massenhafte Überwachung der elektronischen Kommunikation durchführt und dadurch vermutlich auch Rechte von EU-Bürgern und Mitgliedstaaten verletzt. Er schlägt ein breites Maßnahmenbündel vor: Überprüfung und Anpassung von Abkommen mit den USA, Stärkung von ENISA, dem Europol-Cybercrime-Center und dem EDPS und diversen Appellen an die Kommission und die Mitgliedstaaten. Schwerpunkt ist eine „Digitaler Habeas Corpus“, der 7 Punkte beinhaltet:

1. Abschluss des Datenschutzpakets in 2014
Stellungnahme: Grds. möglich. Allerdings sind noch eine Vielzahl bedeutender Frage zu klären. Gründlichkeit muss deshalb vor Schnelligkeit gehen.
2. Abschluss des EU-US-Datenschutzabkommens
Stellungnahme: Keine Bedenken. Zuständig ist EU-KOM.
3. Aussetzung des Safe-Harbour-Abkommens
Stellungnahme: Die Bundesregierung hat sich dafür eingesetzt, zur Verbesserung von Safe Harbor in der Datenschutz-Grundverordnung einen rechtlichen Rahmen zu schaffen. Falls die Datenschutz-Grundverordnung nicht bis 2015 verabschiedet werden kann, kann Safe Harbor auch unter der Richtlinie 95/46 überarbeitet und verbessert werden. Die Frage, ob eine Aussetzung des Safe-Harbour-Abkommen in Betracht kommt, wird gemeinsam mit unseren europäischen Partner in Brüssel erörtert.
4. Aussetzung des TFTP-Abkommens (betr. Zugang zu SWIFT-Daten zur Terrorismusbekämpfung) bis zum Abschluss des Datenschutzabkommens
Stellungnahme: Angesichts der Tatsache, dass die Kommission nach Abschluss ihrer Konsultationen zu den Vorwürfen, die USA hätten unter Umgehung des TFTP-Abkommens direkten Zugriff auf den SWIFT-Server genommen, keine Anhaltspunkte für einen Verstoß feststellen konnte, besteht aus unserer Sicht derzeit kein Anlass, das Abkommen auszusetzen.
5. Besserer Schutz der Rechte von EU-Bürgern (ohne Konkretisierung)
Stellungnahme: Keine Bedenken.
6. Entwicklung einer Strategie für eine Europäische (unabhängige) IT-Industrie

Stellungnahme: Zustimmung. Entspricht einer Forderung aus dem Koalitionsvertrag:

„Um Freiheit und Sicherheit im Internet zu schützen, stärken und gestalten wir die Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum. Dazu treten wir für eine europäische Cybersicherheitsstrategie ein, ergreifen Maßnahmen zur Rückgewinnung der technologischen Souveränität, unterstützen die Entwicklung Moderner Staat, innere Sicherheit und Bürgerrechte vertrauenswürdiger IT- und Netz-Infrastruktur sowie die Entwicklung sicherer Soft- und Hardware und sicherer Cloud-Technologie und begrüßen auch Angebote eines nationalen bzw. europäischen Routings.“

7. EU-Politik als Referenz für demokratische und neutrale Internet-Governance

Stellungnahme: Keine Bedenken.

II. Änderungsvorschläge:

Die Schlussfolgerungen überraschen wenig, auch wenn sie teilweise nicht belegt werden können, sondern nur auf Vermutungen oder Presseberichte zurückgreifen. Einige Punkte sind aus deutscher Sicht jedoch kritisch und sollten daher gestrichen werden. Im Einzelnen:

1) S. 16 (Main findings Nr. 2): Der Ausschuss glaubt, dass (neben Frankreich und Schweden) auch Deutschland ähnliche Überwachungsprogramme wie PRISM betreibt. Diesem ist entschieden entgegenzutreten. Deutsche Behörden dürfen Kommunikationsdaten nur im Einzelfall, auf gesetzlicher Grundlage und einer förmlichen Anordnung erheben. Auch die strategische Fernmeldeaufklärung nach § 5 Artikel 10 Gesetz ist nur in eng begrenzten Fällen aufgrund in der Anordnung vorab festgelegter und nach Anordnung der G10-Kommission unter der Kontrolle durch das parlamentarische Kontrollgremium, dass die betroffenen TK-Beziehungen zu bestätigen hat, zulässig. Zudem sieht § 10 Abs. 4 S. 4 G 10 eine Beschränkung auf 20 % des möglichen Aufkommens vor.

2) S. 19 (Recommendations Nr. 20): Dementsprechend ist auch die Aufforderung an Deutschland (neben UK, Frankreich, Schweden und den Niederlanden), seine Gesetzgebung zu überprüfen bzw. zu überarbeiten, zu streichen. Die hier einschlägigen Vorschriften entsprechend den Vorgaben aus den entsprechenden Urteilen des Bundesverfassungsgerichts und sind mit den Grundrechten vereinbar. Unabhängig davon liegt die nationale Sicherheitsgesetzgebung außerhalb der Zuständigkeit der EU und damit auch des EP.

3) S. 24 (Recommendations Nr. 24): Problematisch ist auch die Aufforderung an alle Mitgliedstaaten, die unterstellten Verletzungen ihrer Souveränität auch gerichtlich geltend zu machen. Es obliegt alleine der Entscheidung des Mitgliedstaats, ob er seine Souveränität verletzt sieht und auf welchem Wege er dagegen ggf. vorgehen will.

Mit freundlichen Grüßen

Im Auftrag

Alexandra Kuczynski

Bundesministerium des Innern
 Persönliche Referentin des
 Parlamentarischen Staatssekretärs Dr. Ole Schröder
 Alt-Moabit 101 D, 10559 Berlin

Telefon: +49 (0)30 18 681 1056
 Fax: +49 (0)30 18 681 1137
 E-Mail: alexandra.kuczynski@bmi.bund.de

Von: Kuczynski, Alexandra
Gesendet: Freitag, 10. Januar 2014 11:23
An: 'VOSS Axel'
Betreff: AW: JP/ Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrte Frau Toporan,

vielen Dank für die Übersendung des Entwurfs verbunden mit der Möglichkeit, Änderungsvorschläge zu übermitteln. BMI prüft und Herr Voss erhält eine Rückmeldung von Herrn Schröder.

Viele Grüße von der Spree,

Alexandra Kuczynski
PR'n PStS

S. Bitte übermitteln Sie Herrn Voss auch herzliche Grüße von Herrn Schröder.

Von: VOSS Axel [<mailto:axel.voss@europarl.europa.eu>]
Gesendet: Donnerstag, 9. Januar 2014 18:19
An: PStSchröder_
Betreff: JP/ Berichtsentwurf zum Überwachungsprogramm der US-amerikanischen NSA

Sehr geehrter Herr Dr. Schröder,

anbei sende ich Ihnen im Auftrag von Herrn Voss (MdEP) den Berichtsentwurf von Berichterstatter Claude Moraes (S&D, UK) der NSA-Arbeitsgruppe zum Thema "US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs". Der Berichtsentwurf stellt das Abschlussdokument der NSA-Arbeitsgruppe dar. Diese wurde per Entschließungsantrag am 4. Juli 2013 im Rahmen des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) eingerichtet, um den Sachverhalt um die mutmaßliche Internetüberwachung durch die NSA zu untersuchen und dem LIBE-Ausschuss seine Erkenntnisse in Form eines Endberichts vorzulegen. Nach 15 Anhörungen liegt dieser Bericht nun zur Prüfung vor und kann nun durch Änderungsanträge abgeändert werden.

Sollten Sie Ideen oder Anregungen für Änderungsvorschläge haben, sind diese gerne willkommen. Frist für Änderungsanträge ist der 22. Januar. Der weitere Zeitplan sieht eine Abstimmung im LIBE-Ausschuss im Februar und anschließend eine Abstimmung im Plenum im März vor.

Falls Sie Fragen haben sollten oder weiter Informationen benötigen, stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen,

Selma Toporan

Selma Toporan
(Parlamentarische Referentin)

Büro Axel Voss, MdEP
Europäisches Parlament
ASP 15 E 150
Rue Wiertz
B-1047 Brüssel

Tel.:+32-2-28 47302

Fax:+32-2-28 49302

Email: selma.toporan@europarl.europa.eu

Dokument 2014/0032145

Von: Spitzer, Patrick, Dr.
Gesendet: Dienstag, 21. Januar 2014 18:39
An: VI4_; PGDS_; IT1_; OESII1_; OESIII1_
Cc: RegOeSI3; OESI3AG_; Weinbrenner, Ulrich; Taube, Matthias; Stöber, Karlheinz, Dr.; PGNSA; Bender, Ulrike; Schlender, Katharina; Mammen, Lars, Dr.; Papenkort, Katja, Dr.; Marscholleck, Dietmar; B3_; Wenske, Martina
Betreff: Frist 22.01., 11:00 Uhr: Anforderung eines Berichtsbogens zur Unterrichtung des Deutschen Bundestages (17067/13)

Wichtigkeit: Hoch

ÖS I 3 – 52001/3#2



~~2014_01_21_Patrick_Spitzer_OESI3AG.pdf~~

Liebe Kolleginnen und Kollegen,

ich bitte um Mitzeichnung zum als Anlage 1 beigefügten Berichtsbogen zur Unterrichtung des Deutschen Bundestages **bis morgen, 22. Januar 2014, 11.00 Uhr**. Grundlage der Berichterstattung ist das als Anlage 2 beigefügte Dokument „Rebuilding Trust in EU US Data Flows“.

Freundliche Grüße

Patrick Spitzer

im Auftrag
Dr. Patrick Spitzer

Bundesministerium des Innern
Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,
BKA-Gesetz, Datenschutz im Sicherheitsbereich)
Alt-Moabit 101D, 10559 Berlin
Telefon: +49 (0)30 18681-1390
E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

B E R I C H T S B O G E N

gemäß Anlage zu § 6 Absatz 2 EUZBBG und Ziffer II. 3. der Anlage zu § 9 EUZBLG

Ressort/Referat:	AG ÖS I 3	Datum:	20.01.2014
Referatsleiterin/ Referatsleiter:	MinR Weinbrenner MinR Taube	Telefon:	030 186811300
Bearbeiterin/ Bearbeiter:	RR Dr. Spitzer	Telefon:	030 186811390
abgestimmt mit:	BMJV; BMWi, AA	Telefax:	

Thema:	Mitteilung der Kommission an das Europäische Parlament und den Rat über die Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA
Sachgebiet:	Europäische Justiz- und Innenpolitik
Ratsdok.-Nummer:	17067/13
KOM-Nummer:	COM(2013) 846 final
Nummer des interinstitutionellen Dossiers:	nicht bekannt
Nummer der Bundesratsdrucksache:	nicht bekannt
Nachweis der Zulässigkeit für europäische Regelungen: (Prüfung der Rechtsgrundlage)	entfällt, da kein Rechtsakt
Subsidiaritätsprüfung:	entfällt, da kein Rechtsakt
Verhältnismäßigkeitsprüfung:	entfällt, da kein Rechtsakt
Zielsetzung:	Ausarbeitung von Maßnahmen zur Berücksichtigung beim Datenaustausch zwischen den USA und der EU vor dem Hintergrund der Veröffentlichungen zur Überwachungstätigkeit der NSA.
Inhaltliche Schwerpunkte:	Die Mitteilung ist ein politisches Strategiepapier über die transatlantischen Datenströme, in dem die sich aus den Enthüllungen über die umfangreichen Programme der US-Nachrichtendienste zur Sammlung von Informationen ergebenden Herausforderungen und Risiken beschrieben und die erforderlichen Maßnahmen zur Ausräumung der genannten Bedenken dargelegt werden. Das Papier fasst

- 2 -

verschiedene weitere Veröffentlichungen der EU zu Einzelthemen, wie die Analyse über die Funktionsweise des „Safe Harbour Abkommens“ und den Bericht über das TFTP-Abkommen (auch SWIFT-Abkommen genannt), zusammen.

Folgende Maßnahmen werden aufgegriffen:

Datenschutzreformpaket

KOM sieht ist das von ihr Anfang 2012 vorgeschlagene Datenschutzreformpaket als ein Schlüsselement in Bezug auf den Schutz personenbezogener Daten an. Als Begründung werden fünf Elemente, die aus ihrer Sicht insoweit entscheidend sind, angeführt: das Marktortprinzip, Regelungen zu Drittstaatenübermittlungen, Sanktionen, Regelungen zu Verantwortlichkeiten und die Regelungen im Bereich Polizei und Justiz.

Verbesserung von Safe Harbour

KOM identifiziert als Schwachstellen der Safe-Harbor-Regelung Defizite bei der Transparenz und der Durchsetzung der Vereinbarung (insbesondere Inhalt und Veröffentlichung der Datenschutzerklärung der Safe-Harbor-registrierten Unternehmen, Verfügbarkeit alternativer Konfliktlösungsmechanismen für EU-Bürger, Durchsetzung durch die zuständigen US-Behörden, Zugang zu den Daten durch US-Sicherheitsbehörden) und gibt Empfehlungen zur verbesserten Umsetzung von Safe Harbor ab. Darüber hinaus kündigt KOM Gespräche mit den US-Behörden an, die der Identifizierung von Schwachstellen und deren Abhilfe bis Sommer 2014 dienen sollen.

Abschluss eines EU-US Datenschutzabkommens

KOM strebt den Abschluss eines Rahmenabkommens zum Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen an. Ein solches Abkommen solle den Rahmen für eine möglichst hohes Datenschutzniveau vorgeben und u.a. auch für einen effektiven Rechtsschutz für EU-Bürger außerhalb der USA geben und ggf. durch fachspezifische Einzelabkommen, wie das EU-US PNR- und das TFTP- Abkommen ergänzt werden.

Berücksichtigung von EU-Interessen im laufenden US-Reformprozess

Die von US-Präsident Obama initiierte Evaluierung der US-Sicherheitsbehörden soll genutzt werden, um eine Anhebung der Standards für EU-Bürger zu erreichen. Der Bericht spricht u.a. die Ungleichbehandlung von US- und EU-Bürgern, unterschiedliche Auffassungen über die Auslegung des Verhältnismäßigkeitsgrundsatzes und die mangelnden Rechtsschutzmöglichkeiten für EU-Bürger in den USA als zentrale Punkte an.

Politische Bedeutung:	Die politische Bedeutung ist nicht zuletzt vor dem Hintergrund der Veröffentlichungen zu Aktivitäten amerikanischer Nachrichtendienste mit hoch zu bewerten.
Was ist das besondere deutsche Interesse?	<p>Aufgrund der unmittelbaren Betroffenheit Deutschlands durch die Veröffentlichungen Edward Snowdens besteht an allen diesbezüglichen Maßnahmen/Empfehlungen grundsätzlich ein besonderes Interesse. Im Einzelnen:</p> <p><u>Datenschutzreformpaket</u></p> <p>Der dargestellte Zusammenhang zwischen den Überwachungsmaßnahmen und der Datenschutz-Grundverordnung (DSGVO) vermag nur teilweise zu überzeugen. Zutreffend ist, dass das Marktortprinzip zu einer Verbesserung des Datenschutzes im transatlantischen Verhältnis beitragen dürfte, weil US-Unternehmen in Europa unmittelbar an EU-Recht gebunden werden können. Bei den Drittstaatenregelungen ist zu differenzieren. Allgemein dürften die von der KOM vorgeschlagenen Regelungen kaum zu einer Verbesserung führen. Dies gilt insbesondere für Übermittlungen von Unternehmen an US-Behörden. Hierzu hatte DEU einen neuen Art. 42a vorgeschlagen. Die bisher formulierten Anforderungen an die Übermittlung personenbezogener Daten in Drittstaaten werden auch der technischen Entwicklung und Vernetzung noch nicht gerecht. Entgegen der Behauptungen der KOM bleiben insbesondere zentrale Fragen der Übermittlung, z.B. beim „Cloud computing“, ungelöst. Zu begrüßen ist, dass die KOM Ideen der US-Seite aufgegriffen hat, die das Weiße Haus in seinem Papier „Consumer Data Privacy in a Networked World („Consumer Bill of Rights“) im Februar 2012 entwickelt hat. Allerdings lässt KOM offen, wie sich diese Ideen in die DSGVO inkorporieren lassen.</p> <p><u>Safe Harbour</u></p> <p>Die Bundesregierung hat sich wiederholt für eine Verbesserung der Safe-Harbor-Regelung ausgesprochen, die schnellstmögliche Vorlage des KOM-Berichts zu Safe Harbor gefordert und drängt in der EU auf Nachverhandlungen des Safe-Harbor-Abkommens. Sie unterstützt die Vorschläge der KOM zur Verbesserung von Safe Harbor. Darüber hinaus setzt sie sich dafür ein, für Modelle wie Safe Harbor in der europäischen Datenschutz-Grundverordnung einen robusten Rechtsrahmen mit klaren Vorgaben für Garantien der Bürgerinnen und Bürger zu schaffen und hat bereits einen entsprechenden Vorschlag in die Verhandlungen in der Ratsarbeitsgruppe DAPIX eingebracht. Ziel ist es, die Individualrechte der Bürgerinnen und Bürger zu stärken und ihnen bessere Rechtsschutzmöglichkeiten zur Verfügung zu stellen, die Registrierung der Unternehmen in der EU vorzunehmen und die staatliche Kontrolle seitens der EU-Datenschutzaufsichtsbehörden in Modellen wie Safe-Harbor zu stärken.</p>

- 4 -

	<p><u>EU-US-Datenschutzabkommen</u></p> <p>Deutschland hat sich für einen baldigen Abschluss des Abkommens unter der Voraussetzung, dass damit mit Blick auf den Schutz personenbezogener Daten und den Individualrechtsschutz ein wirklicher Mehrwert geschaffen wird, ausgesprochen.</p> <p>Bislang haben sich die Verhandlungen schwierig gestaltet. In wichtigen Punkten herrscht weiterhin keine Einigung, so bei der Speicherdauer, der unabhängigen Aufsicht, den Individualrechten und dem Rechtsschutz. Auch wollen die USA weiterhin das Abkommen als sog. „executive agreement“ abschließen; ein solches kann US-Recht nicht abändern. Bei EU/US Justice and Home Affairs Ministerial Treffen am 18.11.2013 haben beide Seiten das Ziel bekräftigt, die Verhandlungen bis zum Sommer 2014 abzuschließen.</p> <p><u>Berücksichtigung von EU-Interessen im laufenden US-Reformprozess</u></p> <p>Deutschland hat sich auch auf EU-Ebene in den Prozess zur Aufklärung des Sachverhalts im Zusammenhang mit den Veröffentlichungen von Edward Snowden und zur Erarbeitung konkreter Empfehlungen der EU und der MS zur Berücksichtigung in der laufenden US-internen Evaluierung der Überwachungsprogramme intensiv eingebracht. Ein entsprechendes Dokument mit Vorschlägen zur Anwendung des Verhältnismäßigkeitsprinzips, zum verbesserten Individualrechtsschutz und zur Gleichstellung von EU- und US-Bürgern wurde am 6. Dezember 2013 im Rahmen des JI-Ministertreffens in Brüssel verabschiedet.</p>
bisherige Position des Deutschen Bundestages:	nicht bekannt
Position des Bundesrates:	nicht bekannt
Position des Europäischen Parlaments:	nicht bekannt
Meinungsstand im Rat:	nicht bekannt
Verfahrensstand: (Stand der Befassung)	
Finanzielle Auswirkungen:	

Zeitplan für die Behandlung im

- 5 -

a) Bundesrat:	nicht bekannt
b) Europäischen Parlament:	nicht bekannt
c) Rat:	nicht bekannt



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 29 November 2013

17067/13

**JAI 1095
USA 64
DATAPROTECT 190
COTER 154**

COVER NOTE

from: Secretary-General of the European Commission,
signed by Mr Jordi AYET PUIGARNAU, Director

date of receipt: 28 November 2013

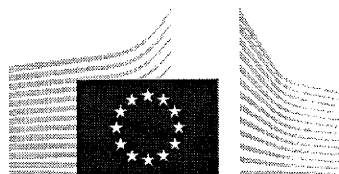
to: Mr Uwe CORSEPIUS, Secretary-General of the Council of the European
Union

No Cion doc.: COM(2013) 846 final

Subject: Communication from the Commission to the European Parliament and the
Council
Rebuilding Trust in EU-US Data Flows

Delegations will find attached Commission document COM(2013) 846 final.

Encl.: COM(2013) 846 final



**EUROPEAN
COMMISSION**

Brussels, 27.11.2013
COM(2013) 846 final

**COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN
PARLIAMENT AND THE COUNCIL**

Rebuilding Trust in EU-US Data Flows

1. INTRODUCTION: THE CHANGING ENVIRONMENT OF EU-US DATA PROCESSING

The European Union and the United States are strategic partners, and this partnership is critical for the promotion of our shared values, our security and our common leadership in global affairs.

However, trust in the partnership has been negatively affected and needs to be restored. The EU, its Member States and European citizens have expressed deep concerns at revelations of large-scale US intelligence collection programmes, in particular as regards the protection of personal data¹. Mass surveillance of private communication, be it of citizens, enterprises or political leaders, is unacceptable.

Transfers of personal data are an important and necessary element of the transatlantic relationship. They form an integral part of commercial exchanges across the Atlantic including for new growing digital businesses, such as social media or cloud computing, with large amounts of data going from the EU to the US. They also constitute a crucial component of EU-US co-operation in the law enforcement field, and of the cooperation between Member States and the US in the field of national security. In order to facilitate data flows, while ensuring a high level of data protection as required under EU law, the US and the EU have put in place a series of agreements and arrangements.

Commercial exchanges are addressed by Decision 2000/520/EC² (hereafter “the Safe Harbour Decision”). This Decision provides a legal basis for transfers of personal data from the EU to companies established in the US which have adhered to the Safe Harbour Privacy Principles.

Exchange of personal data between the EU and the US for the purposes of law enforcement, including the prevention and combating of terrorism and other forms of serious crime, is governed by a number of agreements at EU level. These are the Mutual Legal Assistance Agreement³, the Agreement on the use and transfer of Passenger Name Records (PNR)⁴, the Agreement on the processing and transfer of Financial Messaging Data for the purpose of the Terrorist Finance Tracking Program (TFTP)⁵, and the Agreement between Europol and the US. These Agreements respond to important security challenges and meet the common security interests of the EU and US, whilst providing a high level of protection of personal data. In addition, the EU and the US are currently negotiating a framework agreement on data protection in the field of police and judicial cooperation (“umbrella agreement”)⁶. The aim is to ensure a high level of data protection for citizens whose data is exchanged thereby further

¹ For the purposes of this Communication, references to EU citizens include also non-EU data subjects which fall within the scope of European Union's data protection law.

² Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25.8.2000, p. 7.

³ Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 291, 7.11. 2009, p. 40.

⁴ Council Decision 2012/472/EU of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L215, 11.8.2012, p. 4.

⁵ Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195, 27.7.2010, p. 3.

⁶ The Council adopted the Decision authorising the Commission to negotiating the Agreement on 3 December 2010. See IP/10/1661 of 3 December 2010.

advancing EU-US cooperation in the combating of crime and terrorism on the basis of shared values and agreed safeguards.

These instruments operate in an environment in which personal data flows are acquiring increasing relevance.

On the one hand, the development of the digital economy has led to exponential growth in the quantity, quality, diversity and nature of data processing activities. The use of electronic communication services by citizens in their daily lives has increased. Personal data has become a highly valuable asset: the estimated value of EU citizens' data was €315bn in 2011 and has the potential to grow to nearly €1tn annually by 2020⁷. The market for the analysis of large sets of data is growing by 40% per year worldwide⁸. Similarly, technological developments, for example related to cloud computing, put into perspective the notion of international data transfer as cross-border data flows are becoming a day to day reality.⁹

The increase in the use of electronic communications and data processing services, including cloud computing, has also substantially expanded the scope and significance of transatlantic data transfers. Elements such as the central position of US companies in the digital economy¹⁰, the transatlantic routing of a large part of electronic communications and the volume of electronic data flows between the EU and the US have become even more relevant. On the other hand, modern methods of personal data processing raise new and important questions. This applies both to new means of large-scale processing of consumer data by private companies for commercial purposes, and to the increased ability of large-scale surveillance of communications data by intelligence agencies.

Large-scale US intelligence collection programmes, such as PRISM affect the fundamental rights of Europeans and, specifically, their right to privacy and to the protection of personal data. These programmes also point to a connection between Government surveillance and the processing of data by private companies, notably by US internet companies. As a result, they may therefore have an economic impact. If citizens are concerned about the large-scale processing of their personal data by private companies or by the surveillance of their data by intelligence agencies when using Internet services, this may affect their trust in the digital economy, with potential negative consequences on growth.

These developments expose EU-US data flows to new challenges. This Communication addresses these challenges. It explores the way forward on the basis of the findings contained in the Report of the EU Co-Chairs of the ad hoc EU-US Working Group and the Communication on the Safe Harbour.

It seeks to provide an effective way forward to rebuild trust and reinforce EU-US cooperation in these fields and strengthen the broader transatlantic relationship.

This Communication is based on the premise that the standard of protection of personal data must be addressed in its proper context, without affecting other dimensions of EU-US relations, including the on-going negotiations for a Transatlantic Trade and Investment Partnership. For this reason, data protection standards will not be negotiated within the Transatlantic Trade and Investment Partnership, which will fully respect the data protection rules.

⁷ See Boston Consulting Group, "The Value of our Digital Identity", November 2012.

⁸ See McKinsey, "Big data: The next frontier for innovation, competition, and productivity", 2011

⁹ Communication on Unleashing the potential of cloud computing in Europe, COM(2012) 529 final

¹⁰ For example, the combined number of unique visitors to Microsoft Hotmail, Google Gmail and Yahoo! Mail from European countries in June 2012 totalled over 227 million, eclipsing that of all other providers. The combined number of unique European users accessing Facebook and Facebook Mobile in March 2012 was 196.5 million, making Facebook the largest social network in Europe. Google is the leading internet search engine with 90.2% of worldwide internet users. US mobile messaging service What's App was used by 91% of iPhone users in Germany in June 2013.

It is important to note that whilst the EU can take action in areas of EU competence, in particular to safeguard the application of EU law¹¹, national security remains the sole responsibility of each Member State¹².

2. THE IMPACT ON THE INSTRUMENTS FOR DATA TRANSFERS

First, as regards data transferred for commercial purposes, the Safe Harbour has proven to be an important vehicle for EU-US data transfers. Its commercial importance has grown as personal data flows have taken on greater prominence in the transatlantic commercial relationship. Over the past 13 years, the Safe Harbour scheme has evolved to include more than 3.000 companies, over half of which have signed up within the last five years. Yet concerns about the level of protection of personal data of EU citizens transferred to the US under the Safe Harbour scheme have grown. The voluntary and declaratory nature of the scheme has sharpened focus on its transparency and enforcement. While a majority of US companies apply its principles, some self-certified companies do not. The non-compliance of some self-certified companies with the Safe Harbour Privacy Principles places such companies at a competitive advantage in relation to European companies operating in the same markets.

Moreover, while under the Safe Harbour, limitations to data protection rules are permitted where necessary on grounds of national security¹³, the question has arisen whether the large-scale collection and processing of personal information under US surveillance programmes is necessary and proportionate to meet the interests of national security. It is also clear from the findings of the ad hoc EU-US Working Group that, under these programmes, EU citizens do not enjoy the same rights and procedural safeguards as Americans.

The reach of these surveillance programmes, combined with the unequal treatment of EU citizens, brings into question the level of protection afforded by the Safe Harbour arrangement. The personal data of EU citizens sent to the US under the Safe Harbour may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the EU and the purposes for which it was transferred to the US. A majority of the US internet companies that appear to be more directly concerned by these programmes are certified under the Safe Harbour scheme.

Second, as regards exchanges of data for law enforcement purposes, the existing Agreements (PNR, TFTP) have proven highly valuable tools to address common security threats linked to serious transnational crime and terrorism, whilst laying down safeguards that ensure a high level of data protection¹⁴. These safeguards extend to EU citizens, and the Agreements provide for mechanisms to review their implementation and to address issues of concern related thereto. The TFTP Agreement also establishes a system of oversight, with EU independent overseers checking how data covered by the Agreement is searched by the US.

Against the backdrop of concerns raised in the EU about US surveillance programmes, the European Commission has used those mechanisms to check how the agreements are applied. In the case of the PNR Agreement, a joint review was conducted, involving data protection

¹¹ See Judgment of the Court of Justice of the European Union in Case C-300/11, ZZ v Secretary of State for the Home Department.

¹² Article 4(2) TEU.

¹³ See e.g. Safe Harbour Decision, Annex I.

¹⁴ See Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data pursuant to Article 6 (6) of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program.

experts from the EU and the US, looking at how the Agreement has been implemented¹⁵. That review did not give any indication that US surveillance programmes extend to or have impact on the passenger data covered by the PNR Agreement. In the case of the TFTP Agreement, the Commission opened formal consultations after allegations were made of US intelligence agencies directly accessing personal data in the EU, contrary to the Agreement. These consultations did not reveal any elements proving a breach of the TFTP Agreement, and they led the US to provide written assurance that no direct data collection has taken place contrary to the provisions of the Agreement.

The large-scale collection and processing of personal information under US surveillance programmes call, however, for a continuation of very close monitoring of the implementation of the PNR and TFTP Agreements in the future. The EU and the US have therefore agreed to advance the next Joint Review of the TFTP Agreement, which will be held in Spring 2014. Within that and future joint reviews, greater transparency will be ensured on how the system of oversight operates and on how it protects the data of EU citizens. In parallel, steps will be taken to ensure that the system of oversight continues to pay close attention to how data transferred to the US under the Agreement is processed, with a focus on how such data is shared between US authorities.

Third, the increase in the volume of processing of personal data underlines the importance of the legal and administrative safeguards that apply. One of the goals of the Ad Hoc EU-US Working Group was to establish what safeguards apply to minimise the impact of the processing on the fundamental rights of EU citizens. Safeguards are also necessary to protect companies. Certain US laws such as the Patriot Act, enable US authorities to directly request companies access to data stored in the EU. Therefore, European companies, and US companies present in the EU, may be required to transfer data to the US in breach of EU and Member States' laws, and are consequently caught between conflicting legal obligations. Legal uncertainty deriving from such direct requests may hold back the development of new digital services, such as cloud computing, which can provide efficient, lower-cost solutions for individuals and businesses.

3. ENSURING THE EFFECTIVENESS OF DATA PROTECTION

Transfers of personal data between the EU and the US are an essential component of the transatlantic commercial relationship. Information sharing is also an essential component of EU-US security cooperation, critically important to the common goal of preventing and combating serious crime and terrorism. However, recent revelations about US intelligence collection programmes have negatively affected the trust on which this cooperation is based. In particular, it has affected trust in the way personal data is processed. The following steps should be taken to restore trust in data transfers for the benefit of the digital economy, security both in the EU and in the US, and the broader transatlantic relationship.

3.1. The EU data protection reform

The data protection reform proposed by the Commission in January 2012¹⁶ provides a key response as regards the protection of personal data. Five components of the proposed Data Protection package are of particular importance.

¹⁵ See on the Commission report "Joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security".

¹⁶ COM(2012) 10 final: Proposal for a Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25.1.2012, and COM(2012) 11 final: Proposal for a Regulation of the European Parliament and the Council on the protection of individuals

First, as regards territorial scope, the proposed regulation makes clear that companies that are not established in the Union will have to apply EU data protection law when they offer goods and services to European consumers or monitor their behaviour. In other words, the fundamental right to data protection will be respected, independently of the geographical location of a company or of its processing facility¹⁷.

Secondly, on international transfers, the proposed regulation establishes the conditions under which data can be transferred outside the EU. Transfers can only be allowed where these conditions, which safeguard the individuals' rights to a high level of protection, are met¹⁸.

Thirdly, concerning enforcement, the proposed rules provide for proportionate and dissuasive sanctions (up to 2% of a company's annual global turnover) to make sure that companies comply with EU law¹⁹. The existence of credible sanctions will increase companies' incentive to comply with EU law.

Fourthly, the proposed regulation includes clear rules on the obligations and liabilities of data processors such as cloud providers, including on security²⁰. As the revelations about US intelligence collection programmes have shown, this is critical because these programmes affect data stored in the cloud. Also, companies providing storage space in the cloud which are asked to provide personal data to foreign authorities will not be able to escape their responsibility by reference to their status as data processors rather than data controllers.

Fifth, the package will lead to the establishment of comprehensive rules for the protection of personal data processed in the law enforcement sector.

It is expected that the package will be agreed upon in a timely manner in the course of 2014²¹.

3.2. Making Safe Harbour safer

The Safe Harbour scheme is an important component of the EU-US commercial relationship, relied upon by companies on both sides of the Atlantic.

The Commission's report on the functioning of Safe Harbour has identified a number of weaknesses in the scheme. As a result of a lack of transparency and of enforcement, some self-certified Safe Harbour members do not, in practice, comply with its principles. This has a negative impact on EU citizens' fundamental rights. It also creates a disadvantage for European companies compared to those competing US companies that are operating under the scheme but in practice not applying its principles. This weakness also affects the majority of US companies which properly apply the scheme. Safe Harbour also acts as a conduit for the

with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

¹⁷ The Commission takes note that the European Parliament confirmed and strengthened this important principle, enshrined in Art. 3 of the proposed Regulation, in its vote of 21 October 2013 on the data protection reform reports of MEPs Jan-Philipp Albrecht and Dimitrios Droutsas in the Committee for Civil Liberties, Justice and Home Affairs (LIBE).

¹⁸ The Commission takes note that in its vote of 21 October 2013, the LIBE Committee of the European Parliament proposed to include a provision in the future Regulation that would subject requests from foreign authorities to access personal data collected in the EU to the obtaining of a prior authorisation from a national data protection authority, where such a request would be issued outside a mutual legal assistance treaty or another international agreement.

¹⁹ The Commission takes note that in its vote of 21 October 2013, the LIBE Committee proposed strengthening the Commission's proposal by providing that fines can go up to 5% of the annual worldwide turnover of a company.

²⁰ The Commission takes note that in its vote of 21 October 2013, the LIBE Committee endorsed the strengthening of the obligations and liabilities of data processors, in the particular with regard to Art. 26 of the proposed Regulation.

²¹ The Conclusions of the October 2013 European Council state that: "It is important to foster the trust of citizens and businesses in the digital economy. The timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015".

transfer of the personal data of EU citizens from the EU to the US by companies required to surrender data to US intelligence agencies under the US intelligence collection programmes. Unless the deficiencies are corrected, it therefore constitutes a competitive disadvantage for EU business and has a negative impact on the fundamental right to data protection of EU citizens.

The shortcomings of the Safe Harbour scheme have been underlined by the response of European Data Protection Authorities to the recent surveillance revelations. Article 3 of the Safe Harbour Decision authorises these authorities to suspend, under certain conditions, data flows to certified companies.²² German data protection commissioners have decided not to issue new permissions for data transfers to non-EU countries (for example for the use of certain cloud services). They will also examine whether data transfers on the basis of the Safe Harbour should be suspended.²³ The risk is that such measures, taken at national level, would create differences in coverage, which means that Safe Harbour would cease to be a core mechanism for the transfer of personal data between the EU and the US.

The Commission has the authority under Directive 95/46/EC to suspend or revoke the Safe Harbour decision if the scheme no longer provides an adequate level of protection. Furthermore, Article 3 of the Safe Harbour Decision provides that the Commission may reverse, suspend or limit the scope of the decision, while, under article 4, it may adapt the decision at any time in the light of experience with its implementation.

Against this background, a number of policy options can be considered, including:

- Maintaining the *status quo*;
- Strengthening the Safe Harbour scheme and reviewing its functioning thoroughly;
- Suspending or revoking the Safe Harbour decision.

Given the weaknesses identified, the current implementation of Safe Harbour cannot be maintained. However, its revocation would adversely affect the interests of member companies in the EU and in the US. The Commission considers that Safe Harbour should rather be strengthened.

The improvements should address both the structural shortcomings related to transparency and enforcement, the substantive Safe Harbour principles and the operation of the national security exception.

More specifically, for Safe Harbour to work as intended, the monitoring and supervision by US authorities of the compliance of certified companies with the Safe Harbour Privacy Principles needs to be more effective and systematic. The transparency of certified companies' privacy policies needs to be improved. The availability and affordability of dispute resolution mechanisms also needs to be ensured to EU citizens.

As a matter of urgency, the Commission will engage with the US authorities to discuss the shortcomings identified. Remedies should be identified by summer 2014 and implemented as soon as possible. On the basis thereof, the Commission will undertake a complete stock taking of the functioning of the Safe Harbour. This broader review process should involve open consultation and a debate in the European Parliament and the Council as well as discussions with the US authorities.

²² Specifically, pursuant to Art. 3 of the Safe Harbour Decision, such suspensions may take place in cases where there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

²³ Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, press release of 24 July 2013.

It is also important that the national security exception foreseen by the Safe Harbour Decision, is used only to an extent that is strictly necessary and proportionate.

3.3. Strengthening data protection safeguards in law enforcement cooperation

The EU and the US are currently negotiating a data protection “umbrella” agreement on transfers and processing of personal information in the context of police and judicial cooperation in criminal matters. The conclusion of such an agreement providing for a high level of protection of personal data would represent a major contribution to strengthening trust across the Atlantic. By advancing the protection of EU data citizens' rights, it would help strengthen transatlantic cooperation aimed at preventing and combating crime and terrorism.

According to the decision authorising the Commission to negotiate the umbrella agreement, the aim of the negotiations should be to ensure a high level of protection in line with the EU data protection *acquis*. This should be reflected in agreed rules and safeguards on, *inter alia*, purpose limitation, the conditions and the duration of the retention of data. In the context of the negotiation, the Commission should also obtain commitments on enforceable rights including judicial redress mechanisms for EU citizens not resident in the US²⁴. Close EU-US cooperation to address common security challenges should be mirrored by efforts to ensure that citizens benefit from the same rights when the same data is processed for the same purposes on both sides of the Atlantic. It is also important that derogations based on national security needs are narrowly defined. Safeguards and limitations should be agreed in this respect.

These negotiations provide an opportunity to clarify that personal data held by private companies and located in the EU will not be directly accessed by or transferred to US law enforcement authorities outside of formal channels of co-operation, such as Mutual Legal Assistance agreements or sectoral EU-US Agreements authorising such transfers. Access by other means should be excluded, unless it takes place in clearly defined, exceptional and judicially reviewable situations. The US should undertake commitments in that regard²⁵.

An “umbrella agreement” agreed along those lines, should provide the general framework to ensure a high level of protection of personal data when transferred to the US for the purpose of preventing or combating crime and terrorism. Sectoral agreements should, where necessary due to the nature of the data transfer concerned, lay down additional rules and safeguards, building on the example of the EU-US PNR and TFTP Agreements, which set strict conditions for transfer of data and safeguards for EU citizens.

²⁴ See the relevant passage of the Joint Press Statement following the EU-US-Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington: “We are therefore, as a matter of urgency, committed to advancing rapidly in the negotiations on a meaningful and comprehensive data protection umbrella agreement in the field of law enforcement. The agreement would act as a basis to facilitate transfers of data in the context of police and judicial cooperation in criminal matters by ensuring a high level of personal data protection for U.S. and EU citizens. We are committed to working to resolve the remaining issues raised by both sides, including judicial redress (a critical issue for the EU). Our aim is to complete the negotiations on the agreement ahead of summer 2014.”

²⁵ See the relevant passage of the Joint Press Statement following the EU-US Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington: “We also underline the value of the EU-U.S. Mutual Legal Assistance Agreement. We reiterate our commitment to ensure that it is used broadly and effectively for evidence purposes in criminal proceedings. There were also discussions on the need to clarify that personal data held by private entities in the territory of the other party will not be accessed by law enforcement agencies outside of legally authorized channels. We also agree to review the functioning of the Mutual Legal Assistance Agreement, as contemplated in the Agreement, and to consult each other whenever needed.”

3.4. Addressing European concerns in the on-going US reform process

US President Obama has announced a review of US national security authorities' activities, including of the applicable legal framework. This on-going process provides an important opportunity to address EU concerns raised by recent revelations about US intelligence collection programmes. The most important changes would be extending the safeguards available to US citizens and residents to EU citizens not resident in the US, increased transparency of intelligence activities, and further strengthening oversight. Such changes would restore trust in EU-US data exchanges, and promote the use of Internet services by Europeans.

With respect to extending the safeguards available to US citizens and residents to EU citizens, legal standards in relation to US surveillance programmes which treat US and EU citizens differently should be reviewed, including from the perspective of necessity and proportionality, keeping in mind the close transatlantic security partnership based on common values, rights and freedoms. This would reduce the extent to which Europeans are affected by US intelligence collection programmes.

More transparency is needed on the legal framework of US intelligence collection programmes and its interpretation by US Courts as well as on the quantitative dimension of US intelligence collection programmes. EU citizens would also benefit from such changes.

The oversight of US intelligence collection programmes would be improved by strengthening the role of the Foreign Intelligence Surveillance Court and by introducing remedies for individuals. These mechanisms could reduce the processing of personal data of Europeans that are not relevant for national security purposes.

3.5. Promoting privacy standards internationally

Issues raised by modern methods of data protection are not limited to data transfer between the EU and the US. A high level of protection of personal data should also be guaranteed to any individual. EU rules on collection, processing and transfer of data should be promoted internationally.

Recently, a number of initiatives have been proposed to promote the protection of privacy, particularly on the internet²⁶. The EU should ensure that such initiatives, if pursued, fully take into account the principles of protecting fundamental rights, freedom of expression, personal data and privacy as set out in EU law and in the EU Cyber Security Strategy, and do not undermine the freedom, openness and security of cyber space. This includes a democratic and efficient multi stakeholder governance model.

The on-going reforms of data protection laws on both sides of the Atlantic also provide the EU and the US a unique opportunity to set the standard internationally. Data exchanges across the Atlantic and beyond would greatly benefit from the strengthening of the US domestic legal framework, including the passage of the "Consumer Privacy Bill of Rights" announced by President Obama in February 2012 as part of a comprehensive blueprint to improve consumers' privacy protections. The existence of a set of strong and enforceable data protection rules enshrined in both the EU and the US would constitute a solid basis for cross-border data flows.

In view of promoting privacy standards internationally, accession to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), which is open to countries which are not member of the Council of Europe²⁷, should also be favoured. Safeguards and guarantees agreed in international fora should result in a high level of protection compatible with what is required under EU law.

²⁶ See in this respect the draft resolution proposed to the UN General Assembly by Germany and Brazil – calling for the protection of privacy online as offline.

²⁷ The US is already party to another Council of Europe convention: the 2001 Convention on Cybercrime (also known as the "Budapest Convention").

4. CONCLUSIONS AND RECOMMENDATIONS

The issues identified in this Communication require action to be taken by the US as well as by the EU and its Member States.

The concerns around transatlantic data exchanges are, first of all, a wake-up call for the EU and its Member States to advance swiftly and with ambition on the data protection reform. It shows that a strong legislative framework with clear rules that are enforceable also in situations when data are transferred abroad is, more than ever, a necessity. The EU institutions should therefore continue working towards the adoption of the EU data protection reform by spring 2014, to make sure that personal data is effectively and comprehensively protected.

Given the significance of transatlantic data flows, it is essential that the instruments on which these exchanges are based appropriately address the challenges and opportunities of the digital era and new technological developments like cloud computing. Existing and future arrangements and agreements should ensure that the continuity of a high level of protection is guaranteed over the Atlantic.

A robust Safe Harbour scheme is in the interests of EU and US citizens and companies. It should be strengthened by better monitoring and implementation in the short term, and, on this basis, by a broader review of its functioning. Improvements are necessary to ensure that the original objectives of the Safe Harbour Decision – i.e. continuity of data protection, legal certainty and free EU-US flow of data – are still met.

These improvements should focus on the need for the US authorities to better supervise and monitor the compliance of self-certified companies with the Safe Harbour Privacy Principles. It is also important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary and proportionate.

In the area of law enforcement, the current negotiations of an “umbrella agreement” should result in a high level of protection for citizens on both sides of the Atlantic. Such an agreement would strengthen the trust of Europeans in EU-US data exchanges, and provide a basis to further develop EU-US security cooperation and partnership. In the context of the negotiation, commitments should be secured to the effect that procedural safeguards, including judicial redress, are available to Europeans who are not resident in the US.

Commitments should be sought from the US administration to ensure that personal data held by private entities in the EU will not be accessed directly by US law enforcement agencies outside of formal channels of co-operation, such as Mutual Legal Assistance agreements and sectoral EU-US Agreements such as PNR and TFTP authorising such transfers under strict conditions, except in clearly defined, exceptional and judicially reviewable situations.

The US should also extend the safeguards available to US citizens and residents to EU citizens not resident in the US, ensure the necessity and proportionality of the programmes, greater transparency and oversight in the legal framework applicable to US national security authorities.

Areas listed in this communication will require constructive engagement from both sides of the Atlantic. Together, as strategic partners, the EU and the US have the ability to overcome the current tensions in the transatlantic relationship and rebuild trust in EU-US data flows. Undertaking joint political and legal commitments on further cooperation in these areas will strengthen the overall transatlantic relationship.

Dokument 2014/0033239

Von: Spitzer, Patrick, Dr.
Gesendet: Mittwoch, 22. Januar 2014 11:58
An: RegOeSI3
Betreff: Bitte verakten



AWA: FINE: 22.01., WER: spitzer AWA: FINE: 22.01., WER: spitzer
10:00Uhr: A... 22.01., 10:00Uhr: A... 10:00Uhr: A... 10:00Uhr: A...

zVg. ÖS I 3 – 52000/4#1 (ich hoffe, damit liege ich richtig)

Freundliche Grüße

Patrick Spitzer

Von: IT1_
Gesendet: Mittwoch, 22. Januar 2014 11:15
An: Spitzer, Patrick, Dr.
Cc: OESI3AG_
Betreff: AW: Frist 22.01., 11:00 Uhr: Anforderung eines Berichtsbogens zur Unterrichtung des Deutschen Bundestages (17067/13)

IT 1-17000/17#16

Für IT 1 mitgezeichnet.

Grüße
Lars Mammen

Von: Spitzer, Patrick, Dr.
Gesendet: Dienstag, 21. Januar 2014 18:39
An: VI4_; PGDS_; IT1_; OESII1_; OESIII1_
Cc: RegOeSI3; OESI3AG_; Weinbrenner, Ulrich; Taube, Matthias; Stöber, Karlheinz, Dr.; PGNSA; Bender, Ulrike; Schlender, Katharina; Mammen, Lars, Dr.; Papenkort, Katja, Dr.; Marscholleck, Dietmar; B3_; Wenske, Martina
Betreff: Frist 22.01., 11:00 Uhr: Anforderung eines Berichtsbogens zur Unterrichtung des Deutschen Bundestages (17067/13)
Wichtigkeit: Hoch

ÖS I 3 – 52001/3#2

< Datei: 140121_Berichtsb_Rebuilding Trust.doc >> < Datei: 17067.EN13.pdf >>
Liebe Kolleginnen und Kollegen,

ich bitte um Mitzeichnung zum als Anlage 1 beigefügten Berichtsbogen zur Unterrichtung des Deutschen Bundestages **bis morgen, 22. Januar 2014, 11.00 Uhr**. Grundlage der Berichterstattung ist das als Anlage 2 beigefügte Dokument „Rebuilding Trust in EU US Data Flows“.

Freundliche Grüße

Patrick Spitzer

im Auftrag
Dr. Patrick Spitzer

Bundesministerium des Innern
Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,
BKA-Gesetz, Datenschutz im Sicherheitsbereich)
Alt-Moabit 101D, 10559 Berlin
Telefon: +49 (0)30 18681-1390
E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helpen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

Von: Bender, Ulrike
Gesendet: Mittwoch, 22. Januar 2014 10:11
An: Spitzer, Patrick, Dr.
Cc: VI4_; PGDS_; IT1_; OESII1_; OESIII1_; Merz, Jürgen
Betreff: WG: sg Frist 22.01., 11:00 Uhr: Anforderung eines Berichtsbogens zur Unterrichtung des Deutschen Bundestages (17067/13)

Wichtigkeit: Hoch

Lieber Herr Spitzer,

anbei die Anmerkungen von VI4, mit diesen mitgezeichnet. Für Rückfragen stehe ich Ihnen gerne zur Verfügung.



~~Zu Persönliche Postfach~~
 Th...

Mit freundlichen Grüßen
 Ulrike Bender

Von: Spitzer, Patrick, Dr.
Gesendet: Dienstag, 21. Januar 2014 18:39
An: VI4_; PGDS_; IT1_; OESII1_; OESIII1_
Cc: RegOeSI3; OESI3AG_; Weinbrenner, Ulrich; Taube, Matthias; Stöber, Karlheinz, Dr.; PGNSA; Bender, Ulrike; Schlender, Katharina; Mammen, Lars, Dr.; Papenkort, Katja, Dr.; Marscholleck, Dietmar; B3_; Wenske, Martina
Betreff: sg Frist 22.01., 11:00 Uhr: Anforderung eines Berichtsbogens zur Unterrichtung des Deutschen Bundestages (17067/13)
Wichtigkeit: Hoch

ÖS I 3 – 52001/3#2

Liebe Kolleginnen und Kollegen,

ich bitte um Mitzeichnung zum als Anlage 1 beigefügten Berichtsbogen zur Unterrichtung des Deutschen Bundestages **bis morgen, 22. Januar 2014, 11.00 Uhr**. Grundlage der Berichterstattung ist das als Anlage 2 beigefügte Dokument „Rebuilding Trust in EU US Data Flows“.

Freundliche Grüße

Patrick Spitzer

im Auftrag
 Dr. Patrick Spitzer

Bundesministerium des Innern

Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,
BKA-Gesetz, Datenschutz im Sicherheitsbereich)

Alt-Moabit 101D, 10559 Berlin

Telefon: +49 (0)30 18681-1390

E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

Anhang von WG sg Frist 22.01. 1100 Uhr Anforderung
eines Berichtsbogens zur Unterrichtung des Deutschen
Bundestages (1706713).msg

1. 140121_Berichtsb_Rebuilding Trust.doc

5 Seiten

BERICHTSBOGEN

gemäß Anlage zu § 6 Absatz 2 EUZBBG und Ziffer II. 3. der Anlage zu § 9 EUZBLG

Ressort/Referat:	AG ÖS I 3	Datum:	20.01.2014
Referatsleiterin/ Referatsleiter:	MinR Weinbrenner MinR Taube	Telefon:	030 186811300
Bearbeiterin/ Bearbeiter:	RR Dr. Spitzer	Telefon:	030 186811390
abgestimmt mit:	BMJV; BMWi, AA	Telefax:	

Thema:	Mitteilung der Kommission an das Europäische Parlament und den Rat über die Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA
Sachgebiet:	Europäische Justiz- und Innenpolitik
Ratsdok.-Nummer:	17067/13
KOM-Nummer:	COM(2013) 846 final
Nummer des interinstitutionellen Dossiers:	nicht bekannt
Nummer der Bundesratsdrucksache:	nicht bekannt
Nachweis der Zulässigkeit für europäische Regelungen: (Prüfung der Rechtsgrundlage)	entfällt, da kein Rechtsakt
Subsidiaritätsprüfung:	entfällt, da kein Rechtsakt
Verhältnismäßigkeitsprüfung:	entfällt, da kein Rechtsakt
Zielsetzung:	Ausarbeitung von Maßnahmen zur Berücksichtigung beim Datenaustausch zwischen den USA und der EU vor dem Hintergrund der Veröffentlichungen zur Überwachungstätigkeit der NSA.
Inhaltliche Schwerpunkte:	Die Mitteilung ist ein politisches Strategiepapier über die transatlantischen Datenströme, in dem die sich aus den Enthüllungen über die umfangreichen Programme der US-Nachrichtendienste zur Sammlung von Informationen ergebenden Herausforderungen und Risiken <u>aus Sicht der KOM</u> beschrieben und die <u>nach Auffassung der KOM</u> erforderlichen Maßnahmen zur Ausräumung der genannten

- 2 -

Bedenken dargelegt werden. Das Papier fasst verschiedene weitere Veröffentlichungen der EU zu Einzelthemen, wie die Analyse über die Funktionsweise des „Safe Harbour Abkommens“ und den Bericht über das TFTP-Abkommen (auch SWIFT-Abkommen genannt), zusammen.

Folgende Maßnahmen werden von der KOM aufgegriffen:

Datenschutzreformpaket

KOM sieht ~~ist~~ das von ihr Anfang 2012 vorgeschlagene Datenschutzreformpaket als ein Schlüsselement in Bezug auf den Schutz personenbezogener Daten an. Als Begründung werden fünf Elemente, die aus ihrer Sicht insoweit entscheidend sind, angeführt: das Marktortprinzip, Regelungen zu Drittstaatenübermittlungen, Sanktionen, Regelungen zu Verantwortlichkeiten und die Regelungen im Bereich Polizei und Justiz.

Verbesserung von Safe Harbour

KOM identifiziert als Schwachstellen der Safe-Harbor-Regelung Defizite bei der Transparenz und der Durchsetzung der Vereinbarung (insbesondere Inhalt und Veröffentlichung der Datenschutzerklärung der Safe-Harbor-registrierten Unternehmen, Verfügbarkeit alternativer Konfliktlösungsmechanismen für EU-Bürger, Durchsetzung durch die zuständigen US-Behörden, Zugang zu den Daten durch US-Sicherheitsbehörden) und gibt Empfehlungen zur verbesserten Umsetzung von Safe Harbor ab. Darüber hinaus kündigt KOM Gespräche mit den US-Behörden an, die der Identifizierung von Schwachstellen und deren Abhilfe bis Sommer 2014 dienen sollen.

Abschluss eines EU-US Datenschutzabkommens

KOM strebt den Abschluss eines Rahmenabkommens zum Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen an. Ein solches Abkommen solle den Rahmen für eine möglichst hohes Datenschutzniveau vorgeben und u.a. auch für einen effektiven Rechtsschutz für EU-Bürger außerhalb der USA geben und ggf. durch fachspezifische Einzelabkommen, wie das EU-US PNR- und das TFTP- Abkommen ergänzt werden.

Berücksichtigung von EU-Interessen im laufenden US-Reformprozess

Die von US-Präsident Obama initiierte Evaluierung der US-Sicherheitsbehörden soll genutzt werden, um eine Anhebung der Standards für EU-Bürger zu erreichen. Der Bericht spricht u.a. die Ungleichbehandlung von US- und EU-Bürgern, unterschiedliche Auffassungen über die Auslegung des Verhältnismäßigkeitsgrundsatzes und die mangelnden Rechtsschutzmöglichkeiten für EU-Bürger in den USA als zentrale Punkte an.

Kommentar [MJ1]: einheitliche Schreibweise wahren: mit/ohne u

Kommentar [MJ2]: m.E. müsste vor Identifizierung „gemeinsamen“ oder vor Schwachstellen „weiteren“ eingefügt werden+

- 3 -

Politische Bedeutung:	Die politische Bedeutung ist nicht zuletzt vor dem Hintergrund der <u>andauernden Veröffentlichungen zu Aktivitäten amerikanischer Nachrichtendienste und der öffentlichen Diskussion in DEU und auf internationaler Ebene mit als hoch zu bewerten.</u>
Was ist das besondere deutsche Interesse?	<p>Aufgrund der unmittelbaren Betroffenheit Deutschlands durch die Veröffentlichungen Edward Snowdens besteht an allen diesbezüglichen Maßnahmen/Empfehlungen grundsätzlich ein besonderes Interesse. <u>Generell ist dabei zu beachten, dass die EU zwar eine Kompetenz für den Datenschutz, nicht jedoch für die Tätigkeit der Nachrichtendienste hat.</u> Im Einzelnen:</p> <p><u>Datenschutzreformpaket</u></p> <p>Der dargestellte Zusammenhang zwischen den Überwachungsmaßnahmen und der Datenschutz-Grundverordnung (DSGVO) vermag nur teilweise zu überzeugen. Zutreffend ist, dass das Marktortprinzip zu einer Verbesserung des Datenschutzes im transatlantischen Verhältnis beitragen dürfte, weil US-Unternehmen in Europa unmittelbar an EU-Recht gebunden werden können. Bei den Drittstaatenregelungen ist zu differenzieren. Allgemein dürften die von der KOM vorgeschlagenen Regelungen kaum zu einer Verbesserung führen. Dies gilt insbesondere für Übermittlungen von Unternehmen an US-Behörden. Hierzu hatte DEU einen neuen Art. 42a vorgeschlagen. Die bisher formulierten Anforderungen an die Übermittlung personenbezogener Daten in Drittstaaten werden auch der technischen Entwicklung und Vernetzung noch nicht gerecht. Entgegen den Behauptungen der KOM bleiben insbesondere zentrale Fragen der Übermittlung, z.B. beim „Cloud computing“, ungelöst. Zu begrüßen ist, dass die KOM Ideen der US-Seite aufgegriffen hat, die das Weiße Haus in seinem Papier „Consumer Data Privacy in a Networked World („Consumer Bill of Rights“) im Februar 2012 entwickelt hat. Allerdings lässt KOM offen, wie sich diese Ideen in die DSGVO inkorporieren lassen.</p> <p><u>Safe Harbour</u></p> <p>Die Bundesregierung hat sich wiederholt für eine Verbesserung der Safe-Harbor-Regelung ausgesprochen, die schnellstmögliche Vorlage des KOM-Berichts zu Safe Harbor gefordert und drängt in der EU auf Nachverhandlungen des Safe-Harbor-Abkommens. Sie unterstützt die Vorschläge der KOM zur Verbesserung von Safe Harbor. Darüber hinaus setzt sie sich dafür ein, für Modelle wie Safe Harbor in der europäischen Datenschutz-Grundverordnung einen robusten Rechtsrahmen mit klaren Vorgaben für Garantien der Bürgerinnen und Bürger zu schaffen und hat bereits einen entsprechenden Vorschlag in die Verhandlungen in der Ratsarbeitsgruppe DAPIX eingebracht. Ziel ist es, die Individualrechte der Bürgerinnen und Bürger zu</p>

- 4 -

	<p>stärken und ihnen bessere Rechtsschutzmöglichkeiten zur Verfügung zu stellen, die Registrierung der Unternehmen in der EU vorzunehmen und die staatliche Kontrolle seitens der EU-Datenschutzaufsichtsbehörden in Modellen wie Safe-Harbor zu stärken.</p> <p><u>EU-US-Datenschutzabkommen</u></p> <p>Deutschland hat sich für einen baldigen Abschluss des Abkommens unter der Voraussetzung, dass damit mit Blick auf den Schutz personenbezogener Daten und den Individualrechtsschutz ein wirklicher Mehrwert geschaffen wird, ausgesprochen.</p> <p>Bislang haben sich die Verhandlungen schwierig gestaltet. In wichtigen Punkten herrscht weiterhin keine Einigung, so bei der Speicherdauer, der unabhängigen Aufsicht, den Individualrechten und dem Rechtsschutz. Auch wollen die USA weiterhin das Abkommen als sog. „executive agreement“ abschließen; ein solches kann US-Recht nicht abändern. Bei EU/US Justice and Home Affairs Ministerial Treffen am 18.11.2013 haben beide Seiten das Ziel bekräftigt, die Verhandlungen bis zum Sommer 2014 abzuschließen.</p> <p><u>Berücksichtigung von EU-Interessen im laufenden US-Reformprozess</u></p> <p>Deutschland hat sich auch auf EU-Ebene in den Prozess zur Aufklärung des Sachverhalts im Zusammenhang mit den Veröffentlichungen von Edward Snowden und zur Erarbeitung konkreter Empfehlungen der EU und der MS zur Berücksichtigung in der laufenden US-internen Evaluierung der Überwachungsprogramme intensiv eingebracht. Ein entsprechendes Dokument mit Vorschlägen zur Anwendung des Verhältnismäßigkeitsprinzips, zum verbesserten Individualrechtsschutz und zur Gleichstellung von EU- und US-Bürgern wurde am 6. Dezember 2013 im Rahmen des JI-Ministertreffens in Brüssel verabschiedet.</p>
bisherige Position des Deutschen Bundestages:	nicht bekannt
Position des Bundesrates:	nicht bekannt
Position des Europäischen Parlaments:	nicht bekannt
Meinungsstand im Rat:	nicht bekannt
Verfahrensstand: (Stand der Befassung)	
Finanzielle Auswirkungen:	

Kommentar [B3]: Was für ein Dokument? War ein DEU Entwurf die Grundlage? Wurde dies von den JI-Ministern verabschiedet?

Kommentar [MJ4]: Formulierung sollte vermieden werden. Falls der Rat bislang nicht befasst war, sollte dies explizit gesagt werden.

- 5 -

Zeitplan für die Behandlung im

a) Bundesrat:	nicht bekannt
b) Europäischen Parlament:	nicht bekannt
c) Rat:	nicht bekannt

Von: Schlender, Katharina
Gesendet: Mittwoch, 22. Januar 2014 08:42
An: Spitzer, Patrick, Dr.
Cc: OESI3AG_; PGDS_
Betreff: AW: Frist 22.01., 11:00 Uhr: Anforderung eines Berichtsbogens zur Unterrichtung des Deutschen Bundestages (17067/13)

Für PGDS mitgezeichnet.

Mit freundlichen Grüßen
Im Auftrag

Katharina Schlender

Projektgruppe Reform des Datenschutzes
in Deutschland und Europa

Bundesministerium des Innern
Fehrbelliner Platz 3, 10707 Berlin
DEUTSCHLAND

Telefon: +49 30 18681 45559
E-Mail: Katharina.Schlender@bmi.bund.de

Von: Spitzer, Patrick, Dr.
Gesendet: Dienstag, 21. Januar 2014 18:39
An: VI4_; PGDS_; IT1_; OESII1_; OESIII1_
Cc: RegOeSI3; OESI3AG_; Weinbrenner, Ulrich; Taube, Matthias; Stöber, Karlheinz, Dr.; PGNSA; Bender, Ulrike; Schlender, Katharina; Mammen, Lars, Dr.; Papenkort, Katja, Dr.; Marscholleck, Dietmar; B3_; Wenske, Martina
Betreff: Frist 22.01., 11:00 Uhr: Anforderung eines Berichtsbogens zur Unterrichtung des Deutschen Bundestages (17067/13)
Wichtigkeit: Hoch

ÖS I 3 – 52001/3#2

< Datei: 140121_Berichtsb_Rebuilding Trust.doc >> < Datei: 17067.EN13.pdf >>
Liebe Kolleginnen und Kollegen,

ich bitte um Mitzeichnung zum als Anlage 1 beigefügten Berichtsbogen zur Unterrichtung des Deutschen Bundestages **bis morgen, 22. Januar 2014, 11.00 Uhr**. Grundlage der Berichterstattung ist das als Anlage 2 beigefügte Dokument „Rebuilding Trust in EU US Data Flows“.

Freundliche Grüße

Patrick Spitzer

im Auftrag
Dr. Patrick Spitzer

Bundesministerium des Innern
Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,
BKA-Gesetz, Datenschutz im Sicherheitsbereich)
Alt-Moabit 101D, 10559 Berlin
Telefon: +49 (0)30 18681-1390
E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

Von: OESIII1_
Gesendet: Dienstag, 21. Januar 2014 19:09
An: OESI3AG_; Spitzer, Patrick, Dr.
Cc: OESIII1_; Werner, Wolfgang; Menzel, Maja
Betreff: WG: Frist 22.01., 11:00 Uhr: Anforderung eines Berichtsbogens zur Unterrichtung des Deutschen Bundestages (17067/13)

Wichtigkeit: Hoch

Mitgezeichnet (kleine Formulierungsanregung anbei).

Mit freundlichen Grüßen
 Dietmar Marscholleck
 Bundesministerium des Innern, Referat ÖS III 1
 Telefon: (030) 18 681-1952
 Mobil: 0175 574 7486
 e-mail: OESIII1@bmi.bund.de

Von: Spitzer, Patrick, Dr.
Gesendet: Dienstag, 21. Januar 2014 18:39
An: VI4_; PGDS_; IT1_; OESII1_; OESIII1_
Cc: RegOeSI3; OESI3AG_; Weinbrenner, Ulrich; Taube, Matthias; Stöber, Karlheinz, Dr.; PGNSA; Bender, Ulrike; Schlender, Katharina; Mammen, Lars, Dr.; Papenkort, Katja, Dr.; Marscholleck, Dietmar; B3_; Wenske, Martina
Betreff: Frist 22.01., 11:00 Uhr: Anforderung eines Berichtsbogens zur Unterrichtung des Deutschen Bundestages (17067/13)
Wichtigkeit: Hoch

ÖS I 3 – 52001/3#2



~~21_Personlich_Protokoll_17067_13.pdf~~

Liebe Kolleginnen und Kollegen,

ich bitte um Mitzeichnung zum als Anlage 1 beigefügten Berichtsbogen zur Unterrichtung des Deutschen Bundestages **bis morgen, 22. Januar 2014, 11.00 Uhr**. Grundlage der Berichterstattung ist das als Anlage 2 beigefügte Dokument „Rebuilding Trust in EU US Data Flows“.

Freundliche Grüße

Patrick Spitzer

im Auftrag

Dr. Patrick Spitzer

Bundesministerium des Innern
Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,
BKA-Gesetz, Datenschutz im Sicherheitsbereich)
Alt-Moabit 101D, 10559 Berlin
Telefon: +49 (0)30 18681-1390
E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

B E R I C H T S B O G E N

gemäß Anlage zu § 6 Absatz 2 EUZBBG und Ziffer II. 3. der Anlage zu § 9 EUZBLG

Ressort/Referat:	AG ÖS I 3	Datum:	20.01.2014
Referatsleiterin/ Referatsleiter:	MinR Weinbrenner MinR Taube	Telefon:	030 186811300
Bearbeiterin/ Bearbeiter:	RR Dr. Spitzer	Telefon:	030 186811390
abgestimmt mit:	BMJV; BMWi, AA	Telefax:	

Thema:	Mitteilung der Kommission an das Europäische Parlament und den Rat über die Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA
Sachgebiet:	Europäische Justiz- und Innenpolitik
Ratsdok.-Nummer:	17067/13
KOM-Nummer:	COM(2013) 846 final
Nummer des interinstitutionellen Dossiers:	nicht bekannt
Nummer der Bundesratsdrucksache:	nicht bekannt
Nachweis der Zulässigkeit für europäische Regelungen: (Prüfung der Rechtsgrundlage)	entfällt, da kein Rechtsakt
Subsidiaritätsprüfung:	entfällt, da kein Rechtsakt
Verhältnismäßigkeitsprüfung:	entfällt, da kein Rechtsakt
Zielsetzung:	Ausarbeitung von Maßnahmen zur Berücksichtigung beim Datenaustausch zwischen den USA und der EU vor dem Hintergrund der Veröffentlichungen zur Überwachungstätigkeit der NSA.
Inhaltliche Schwerpunkte:	Die Mitteilung ist ein politisches Strategiepapier über die transatlantischen Datenströme, in dem die sich aus den Enthüllungen über die umfangreichen Programme der US-Nachrichtendienste zur Sammlung von Informationen ergebenden Herausforderungen und Risiken beschrieben und die erforderlichen Maßnahmen zur Ausräumung der genannten Bedenken dargelegt werden. Das Papier fasst

verschiedene weitere Veröffentlichungen der EU zu Einzelthemen, wie die Analyse über die Funktionsweise des „Safe Harbour Abkommens“ und den Bericht über das TFTP-Abkommen (auch SWIFT-Abkommen genannt), zusammen.

Folgende Maßnahmen werden aufgegriffen angestrebt:

Datenschutzreformpaket

KOM sieht ist das von ihr Anfang 2012 vorgeschlagene Datenschutzreformpaket als ein Schlüsselement in Bezug auf den Schutz personenbezogener Daten an. Als Begründung werden fünf Elemente, die aus ihrer Sicht insoweit entscheidend sind, angeführt: das Marktortprinzip, Regelungen zu Drittstaatenübermittlungen, Sanktionen, Regelungen zu Verantwortlichkeiten und die Regelungen im Bereich Polizei und Justiz.

Verbesserung von Safe Harbour

KOM identifiziert als Schwachstellen der Safe-Harbor-Regelung Defizite bei der Transparenz und der Durchsetzung der Vereinbarung (insbesondere Inhalt und Veröffentlichung der Datenschutzerklärung der Safe-Harbor-registrierten Unternehmen, Verfügbarkeit alternativer Konfliktlösungsmechanismen für EU-Bürger, Durchsetzung durch die zuständigen US-Behörden, Zugang zu den Daten durch US-Sicherheitsbehörden) und gibt Empfehlungen zur verbesserten Umsetzung von Safe Harbor ab. Darüber hinaus kündigt KOM Gespräche mit den US-Behörden an, die der Identifizierung von Schwachstellen und deren Abhilfe bis Sommer 2014 dienen sollen.

Abschluss eines EU-US Datenschutzabkommens

KOM strebt den Abschluss eines Rahmenabkommens zum Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen an. Ein solches Abkommen solle den Rahmen für eine möglichst hohes Datenschutzniveau vorgeben und u.a. auch für einen effektiven Rechtsschutz für EU-Bürger außerhalb der USA geben und ggf. durch fachspezifische Einzelabkommen, wie das EU-US PNR- und das TFTP- Abkommen ergänzt werden.

Berücksichtigung von EU-Interessen im laufenden US-Reformprozess

Die von US-Präsident Obama initiierte Evaluierung der US-Sicherheitsbehörden soll genutzt werden, um eine Anhebung der Standards für EU-Bürger zu erreichen. Der Bericht spricht u.a. die Ungleichbehandlung von US- und EU-Bürgern, unterschiedliche Auffassungen über die Auslegung des Verhältnismäßigkeitsgrundsatzes und die mangelnden Rechtsschutzmöglichkeiten für EU-Bürger in den USA als zentrale Punkte an.

- 3 -

Politische Bedeutung:	Die politische Bedeutung ist nicht zuletzt vor dem Hintergrund der Veröffentlichungen zu Aktivitäten amerikanischer Nachrichtendienste mit hoch zu bewerten.
Was ist das besondere deutsche Interesse?	<p>Aufgrund der unmittelbaren Betroffenheit Deutschlands durch die Veröffentlichungen Edward Snowdens besteht an allen diesbezüglichen Maßnahmen/Empfehlungen grundsätzlich ein besonderes Interesse. Im Einzelnen:</p> <p><u>Datenschutzreformpaket</u></p> <p>Der dargestellte Zusammenhang zwischen den Überwachungsmaßnahmen und der Datenschutz-Grundverordnung (DSGVO) vermag nur teilweise zu überzeugen. Zutreffend ist, dass das Marktortprinzip zu einer Verbesserung des Datenschutzes im transatlantischen Verhältnis beitragen dürfte, weil US-Unternehmen in Europa unmittelbar an EU-Recht gebunden werden können. Bei den Drittstaatenregelungen ist zu differenzieren. Allgemein dürften die von der KOM vorgeschlagenen Regelungen kaum zu einer Verbesserung führen. Dies gilt insbesondere für Übermittlungen von Unternehmen an US-Behörden. Hierzu hatte DEU einen neuen Art. 42a vorgeschlagen. Die bisher formulierten Anforderungen an die Übermittlung personenbezogener Daten in Drittstaaten werden auch der technischen Entwicklung und Vernetzung noch nicht gerecht. Entgegen der Behauptungen der KOM bleiben insbesondere zentrale Fragen der Übermittlung, z.B. beim „Cloud computing“, ungelöst. Zu begrüßen ist, dass die KOM Ideen der US-Seite aufgegriffen hat, die das Weiße Haus in seinem Papier „Consumer Data Privacy in a Networked World („Consumer Bill of Rights“) im Februar 2012 entwickelt hat. Allerdings lässt KOM offen, wie sich diese Ideen in die DSGVO inkorporieren lassen.</p> <p><u>Safe Harbour</u></p> <p>Die Bundesregierung hat sich wiederholt für eine Verbesserung der Safe-Harbor-Regelung ausgesprochen, die schnellstmögliche Vorlage des KOM-Berichts zu Safe Harbor gefordert und drängt in der EU auf Nachverhandlungen des Safe-Harbor-Abkommens. Sie unterstützt die Vorschläge der KOM zur Verbesserung von Safe Harbor. Darüber hinaus setzt sie sich dafür ein, für Modelle wie Safe Harbor in der europäischen Datenschutz-Grundverordnung einen robusten Rechtsrahmen mit klaren Vorgaben für Garantien der Bürgerinnen und Bürger zu schaffen und hat bereits einen entsprechenden Vorschlag in die Verhandlungen in der Ratsarbeitsgruppe DAPIX eingebracht. Ziel ist es, die Individualrechte der Bürgerinnen und Bürger zu stärken und ihnen bessere Rechtsschutzmöglichkeiten zur Verfügung zu stellen, die Registrierung der Unternehmen in der EU vorzunehmen und die staatliche Kontrolle seitens der EU-Datenschutzaufsichtsbehörden in Modellen wie Safe-Harbor zu stärken.</p>

- 4 -

	<p><u>EU-US-Datenschutzabkommen</u></p> <p>Deutschland hat sich für einen baldigen Abschluss des Abkommens unter der Voraussetzung, dass damit mit Blick auf den Schutz personenbezogener Daten und den Individualrechtsschutz ein wirklicher Mehrwert geschaffen wird, ausgesprochen.</p> <p>Bislang haben sich die Verhandlungen schwierig gestaltet. In wichtigen Punkten herrscht weiterhin keine Einigung, so bei der Speicherdauer, der unabhängigen Aufsicht, den Individualrechten und dem Rechtsschutz. Auch wollen die USA weiterhin das Abkommen als sog. „executive agreement“ abschließen; ein solches kann US-Recht nicht abändern. Bei EU/US Justice and Home Affairs Ministerial Treffen am 18.11.2013 haben beide Seiten das Ziel bekräftigt, die Verhandlungen bis zum Sommer 2014 abzuschließen.</p> <p><u>Berücksichtigung von EU-Interessen im laufenden US-Reformprozess</u></p> <p>Deutschland hat sich auch auf EU-Ebene in den Prozess zur Aufklärung des Sachverhalts im Zusammenhang mit den Veröffentlichungen von Edward Snowden und zur Erarbeitung konkreter Empfehlungen der EU und der MS zur Berücksichtigung in der laufenden US-internen Evaluierung der Überwachungsprogramme intensiv eingebracht. Ein entsprechendes Dokument mit Vorschlägen zur Anwendung des Verhältnismäßigkeitsprinzips, zum verbesserten Individualrechtsschutz und zur Gleichstellung von EU- und US-Bürgern wurde am 6. Dezember 2013 im Rahmen des JI-Ministertreffens in Brüssel verabschiedet.</p>
bisherige Position des Deutschen Bundestages:	nicht bekannt
Position des Bundesrates:	nicht bekannt
Position des Europäischen Parlaments:	nicht bekannt
Meinungsstand im Rat:	nicht bekannt
Verfahrensstand: (Stand der Befassung)	
Finanzielle Auswirkungen:	

Zeitplan für die Behandlung im

- 5 -

a) Bundesrat:	nicht bekannt
b) Europäischen Parlament:	nicht bekannt
c) Rat:	nicht bekannt



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 29 November 2013

17067/13

**JAI 1095
USA 64
DATAPROTECT 190
COTER 154**

COVER NOTE

from:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	28 November 2013
to:	Mr Uwe CORSEPIUS, Secretary-General of the Council of the European Union
No Cion doc.:	COM(2013) 846 final
Subject:	Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-US Data Flows

Delegations will find attached Commission document COM(2013) 846 final.

Encl.: COM(2013) 846 final



EUROPEAN
COMMISSION

Brussels, 27.11.2013
COM(2013) 846 final

**COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN
PARLIAMENT AND THE COUNCIL**

Rebuilding Trust in EU-US Data Flows

1. INTRODUCTION: THE CHANGING ENVIRONMENT OF EU-US DATA PROCESSING

The European Union and the United States are strategic partners, and this partnership is critical for the promotion of our shared values, our security and our common leadership in global affairs.

However, trust in the partnership has been negatively affected and needs to be restored. The EU, its Member States and European citizens have expressed deep concerns at revelations of large-scale US intelligence collection programmes, in particular as regards the protection of personal data¹. Mass surveillance of private communication, be it of citizens, enterprises or political leaders, is unacceptable.

Transfers of personal data are an important and necessary element of the transatlantic relationship. They form an integral part of commercial exchanges across the Atlantic including for new growing digital businesses, such as social media or cloud computing, with large amounts of data going from the EU to the US. They also constitute a crucial component of EU-US co-operation in the law enforcement field, and of the cooperation between Member States and the US in the field of national security. In order to facilitate data flows, while ensuring a high level of data protection as required under EU law, the US and the EU have put in place a series of agreements and arrangements.

Commercial exchanges are addressed by Decision 2000/520/EC² (hereafter “the Safe Harbour Decision”). This Decision provides a legal basis for transfers of personal data from the EU to companies established in the US which have adhered to the Safe Harbour Privacy Principles.

Exchange of personal data between the EU and the US for the purposes of law enforcement, including the prevention and combating of terrorism and other forms of serious crime, is governed by a number of agreements at EU level. These are the Mutual Legal Assistance Agreement³, the Agreement on the use and transfer of Passenger Name Records (PNR)⁴, the Agreement on the processing and transfer of Financial Messaging Data for the purpose of the Terrorist Finance Tracking Program (TFTP)⁵, and the Agreement between Europol and the US. These Agreements respond to important security challenges and meet the common security interests of the EU and US, whilst providing a high level of protection of personal data. In addition, the EU and the US are currently negotiating a framework agreement on data protection in the field of police and judicial cooperation (“umbrella agreement”)⁶. The aim is to ensure a high level of data protection for citizens whose data is exchanged thereby further

¹ For the purposes of this Communication, references to EU citizens include also non-EU data subjects which fall within the scope of European Union's data protection law.

² Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25.8.2000, p. 7.

³ Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 291, 7.11. 2009, p. 40.

⁴ Council Decision 2012/472/EU of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L215, 11.8.2012, p. 4.

⁵ Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195, 27.7.2010, p. 3.

⁶ The Council adopted the Decision authorising the Commission to negotiating the Agreement on 3 December 2010. See IP/10/1661 of 3 December 2010.

advancing EU-US cooperation in the combating of crime and terrorism on the basis of shared values and agreed safeguards.

These instruments operate in an environment in which personal data flows are acquiring increasing relevance.

On the one hand, the development of the digital economy has led to exponential growth in the quantity, quality, diversity and nature of data processing activities. The use of electronic communication services by citizens in their daily lives has increased. Personal data has become a highly valuable asset: the estimated value of EU citizens' data was €315bn in 2011 and has the potential to grow to nearly €1tn annually by 2020⁷. The market for the analysis of large sets of data is growing by 40% per year worldwide⁸. Similarly, technological developments, for example related to cloud computing, put into perspective the notion of international data transfer as cross-border data flows are becoming a day to day reality.⁹

The increase in the use of electronic communications and data processing services, including cloud computing, has also substantially expanded the scope and significance of transatlantic data transfers. Elements such as the central position of US companies in the digital economy¹⁰, the transatlantic routing of a large part of electronic communications and the volume of electronic data flows between the EU and the US have become even more relevant. On the other hand, modern methods of personal data processing raise new and important questions. This applies both to new means of large-scale processing of consumer data by private companies for commercial purposes, and to the increased ability of large-scale surveillance of communications data by intelligence agencies.

Large-scale US intelligence collection programmes, such as PRISM affect the fundamental rights of Europeans and, specifically, their right to privacy and to the protection of personal data. These programmes also point to a connection between Government surveillance and the processing of data by private companies, notably by US internet companies. As a result, they may therefore have an economic impact. If citizens are concerned about the large-scale processing of their personal data by private companies or by the surveillance of their data by intelligence agencies when using Internet services, this may affect their trust in the digital economy, with potential negative consequences on growth.

These developments expose EU-US data flows to new challenges. This Communication addresses these challenges. It explores the way forward on the basis of the findings contained in the Report of the EU Co-Chairs of the ad hoc EU-US Working Group and the Communication on the Safe Harbour.

It seeks to provide an effective way forward to rebuild trust and reinforce EU-US cooperation in these fields and strengthen the broader transatlantic relationship.

This Communication is based on the premise that the standard of protection of personal data must be addressed in its proper context, without affecting other dimensions of EU-US relations, including the on-going negotiations for a Transatlantic Trade and Investment Partnership. For this reason, data protection standards will not be negotiated within the Transatlantic Trade and Investment Partnership, which will fully respect the data protection rules.

⁷ See Boston Consulting Group, "The Value of our Digital Identity", November 2012.

⁸ See McKinsey, "Big data: The next frontier for innovation, competition, and productivity", 2011

⁹ Communication on Unleashing the potential of cloud computing in Europe, COM(2012) 529 final

¹⁰ For example, the combined number of unique visitors to Microsoft Hotmail, Google Gmail and Yahoo! Mail from European countries in June 2012 totalled over 227 million, eclipsing that of all other providers. The combined number of unique European users accessing Facebook and Facebook Mobile in March 2012 was 196.5 million, making Facebook the largest social network in Europe. Google is the leading internet search engine with 90.2% of worldwide internet users. US mobile messaging service What's App was used by 91% of iPhone users in Germany in June 2013.

It is important to note that whilst the EU can take action in areas of EU competence, in particular to safeguard the application of EU law¹¹, national security remains the sole responsibility of each Member State¹².

2. THE IMPACT ON THE INSTRUMENTS FOR DATA TRANSFERS

First, as regards data transferred for commercial purposes, the Safe Harbour has proven to be an important vehicle for EU-US data transfers. Its commercial importance has grown as personal data flows have taken on greater prominence in the transatlantic commercial relationship. Over the past 13 years, the Safe Harbour scheme has evolved to include more than 3.000 companies, over half of which have signed up within the last five years. Yet concerns about the level of protection of personal data of EU citizens transferred to the US under the Safe Harbour scheme have grown. The voluntary and declaratory nature of the scheme has sharpened focus on its transparency and enforcement. While a majority of US companies apply its principles, some self-certified companies do not. The non-compliance of some self-certified companies with the Safe Harbour Privacy Principles places such companies at a competitive advantage in relation to European companies operating in the same markets.

Moreover, while under the Safe Harbour, limitations to data protection rules are permitted where necessary on grounds of national security¹³, the question has arisen whether the large-scale collection and processing of personal information under US surveillance programmes is necessary and proportionate to meet the interests of national security. It is also clear from the findings of the ad hoc EU-US Working Group that, under these programmes, EU citizens do not enjoy the same rights and procedural safeguards as Americans.

The reach of these surveillance programmes, combined with the unequal treatment of EU citizens, brings into question the level of protection afforded by the Safe Harbour arrangement. The personal data of EU citizens sent to the US under the Safe Harbour may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the EU and the purposes for which it was transferred to the US. A majority of the US internet companies that appear to be more directly concerned by these programmes are certified under the Safe Harbour scheme.

Second, as regards exchanges of data for law enforcement purposes, the existing Agreements (PNR, TFTP) have proven highly valuable tools to address common security threats linked to serious transnational crime and terrorism, whilst laying down safeguards that ensure a high level of data protection¹⁴. These safeguards extend to EU citizens, and the Agreements provide for mechanisms to review their implementation and to address issues of concern related thereto. The TFTP Agreement also establishes a system of oversight, with EU independent overseers checking how data covered by the Agreement is searched by the US.

Against the backdrop of concerns raised in the EU about US surveillance programmes, the European Commission has used those mechanisms to check how the agreements are applied. In the case of the PNR Agreement, a joint review was conducted, involving data protection

¹¹ See Judgment of the Court of Justice of the European Union in Case C-300/11, ZZ v Secretary of State for the Home Department.

¹² Article 4(2) TEU.

¹³ See e.g. Safe Harbour Decision, Annex I.

¹⁴ See Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data pursuant to Article 6 (6) of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program.

experts from the EU and the US, looking at how the Agreement has been implemented¹⁵. That review did not give any indication that US surveillance programmes extend to or have impact on the passenger data covered by the PNR Agreement. In the case of the TFTP Agreement, the Commission opened formal consultations after allegations were made of US intelligence agencies directly accessing personal data in the EU, contrary to the Agreement. These consultations did not reveal any elements proving a breach of the TFTP Agreement, and they led the US to provide written assurance that no direct data collection has taken place contrary to the provisions of the Agreement.

The large-scale collection and processing of personal information under US surveillance programmes call, however, for a continuation of very close monitoring of the implementation of the PNR and TFTP Agreements in the future. The EU and the US have therefore agreed to advance the next Joint Review of the TFTP Agreement, which will be held in Spring 2014. Within that and future joint reviews, greater transparency will be ensured on how the system of oversight operates and on how it protects the data of EU citizens. In parallel, steps will be taken to ensure that the system of oversight continues to pay close attention to how data transferred to the US under the Agreement is processed, with a focus on how such data is shared between US authorities.

Third, the increase in the volume of processing of personal data underlines the importance of the legal and administrative safeguards that apply. One of the goals of the Ad Hoc EU-US Working Group was to establish what safeguards apply to minimise the impact of the processing on the fundamental rights of EU citizens. Safeguards are also necessary to protect companies. Certain US laws such as the Patriot Act, enable US authorities to directly request companies access to data stored in the EU. Therefore, European companies, and US companies present in the EU, may be required to transfer data to the US in breach of EU and Member States' laws, and are consequently caught between conflicting legal obligations. Legal uncertainty deriving from such direct requests may hold back the development of new digital services, such as cloud computing, which can provide efficient, lower-cost solutions for individuals and businesses.

3. ENSURING THE EFFECTIVENESS OF DATA PROTECTION

Transfers of personal data between the EU and the US are an essential component of the transatlantic commercial relationship. Information sharing is also an essential component of EU-US security cooperation, critically important to the common goal of preventing and combating serious crime and terrorism. However, recent revelations about US intelligence collection programmes have negatively affected the trust on which this cooperation is based. In particular, it has affected trust in the way personal data is processed. The following steps should be taken to restore trust in data transfers for the benefit of the digital economy, security both in the EU and in the US, and the broader transatlantic relationship.

3.1. The EU data protection reform

The data protection reform proposed by the Commission in January 2012¹⁶ provides a key response as regards the protection of personal data. Five components of the proposed Data Protection package are of particular importance.

¹⁵ See on the Commission report "Joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security".

¹⁶ COM(2012) 10 final: Proposal for a Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25.1.2012, and COM(2012) 11 final: Proposal for a Regulation of the European Parliament and the Council on the protection of individuals

First, as regards territorial scope, the proposed regulation makes clear that companies that are not established in the Union will have to apply EU data protection law when they offer goods and services to European consumers or monitor their behaviour. In other words, the fundamental right to data protection will be respected, independently of the geographical location of a company or of its processing facility¹⁷.

Secondly, on international transfers, the proposed regulation establishes the conditions under which data can be transferred outside the EU. Transfers can only be allowed where these conditions, which safeguard the individuals' rights to a high level of protection, are met¹⁸.

Thirdly, concerning enforcement, the proposed rules provide for proportionate and dissuasive sanctions (up to 2% of a company's annual global turnover) to make sure that companies comply with EU law¹⁹. The existence of credible sanctions will increase companies' incentive to comply with EU law.

Fourthly, the proposed regulation includes clear rules on the obligations and liabilities of data processors such as cloud providers, including on security²⁰. As the revelations about US intelligence collection programmes have shown, this is critical because these programmes affect data stored in the cloud. Also, companies providing storage space in the cloud which are asked to provide personal data to foreign authorities will not be able to escape their responsibility by reference to their status as data processors rather than data controllers.

Fifth, the package will lead to the establishment of comprehensive rules for the protection of personal data processed in the law enforcement sector.

It is expected that the package will be agreed upon in a timely manner in the course of 2014²¹.

3.2. Making Safe Harbour safer

The Safe Harbour scheme is an important component of the EU-US commercial relationship, relied upon by companies on both sides of the Atlantic.

The Commission's report on the functioning of Safe Harbour has identified a number of weaknesses in the scheme. As a result of a lack of transparency and of enforcement, some self-certified Safe Harbour members do not, in practice, comply with its principles. This has a negative impact on EU citizens' fundamental rights. It also creates a disadvantage for European companies compared to those competing US companies that are operating under the scheme but in practice not applying its principles. This weakness also affects the majority of US companies which properly apply the scheme. Safe Harbour also acts as a conduit for the

with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

¹⁷ The Commission takes note that the European Parliament confirmed and strengthened this important principle, enshrined in Art. 3 of the proposed Regulation, in its vote of 21 October 2013 on the data protection reform reports of MEPs Jan-Philipp Albrecht and Dimitrios Droutsas in the Committee for Civil Liberties, Justice and Home Affairs (LIBE).

¹⁸ The Commission takes note that in its vote of 21 October 2013, the LIBE Committee of the European Parliament proposed to include a provision in the future Regulation that would subject requests from foreign authorities to access personal data collected in the EU to the obtaining of a prior authorisation from a national data protection authority, where such a request would be issued outside a mutual legal assistance treaty or another international agreement.

¹⁹ The Commission takes note that in its vote of 21 October 2013, the LIBE Committee proposed strengthening the Commission's proposal by providing that fines can go up to 5% of the annual worldwide turnover of a company.

²⁰ The Commission takes note that in its vote of 21 October 2013, the LIBE Committee endorsed the strengthening of the obligations and liabilities of data processors, in the particular with regard to Art. 26 of the proposed Regulation.

²¹ The Conclusions of the October 2013 European Council state that: "It is important to foster the trust of citizens and businesses in the digital economy. The timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015".

transfer of the personal data of EU citizens from the EU to the US by companies required to surrender data to US intelligence agencies under the US intelligence collection programmes. Unless the deficiencies are corrected, it therefore constitutes a competitive disadvantage for EU business and has a negative impact on the fundamental right to data protection of EU citizens.

The shortcomings of the Safe Harbour scheme have been underlined by the response of European Data Protection Authorities to the recent surveillance revelations. Article 3 of the Safe Harbour Decision authorises these authorities to suspend, under certain conditions, data flows to certified companies.²² German data protection commissioners have decided not to issue new permissions for data transfers to non-EU countries (for example for the use of certain cloud services). They will also examine whether data transfers on the basis of the Safe Harbour should be suspended.²³ The risk is that such measures, taken at national level, would create differences in coverage, which means that Safe Harbour would cease to be a core mechanism for the transfer of personal data between the EU and the US.

The Commission has the authority under Directive 95/46/EC to suspend or revoke the Safe Harbour decision if the scheme no longer provides an adequate level of protection. Furthermore, Article 3 of the Safe Harbour Decision provides that the Commission may reverse, suspend or limit the scope of the decision, while, under article 4, it may adapt the decision at any time in the light of experience with its implementation.

Against this background, a number of policy options can be considered, including:

- Maintaining the *status quo*;
- Strengthening the Safe Harbour scheme and reviewing its functioning thoroughly;
- Suspending or revoking the Safe Harbour decision.

Given the weaknesses identified, the current implementation of Safe Harbour cannot be maintained. However, its revocation would adversely affect the interests of member companies in the EU and in the US. The Commission considers that Safe Harbour should rather be strengthened.

The improvements should address both the structural shortcomings related to transparency and enforcement, the substantive Safe Harbour principles and the operation of the national security exception.

More specifically, for Safe Harbour to work as intended, the monitoring and supervision by US authorities of the compliance of certified companies with the Safe Harbour Privacy Principles needs to be more effective and systematic. The transparency of certified companies' privacy policies needs to be improved. The availability and affordability of dispute resolution mechanisms also needs to be ensured to EU citizens.

As a matter of urgency, the Commission will engage with the US authorities to discuss the shortcomings identified. Remedies should be identified by summer 2014 and implemented as soon as possible. On the basis thereof, the Commission will undertake a complete stock taking of the functioning of the Safe Harbour. This broader review process should involve open consultation and a debate in the European Parliament and the Council as well as discussions with the US authorities.

²² Specifically, pursuant to Art. 3 of the Safe Harbour Decision, such suspensions may take place in cases where there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

²³ Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, press release of 24 July 2013.

It is also important that the national security exception foreseen by the Safe Harbour Decision, is used only to an extent that is strictly necessary and proportionate.

3.3. Strengthening data protection safeguards in law enforcement cooperation

The EU and the US are currently negotiating a data protection "umbrella" agreement on transfers and processing of personal information in the context of police and judicial cooperation in criminal matters. The conclusion of such an agreement providing for a high level of protection of personal data would represent a major contribution to strengthening trust across the Atlantic. By advancing the protection of EU data citizens' rights, it would help strengthen transatlantic cooperation aimed at preventing and combating crime and terrorism.

According to the decision authorising the Commission to negotiate the umbrella agreement, the aim of the negotiations should be to ensure a high level of protection in line with the EU data protection *acquis*. This should be reflected in agreed rules and safeguards on, *inter alia*, purpose limitation, the conditions and the duration of the retention of data. In the context of the negotiation, the Commission should also obtain commitments on enforceable rights including judicial redress mechanisms for EU citizens not resident in the US²⁴. Close EU-US cooperation to address common security challenges should be mirrored by efforts to ensure that citizens benefit from the same rights when the same data is processed for the same purposes on both sides of the Atlantic. It is also important that derogations based on national security needs are narrowly defined. Safeguards and limitations should be agreed in this respect.

These negotiations provide an opportunity to clarify that personal data held by private companies and located in the EU will not be directly accessed by or transferred to US law enforcement authorities outside of formal channels of co-operation, such as Mutual Legal Assistance agreements or sectoral EU-US Agreements authorising such transfers. Access by other means should be excluded, unless it takes place in clearly defined, exceptional and judicially reviewable situations. The US should undertake commitments in that regard²⁵.

An "umbrella agreement" agreed along those lines, should provide the general framework to ensure a high level of protection of personal data when transferred to the US for the purpose of preventing or combating crime and terrorism. Sectoral agreements should, where necessary due to the nature of the data transfer concerned, lay down additional rules and safeguards, building on the example of the EU-US PNR and TFTP Agreements, which set strict conditions for transfer of data and safeguards for EU citizens.

²⁴ See the relevant passage of the Joint Press Statement following the EU-US-Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington: "We are therefore, as a matter of urgency, committed to advancing rapidly in the negotiations on a meaningful and comprehensive data protection umbrella agreement in the field of law enforcement. The agreement would act as a basis to facilitate transfers of data in the context of police and judicial cooperation in criminal matters by ensuring a high level of personal data protection for U.S. and EU citizens. We are committed to working to resolve the remaining issues raised by both sides, including judicial redress (a critical issue for the EU). Our aim is to complete the negotiations on the agreement ahead of summer 2014."

²⁵ See the relevant passage of the Joint Press Statement following the EU-US Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington: "We also underline the value of the EU-U.S. Mutual Legal Assistance Agreement. We reiterate our commitment to ensure that it is used broadly and effectively for evidence purposes in criminal proceedings. There were also discussions on the need to clarify that personal data held by private entities in the territory of the other party will not be accessed by law enforcement agencies outside of legally authorized channels. We also agree to review the functioning of the Mutual Legal Assistance Agreement, as contemplated in the Agreement, and to consult each other whenever needed."

3.4. Addressing European concerns in the on-going US reform process

US President Obama has announced a review of US national security authorities' activities, including of the applicable legal framework. This on-going process provides an important opportunity to address EU concerns raised by recent revelations about US intelligence collection programmes. The most important changes would be extending the safeguards available to US citizens and residents to EU citizens not resident in the US, increased transparency of intelligence activities, and further strengthening oversight. Such changes would restore trust in EU-US data exchanges, and promote the use of Internet services by Europeans.

With respect to extending the safeguards available to US citizens and residents to EU citizens, legal standards in relation to US surveillance programmes which treat US and EU citizens differently should be reviewed, including from the perspective of necessity and proportionality, keeping in mind the close transatlantic security partnership based on common values, rights and freedoms. This would reduce the extent to which Europeans are affected by US intelligence collection programmes.

More transparency is needed on the legal framework of US intelligence collection programmes and its interpretation by US Courts as well as on the quantitative dimension of US intelligence collection programmes. EU citizens would also benefit from such changes.

The oversight of US intelligence collection programmes would be improved by strengthening the role of the Foreign Intelligence Surveillance Court and by introducing remedies for individuals. These mechanisms could reduce the processing of personal data of Europeans that are not relevant for national security purposes.

3.5. Promoting privacy standards internationally

Issues raised by modern methods of data protection are not limited to data transfer between the EU and the US. A high level of protection of personal data should also be guaranteed to any individual. EU rules on collection, processing and transfer of data should be promoted internationally.

Recently, a number of initiatives have been proposed to promote the protection of privacy, particularly on the internet²⁶. The EU should ensure that such initiatives, if pursued, fully take into account the principles of protecting fundamental rights, freedom of expression, personal data and privacy as set out in EU law and in the EU Cyber Security Strategy, and do not undermine the freedom, openness and security of cyber space. This includes a democratic and efficient multi stakeholder governance model.

The on-going reforms of data protection laws on both sides of the Atlantic also provide the EU and the US a unique opportunity to set the standard internationally. Data exchanges across the Atlantic and beyond would greatly benefit from the strengthening of the US domestic legal framework, including the passage of the "Consumer Privacy Bill of Rights" announced by President Obama in February 2012 as part of a comprehensive blueprint to improve consumers' privacy protections. The existence of a set of strong and enforceable data protection rules enshrined in both the EU and the US would constitute a solid basis for cross-border data flows.

In view of promoting privacy standards internationally, accession to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), which is open to countries which are not member of the Council of Europe²⁷, should also be favoured. Safeguards and guarantees agreed in international fora should result in a high level of protection compatible with what is required under EU law.

²⁶ See in this respect the draft resolution proposed to the UN General Assembly by Germany and Brazil – calling for the protection of privacy online as offline.

²⁷ The US is already party to another Council of Europe convention: the 2001 Convention on Cybercrime (also known as the "Budapest Convention").

4. CONCLUSIONS AND RECOMMENDATIONS

The issues identified in this Communication require action to be taken by the US as well as by the EU and its Member States.

The concerns around transatlantic data exchanges are, first of all, a wake-up call for the EU and its Member States to advance swiftly and with ambition on the data protection reform. It shows that a strong legislative framework with clear rules that are enforceable also in situations when data are transferred abroad is, more than ever, a necessity. The EU institutions should therefore continue working towards the adoption of the EU data protection reform by spring 2014, to make sure that personal data is effectively and comprehensively protected.

Given the significance of transatlantic data flows, it is essential that the instruments on which these exchanges are based appropriately address the challenges and opportunities of the digital era and new technological developments like cloud computing. Existing and future arrangements and agreements should ensure that the continuity of a high level of protection is guaranteed over the Atlantic.

A robust Safe Harbour scheme is in the interests of EU and US citizens and companies. It should be strengthened by better monitoring and implementation in the short term, and, on this basis, by a broader review of its functioning. Improvements are necessary to ensure that the original objectives of the Safe Harbour Decision – i.e. continuity of data protection, legal certainty and free EU-US flow of data – are still met.

These improvements should focus on the need for the US authorities to better supervise and monitor the compliance of self-certified companies with the Safe Harbour Privacy Principles. It is also important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary and proportionate.

In the area of law enforcement, the current negotiations of an “umbrella agreement” should result in a high level of protection for citizens on both sides of the Atlantic. Such an agreement would strengthen the trust of Europeans in EU-US data exchanges, and provide a basis to further develop EU-US security cooperation and partnership. In the context of the negotiation, commitments should be secured to the effect that procedural safeguards, including judicial redress, are available to Europeans who are not resident in the US.

Commitments should be sought from the US administration to ensure that personal data held by private entities in the EU will not be accessed directly by US law enforcement agencies outside of formal channels of co-operation, such as Mutual Legal Assistance agreements and sectoral EU-US Agreements such as PNR and TFTP authorising such transfers under strict conditions, except in clearly defined, exceptional and judicially reviewable situations.

The US should also extend the safeguards available to US citizens and residents to EU citizens not resident in the US, ensure the necessity and proportionality of the programmes, greater transparency and oversight in the legal framework applicable to US national security authorities.

Areas listed in this communication will require constructive engagement from both sides of the Atlantic. Together, as strategic partners, the EU and the US have the ability to overcome the current tensions in the transatlantic relationship and rebuild trust in EU-US data flows. Undertaking joint political and legal commitments on further cooperation in these areas will strengthen the overall transatlantic relationship.

Dokument 2014/0033235

Von: Spitzer, Patrick, Dr.
Gesendet: Mittwoch, 22. Januar 2014 12:08
An: BMWI BUERO-EA2; AA Oelfke, Christian; AA Kinder, Kristin; AA Wendel, Philipp; BMJ Henrichs, Christoph; BMJ Harms, Katharina
Cc: PGDS_; VI4_; IT1_; OESIII1_; BMWI Bölhoff, Corinna; 'ref132@bk.bund.de'; BK Rensmann, Michael; Bender, Ulrike; Merz, Jürgen; Schlender, Katharina; Marscholleck, Dietmar; OESI3AG_; Stöber, Karlheinz, Dr.; Weinbrenner, Ulrich; RegOeSI3; Kotira, Jan; Stang, Rüdiger
Betreff: Frist 22.01., 17:000 Uhr: Anforderung eines Berichtsbogens zur Unterrichtung des Deutschen Bundestages (17067/13)
Anlagen: 140122_Berichtsb_Rebuilding Trust.doc; 17067.EN13.pdf
Wichtigkeit: Hoch

ÖS I 3-52000/4#1

Liebe Kolleginnen und Kollegen,

ich bitte um Mitzeichnung zum als **Anlage 1** beigefügten Berichtsbogen zur Unterrichtung des Deutschen Bundestages **bis heute, 22. Januar 2014, 17.00 Uhr** (Rückmeldungen bitte auch an das Postfach oesi3ag@bmi.bund.de). Grundlage der Berichterstattung ist das als **Anlage 2** beigefügte Dokument „Rebuilding Trust in EU US Data Flows“.

Freundliche Grüße

Patrick Spitzer

im Auftrag
Dr. Patrick Spitzer

Bundesministerium des Innern
Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,
BKA-Gesetz, Datenschutz im Sicherheitsbereich)
Alt-Moabit 101D, 10559 Berlin
Telefon: +49 (0)30 18681-1390
E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

B E R I C H T S B O G E N

gemäß Anlage zu § 6 Absatz 2 EUZBBG und Ziffer II. 3. der Anlage zu § 9 EUZBLG

Ressort/Referat:	AG ÖS I 3	Datum:	20.01.2014
Referatsleiterin/ Referatsleiter:	MinR Weinbrenner MinR Taube	Telefon:	030 186811300
Bearbeiterin/ Bearbeiter:	RR Dr. Spitzer	Telefon:	030 186811390
abgestimmt mit:	BMJV; BMWi, AA	Telefax:	

Thema:	Mitteilung der Kommission an das Europäische Parlament und den Rat über die Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA
Sachgebiet:	Europäische Justiz- und Innenpolitik
Ratsdok.-Nummer:	17067/13
KOM-Nummer:	COM(2013) 846 final
Nummer des interinstitutionellen Dossiers:	nicht bekannt
Nummer der Bundesratsdrucksache:	nicht bekannt
Nachweis der Zulässigkeit für europäische Regelungen: (Prüfung der Rechtsgrundlage)	entfällt, da kein Rechtsakt
Subsidiaritätsprüfung:	entfällt, da kein Rechtsakt
Verhältnismäßigkeitsprüfung:	entfällt, da kein Rechtsakt
Zielsetzung:	Ausarbeitung von Maßnahmen zur Berücksichtigung beim Datenaustausch zwischen den USA und der EU vor dem Hintergrund der Veröffentlichungen zur Überwachungstätigkeit der NSA.
Inhaltliche Schwerpunkte:	Die Mitteilung ist ein politisches Strategiepapier über die transatlantischen Datenströme, in dem die sich aus den Enthüllungen über die umfangreichen Programme der US-Nachrichtendienste zur Sammlung von Informationen ergebenden Herausforderungen und Risiken aus Sicht der KOM beschrieben und die nach Auffassung der KOM erforderlichen Maßnahmen zur Ausräumung der genannten

- 2 -

Bedenken dargelegt werden. Das Papier fasst verschiedene weitere Veröffentlichungen der EU zu Einzelthemen, wie die Analyse über die Funktionsweise des „Safe Harbor Abkommens“ und den Bericht über das TFTP-Abkommen (auch SWIFT-Abkommen genannt), zusammen.

Folgende Maßnahmen werden von der KOM aufgegriffen:

Datenschutzreformpaket

KOM sieht das von ihr Anfang 2012 vorgeschlagene Datenschutzreformpaket als ein Schlüsselement in Bezug auf den Schutz personenbezogener Daten an. Als Begründung werden fünf Elemente, die aus ihrer Sicht insoweit entscheidend sind, angeführt: das Marktortprinzip, Regelungen zu Drittstaatenübermittlungen, Sanktionen, Regelungen zu Verantwortlichkeiten und die Regelungen im Bereich Polizei und Justiz.

Verbesserung von Safe Harbor

KOM identifiziert als Schwachstellen der Safe-Harbor-Regelung Defizite bei der Transparenz und der Durchsetzung der Vereinbarung (insbesondere Inhalt und Veröffentlichung der Datenschutzerklärung der Safe-Harbor-registrierten Unternehmen, Verfügbarkeit alternativer Konfliktlösungsmechanismen für EU-Bürger, Durchsetzung durch die zuständigen US-Behörden, Zugang zu den Daten durch US-Sicherheitsbehörden) und gibt Empfehlungen zur verbesserten Umsetzung von Safe Harbor ab. Darüber hinaus kündigt KOM Gespräche mit den US-Behörden an, die der gemeinsamen Identifizierung von Schwachstellen und deren Abhilfe bis Sommer 2014 dienen sollen.

Abschluss eines EU-US Datenschutzabkommens

KOM strebt den Abschluss eines Rahmenabkommens zum Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen an. Ein solches Abkommen solle den Rahmen für eine möglichst hohes Datenschutzniveau vorgeben und u.a. auch für einen effektiven Rechtsschutz für EU-Bürger außerhalb der USA geben und ggf. durch fachspezifische Einzelabkommen, wie das EU-US PNR- und das TFTP- Abkommen ergänzt werden.

Berücksichtigung von EU-Interessen im laufenden US-Reformprozess

Die von US-Präsident Obama initiierte Evaluierung der US-Sicherheitsbehörden soll genutzt werden, um eine Anhebung der Standards für EU-Bürger zu erreichen. Der Bericht spricht u.a. die Ungleichbehandlung von US- und EU-Bürgern, unterschiedliche Auffassungen über die Auslegung des Verhältnismäßigkeitsgrundsatzes und die mangelnden Rechtsschutzmöglichkeiten für EU-Bürger in den USA als zentrale Punkte an.

<p>Politische Bedeutung:</p>	<p>Die politische Bedeutung ist vor dem Hintergrund der andauernden Veröffentlichungen zu Aktivitäten amerikanischer Nachrichtendienste und der öffentlichen Diskussion in DEU und auf internationaler Ebene als hoch zu bewerten.</p>
<p>Was ist das besondere deutsche Interesse?</p>	<p>Aufgrund der unmittelbaren Betroffenheit Deutschlands durch die Veröffentlichungen Edward Snowdens besteht an allen diesbezüglichen Maßnahmen/Empfehlungen grundsätzlich ein besonderes Interesse. Generell ist dabei zu beachten, dass die EU zwar eine Kompetenz für den Datenschutz, nicht jedoch für die Tätigkeit der Nachrichtendienste hat. Im Einzelnen:</p> <p><u>Datenschutzreformpaket</u></p> <p>Der dargestellte Zusammenhang zwischen den Überwachungsmaßnahmen und der Datenschutz-Grundverordnung (DSGVO) vermag nur teilweise zu überzeugen. Zutreffend ist, dass das Marktortprinzip zu einer Verbesserung des Datenschutzes im transatlantischen Verhältnis beitragen dürfte, weil US-Unternehmen in Europa unmittelbar an EU-Recht gebunden werden können. Bei den Drittstaatenregelungen ist zu differenzieren. Allgemein dürften die von der KOM vorgeschlagenen Regelungen kaum zu einer Verbesserung führen. Dies gilt insbesondere für Übermittlungen von Unternehmen an US-Behörden. Hierzu hatte DEU einen neuen Art. 42a vorgeschlagen. Die bisher formulierten Anforderungen an die Übermittlung personenbezogener Daten in Drittstaaten werden auch der technischen Entwicklung und Vernetzung noch nicht gerecht. Entgegen den Behauptungen der KOM bleiben insbesondere zentrale Fragen der Übermittlung, z.B. beim „Cloud computing“, ungelöst. Zu begrüßen ist, dass die KOM Ideen der US-Seite aufgegriffen hat, die das Weiße Haus in seinem Papier „Consumer Data Privacy in a Networked World („Consumer Bill of Rights“) im Februar 2012 entwickelt hat. Allerdings lässt KOM offen, wie sich diese Ideen in die DSGVO inkorporieren lassen.</p> <p><u>Safe Harbor</u></p> <p>Die Bundesregierung hat sich wiederholt für eine Verbesserung der Safe-Harbor-Regelung ausgesprochen, die schnellstmögliche Vorlage des KOM-Berichts zu Safe Harbor gefordert und drängt in der EU auf Nachverhandlungen des Safe-Harbor-Abkommens. Sie unterstützt die Vorschläge der KOM zur Verbesserung von Safe Harbor. Darüber hinaus setzt sie sich dafür ein, für Modelle wie Safe Harbor in der europäischen Datenschutz-Grundverordnung einen robusten Rechtsrahmen mit klaren Vorgaben für Garantien der Bürgerinnen und Bürger zu schaffen und hat bereits einen entsprechenden Vorschlag in die Verhandlungen in der Ratsarbeitsgruppe DAPIX eingebracht. Ziel ist es, die Individualrechte der Bürgerinnen und Bürger zu</p>

- 4 -

	<p>stärken und ihnen bessere Rechtsschutzmöglichkeiten zur Verfügung zu stellen, die Registrierung der Unternehmen in der EU vorzunehmen und die staatliche Kontrolle seitens der EU-Datenschutzaufsichtsbehörden in Modellen wie Safe-Harbor zu stärken.</p> <p><u>EU-US-Datenschutzabkommen</u></p> <p>Deutschland hat sich für einen baldigen Abschluss des Abkommens unter der Voraussetzung, dass damit mit Blick auf den Schutz personenbezogener Daten und den Individualrechtsschutz ein wirklicher Mehrwert geschaffen wird, ausgesprochen.</p> <p>Bislang haben sich die Verhandlungen schwierig gestaltet. In wichtigen Punkten herrscht weiterhin keine Einigkeit so bei der Speicherdauer, der unabhängigen Aufsicht, den Individualrechten und dem Rechtsschutz. Auch wollen die USA weiterhin das Abkommen als sog. „executive agreement“ abschließen; ein solches kann US-Recht nicht abändern. Bei EU/US Justice and Home Affairs Ministerial Treffen am 18.11.2013 haben beide Seiten das Ziel bekräftigt, die Verhandlungen bis zum Sommer 2014 abzuschließen.</p> <p><u>Berücksichtigung von EU-Interessen im laufenden US-Reformprozess</u></p> <p>Deutschland hat sich auch auf EU-Ebene in den Prozess zur Aufklärung des Sachverhalts im Zusammenhang mit den Veröffentlichungen von Edward Snowden und zur Erarbeitung konkreter Empfehlungen der EU und der MS zur Berücksichtigung in der laufenden US-internen Evaluierung der Überwachungsprogramme intensiv eingebracht. Ein Dokument der EU und der MS mit Vorschlägen zur Anwendung des Verhältnismäßigkeitsprinzips, zum verbesserten Individualrechtsschutz und zur Gleichstellung von EU- und US-Bürgern wurde am 6. Dezember 2013 im Rahmen des JI-Ministertreffens in Brüssel behandelt.</p>
bisherige Position des Deutschen Bundestages:	nicht bekannt
Position des Bundesrates:	nicht bekannt
Position des Europäischen Parlaments:	nicht bekannt
Meinungsstand im Rat:	keine Behandlung durch den Rat
Verfahrensstand: (Stand der Befassung)	
Finanzielle Auswirkungen:	

- 5 -

Zeitplan für die Behandlung im

a) Bundesrat:	nicht bekannt
b) Europäischen Parlament:	nicht bekannt
c) Rat:	nicht bekannt



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 29 November 2013

17067/13

**JAI 1095
USA 64
DATAPROTECT 190
COTER 154**

COVER NOTE

from: Secretary-General of the European Commission,
signed by Mr Jordi AYET PUIGARNAU, Director

date of receipt: 28 November 2013

to: Mr Uwe CORSEPIUS, Secretary-General of the Council of the European
Union

No Cion doc.: COM(2013) 846 final

Subject: Communication from the Commission to the European Parliament and the
Council
Rebuilding Trust in EU-US Data Flows

Delegations will find attached Commission document COM(2013) 846 final.

Encl.: COM(2013) 846 final



EUROPEAN
COMMISSION

Brussels, 27.11.2013
COM(2013) 846 final

**COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN
PARLIAMENT AND THE COUNCIL**

Rebuilding Trust in EU-US Data Flows

1. INTRODUCTION: THE CHANGING ENVIRONMENT OF EU-US DATA PROCESSING

The European Union and the United States are strategic partners, and this partnership is critical for the promotion of our shared values, our security and our common leadership in global affairs.

However, trust in the partnership has been negatively affected and needs to be restored. The EU, its Member States and European citizens have expressed deep concerns at revelations of large-scale US intelligence collection programmes, in particular as regards the protection of personal data¹. Mass surveillance of private communication, be it of citizens, enterprises or political leaders, is unacceptable.

Transfers of personal data are an important and necessary element of the transatlantic relationship. They form an integral part of commercial exchanges across the Atlantic including for new growing digital businesses, such as social media or cloud computing, with large amounts of data going from the EU to the US. They also constitute a crucial component of EU-US co-operation in the law enforcement field, and of the cooperation between Member States and the US in the field of national security. In order to facilitate data flows, while ensuring a high level of data protection as required under EU law, the US and the EU have put in place a series of agreements and arrangements.

Commercial exchanges are addressed by Decision 2000/520/EC² (hereafter “the Safe Harbour Decision”). This Decision provides a legal basis for transfers of personal data from the EU to companies established in the US which have adhered to the Safe Harbour Privacy Principles.

Exchange of personal data between the EU and the US for the purposes of law enforcement, including the prevention and combating of terrorism and other forms of serious crime, is governed by a number of agreements at EU level. These are the Mutual Legal Assistance Agreement³, the Agreement on the use and transfer of Passenger Name Records (PNR)⁴, the Agreement on the processing and transfer of Financial Messaging Data for the purpose of the Terrorist Finance Tracking Program (TFTP)⁵, and the Agreement between Europol and the US. These Agreements respond to important security challenges and meet the common security interests of the EU and US, whilst providing a high level of protection of personal data. In addition, the EU and the US are currently negotiating a framework agreement on data protection in the field of police and judicial cooperation (“umbrella agreement”)⁶. The aim is to ensure a high level of data protection for citizens whose data is exchanged thereby further

¹ For the purposes of this Communication, references to EU citizens include also non-EU data subjects which fall within the scope of European Union's data protection law.

² Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25.8.2000, p. 7.

³ Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 291, 7.11. 2009, p. 40.

⁴ Council Decision 2012/472/EU of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L215, 11.8.2012, p. 4.

⁵ Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195, 27.7.2010, p. 3.

⁶ The Council adopted the Decision authorising the Commission to negotiating the Agreement on 3 December 2010. See IP/10/1661 of 3 December 2010.

advancing EU-US cooperation in the combating of crime and terrorism on the basis of shared values and agreed safeguards.

These instruments operate in an environment in which personal data flows are acquiring increasing relevance.

On the one hand, the development of the digital economy has led to exponential growth in the quantity, quality, diversity and nature of data processing activities. The use of electronic communication services by citizens in their daily lives has increased. Personal data has become a highly valuable asset: the estimated value of EU citizens' data was €315bn in 2011 and has the potential to grow to nearly €1tn annually by 2020⁷. The market for the analysis of large sets of data is growing by 40% per year worldwide⁸. Similarly, technological developments, for example related to cloud computing, put into perspective the notion of international data transfer as cross-border data flows are becoming a day to day reality.⁹

The increase in the use of electronic communications and data processing services, including cloud computing, has also substantially expanded the scope and significance of transatlantic data transfers. Elements such as the central position of US companies in the digital economy¹⁰, the transatlantic routing of a large part of electronic communications and the volume of electronic data flows between the EU and the US have become even more relevant. On the other hand, modern methods of personal data processing raise new and important questions. This applies both to new means of large-scale processing of consumer data by private companies for commercial purposes, and to the increased ability of large-scale surveillance of communications data by intelligence agencies.

Large-scale US intelligence collection programmes, such as PRISM affect the fundamental rights of Europeans and, specifically, their right to privacy and to the protection of personal data. These programmes also point to a connection between Government surveillance and the processing of data by private companies, notably by US internet companies. As a result, they may therefore have an economic impact. If citizens are concerned about the large-scale processing of their personal data by private companies or by the surveillance of their data by intelligence agencies when using Internet services, this may affect their trust in the digital economy, with potential negative consequences on growth.

These developments expose EU-US data flows to new challenges. This Communication addresses these challenges. It explores the way forward on the basis of the findings contained in the Report of the EU Co-Chairs of the ad hoc EU-US Working Group and the Communication on the Safe Harbour.

It seeks to provide an effective way forward to rebuild trust and reinforce EU-US cooperation in these fields and strengthen the broader transatlantic relationship.

This Communication is based on the premise that the standard of protection of personal data must be addressed in its proper context, without affecting other dimensions of EU-US relations, including the on-going negotiations for a Transatlantic Trade and Investment Partnership. For this reason, data protection standards will not be negotiated within the Transatlantic Trade and Investment Partnership, which will fully respect the data protection rules.

⁷ See Boston Consulting Group, "The Value of our Digital Identity", November 2012.

⁸ See McKinsey, "Big data: The next frontier for innovation, competition, and productivity", 2011

⁹ Communication on Unleashing the potential of cloud computing in Europe, COM(2012) 529 final

¹⁰ For example, the combined number of unique visitors to Microsoft Hotmail, Google Gmail and Yahoo! Mail from European countries in June 2012 totalled over 227 million, eclipsing that of all other providers. The combined number of unique European users accessing Facebook and Facebook Mobile in March 2012 was 196.5 million, making Facebook the largest social network in Europe. Google is the leading internet search engine with 90.2% of worldwide internet users. US mobile messaging service What's App was used by 91% of iPhone users in Germany in June 2013.

It is important to note that whilst the EU can take action in areas of EU competence, in particular to safeguard the application of EU law¹¹, national security remains the sole responsibility of each Member State¹².

2. THE IMPACT ON THE INSTRUMENTS FOR DATA TRANSFERS

First, as regards data transferred for commercial purposes, the Safe Harbour has proven to be an important vehicle for EU-US data transfers. Its commercial importance has grown as personal data flows have taken on greater prominence in the transatlantic commercial relationship. Over the past 13 years, the Safe Harbour scheme has evolved to include more than 3.000 companies, over half of which have signed up within the last five years. Yet concerns about the level of protection of personal data of EU citizens transferred to the US under the Safe Harbour scheme have grown. The voluntary and declaratory nature of the scheme has sharpened focus on its transparency and enforcement. While a majority of US companies apply its principles, some self-certified companies do not. The non-compliance of some self-certified companies with the Safe Harbour Privacy Principles places such companies at a competitive advantage in relation to European companies operating in the same markets.

Moreover, while under the Safe Harbour, limitations to data protection rules are permitted where necessary on grounds of national security¹³, the question has arisen whether the large-scale collection and processing of personal information under US surveillance programmes is necessary and proportionate to meet the interests of national security. It is also clear from the findings of the ad hoc EU-US Working Group that, under these programmes, EU citizens do not enjoy the same rights and procedural safeguards as Americans.

The reach of these surveillance programmes, combined with the unequal treatment of EU citizens, brings into question the level of protection afforded by the Safe Harbour arrangement. The personal data of EU citizens sent to the US under the Safe Harbour may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the EU and the purposes for which it was transferred to the US. A majority of the US internet companies that appear to be more directly concerned by these programmes are certified under the Safe Harbour scheme.

Second, as regards exchanges of data for law enforcement purposes, the existing Agreements (PNR, TFTP) have proven highly valuable tools to address common security threats linked to serious transnational crime and terrorism, whilst laying down safeguards that ensure a high level of data protection¹⁴. These safeguards extend to EU citizens, and the Agreements provide for mechanisms to review their implementation and to address issues of concern related thereto. The TFTP Agreement also establishes a system of oversight, with EU independent overseers checking how data covered by the Agreement is searched by the US.

Against the backdrop of concerns raised in the EU about US surveillance programmes, the European Commission has used those mechanisms to check how the agreements are applied. In the case of the PNR Agreement, a joint review was conducted, involving data protection

¹¹ See Judgment of the Court of Justice of the European Union in Case C-300/11, ZZ v Secretary of State for the Home Department.

¹² Article 4(2) TEU.

¹³ See e.g. Safe Harbour Decision, Annex I.

¹⁴ See Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data pursuant to Article 6 (6) of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program.

experts from the EU and the US, looking at how the Agreement has been implemented¹⁵. That review did not give any indication that US surveillance programmes extend to or have impact on the passenger data covered by the PNR Agreement. In the case of the TFTP Agreement, the Commission opened formal consultations after allegations were made of US intelligence agencies directly accessing personal data in the EU, contrary to the Agreement. These consultations did not reveal any elements proving a breach of the TFTP Agreement, and they led the US to provide written assurance that no direct data collection has taken place contrary to the provisions of the Agreement.

The large-scale collection and processing of personal information under US surveillance programmes call, however, for a continuation of very close monitoring of the implementation of the PNR and TFTP Agreements in the future. The EU and the US have therefore agreed to advance the next Joint Review of the TFTP Agreement, which will be held in Spring 2014. Within that and future joint reviews, greater transparency will be ensured on how the system of oversight operates and on how it protects the data of EU citizens. In parallel, steps will be taken to ensure that the system of oversight continues to pay close attention to how data transferred to the US under the Agreement is processed, with a focus on how such data is shared between US authorities.

Third, the increase in the volume of processing of personal data underlines the importance of the legal and administrative safeguards that apply. One of the goals of the Ad Hoc EU-US Working Group was to establish what safeguards apply to minimise the impact of the processing on the fundamental rights of EU citizens. Safeguards are also necessary to protect companies. Certain US laws such as the Patriot Act, enable US authorities to directly request companies access to data stored in the EU. Therefore, European companies, and US companies present in the EU, may be required to transfer data to the US in breach of EU and Member States' laws, and are consequently caught between conflicting legal obligations. Legal uncertainty deriving from such direct requests may hold back the development of new digital services, such as cloud computing, which can provide efficient, lower-cost solutions for individuals and businesses.

3. ENSURING THE EFFECTIVENESS OF DATA PROTECTION

Transfers of personal data between the EU and the US are an essential component of the transatlantic commercial relationship. Information sharing is also an essential component of EU-US security cooperation, critically important to the common goal of preventing and combating serious crime and terrorism. However, recent revelations about US intelligence collection programmes have negatively affected the trust on which this cooperation is based. In particular, it has affected trust in the way personal data is processed. The following steps should be taken to restore trust in data transfers for the benefit of the digital economy, security both in the EU and in the US, and the broader transatlantic relationship.

3.1. The EU data protection reform

The data protection reform proposed by the Commission in January 2012¹⁶ provides a key response as regards the protection of personal data. Five components of the proposed Data Protection package are of particular importance.

¹⁵ See on the Commission report "Joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security".

¹⁶ COM(2012) 10 final: Proposal for a Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25.1.2012, and COM(2012) 11 final: Proposal for a Regulation of the European Parliament and the Council on the protection of individuals

First, as regards territorial scope, the proposed regulation makes clear that companies that are not established in the Union will have to apply EU data protection law when they offer goods and services to European consumers or monitor their behaviour. In other words, the fundamental right to data protection will be respected, independently of the geographical location of a company or of its processing facility¹⁷.

Secondly, on international transfers, the proposed regulation establishes the conditions under which data can be transferred outside the EU. Transfers can only be allowed where these conditions, which safeguard the individuals' rights to a high level of protection, are met¹⁸.

Thirdly, concerning enforcement, the proposed rules provide for proportionate and dissuasive sanctions (up to 2% of a company's annual global turnover) to make sure that companies comply with EU law¹⁹. The existence of credible sanctions will increase companies' incentive to comply with EU law.

Fourthly, the proposed regulation includes clear rules on the obligations and liabilities of data processors such as cloud providers, including on security²⁰. As the revelations about US intelligence collection programmes have shown, this is critical because these programmes affect data stored in the cloud. Also, companies providing storage space in the cloud which are asked to provide personal data to foreign authorities will not be able to escape their responsibility by reference to their status as data processors rather than data controllers.

Fifth, the package will lead to the establishment of comprehensive rules for the protection of personal data processed in the law enforcement sector.

It is expected that the package will be agreed upon in a timely manner in the course of 2014²¹.

3.2. Making Safe Harbour safer

The Safe Harbour scheme is an important component of the EU-US commercial relationship, relied upon by companies on both sides of the Atlantic.

The Commission's report on the functioning of Safe Harbour has identified a number of weaknesses in the scheme. As a result of a lack of transparency and of enforcement, some self-certified Safe Harbour members do not, in practice, comply with its principles. This has a negative impact on EU citizens' fundamental rights. It also creates a disadvantage for European companies compared to those competing US companies that are operating under the scheme but in practice not applying its principles. This weakness also affects the majority of US companies which properly apply the scheme. Safe Harbour also acts as a conduit for the

with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

¹⁷ The Commission takes note that the European Parliament confirmed and strengthened this important principle, enshrined in Art. 3 of the proposed Regulation, in its vote of 21 October 2013 on the data protection reform reports of MEPs Jan-Philipp Albrecht and Dimitrios Droutsas in the Committee for Civil Liberties, Justice and Home Affairs (LIBE).

¹⁸ The Commission takes note that in its vote of 21 October 2013, the LIBE Committee of the European Parliament proposed to include a provision in the future Regulation that would subject requests from foreign authorities to access personal data collected in the EU to the obtaining of a prior authorisation from a national data protection authority, where such a request would be issued outside a mutual legal assistance treaty or another international agreement.

¹⁹ The Commission takes note that in its vote of 21 October 2013, the LIBE Committee proposed strengthening the Commission's proposal by providing that fines can go up to 5% of the annual worldwide turnover of a company.

²⁰ The Commission takes note that in its vote of 21 October 2013, the LIBE Committee endorsed the strengthening of the obligations and liabilities of data processors, in the particular with regard to Art. 26 of the proposed Regulation.

²¹ The Conclusions of the October 2013 European Council state that: "It is important to foster the trust of citizens and businesses in the digital economy. The timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015".

transfer of the personal data of EU citizens from the EU to the US by companies required to surrender data to US intelligence agencies under the US intelligence collection programmes. Unless the deficiencies are corrected, it therefore constitutes a competitive disadvantage for EU business and has a negative impact on the fundamental right to data protection of EU citizens.

The shortcomings of the Safe Harbour scheme have been underlined by the response of European Data Protection Authorities to the recent surveillance revelations. Article 3 of the Safe Harbour Decision authorises these authorities to suspend, under certain conditions, data flows to certified companies.²² German data protection commissioners have decided not to issue new permissions for data transfers to non-EU countries (for example for the use of certain cloud services). They will also examine whether data transfers on the basis of the Safe Harbour should be suspended.²³ The risk is that such measures, taken at national level, would create differences in coverage, which means that Safe Harbour would cease to be a core mechanism for the transfer of personal data between the EU and the US.

The Commission has the authority under Directive 95/46/EC to suspend or revoke the Safe Harbour decision if the scheme no longer provides an adequate level of protection. Furthermore, Article 3 of the Safe Harbour Decision provides that the Commission may reverse, suspend or limit the scope of the decision, while, under article 4, it may adapt the decision at any time in the light of experience with its implementation.

Against this background, a number of policy options can be considered, including:

- Maintaining the *status quo*;
- Strengthening the Safe Harbour scheme and reviewing its functioning thoroughly;
- Suspending or revoking the Safe Harbour decision.

Given the weaknesses identified, the current implementation of Safe Harbour cannot be maintained. However, its revocation would adversely affect the interests of member companies in the EU and in the US. The Commission considers that Safe Harbour should rather be strengthened.

The improvements should address both the structural shortcomings related to transparency and enforcement, the substantive Safe Harbour principles and the operation of the national security exception.

More specifically, for Safe Harbour to work as intended, the monitoring and supervision by US authorities of the compliance of certified companies with the Safe Harbour Privacy Principles needs to be more effective and systematic. The transparency of certified companies' privacy policies needs to be improved. The availability and affordability of dispute resolution mechanisms also needs to be ensured to EU citizens.

As a matter of urgency, the Commission will engage with the US authorities to discuss the shortcomings identified. Remedies should be identified by summer 2014 and implemented as soon as possible. On the basis thereof, the Commission will undertake a complete stock taking of the functioning of the Safe Harbour. This broader review process should involve open consultation and a debate in the European Parliament and the Council as well as discussions with the US authorities.

²² Specifically, pursuant to Art. 3 of the Safe Harbour Decision, such suspensions may take place in cases where there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

²³ Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, press release of 24 July 2013.

It is also important that the national security exception foreseen by the Safe Harbour Decision, is used only to an extent that is strictly necessary and proportionate.

3.3. Strengthening data protection safeguards in law enforcement cooperation

The EU and the US are currently negotiating a data protection “umbrella” agreement on transfers and processing of personal information in the context of police and judicial cooperation in criminal matters. The conclusion of such an agreement providing for a high level of protection of personal data would represent a major contribution to strengthening trust across the Atlantic. By advancing the protection of EU data citizens' rights, it would help strengthen transatlantic cooperation aimed at preventing and combating crime and terrorism. According to the decision authorising the Commission to negotiate the umbrella agreement, the aim of the negotiations should be to ensure a high level of protection in line with the EU data protection *acquis*. This should be reflected in agreed rules and safeguards on, *inter alia*, purpose limitation, the conditions and the duration of the retention of data. In the context of the negotiation, the Commission should also obtain commitments on enforceable rights including judicial redress mechanisms for EU citizens not resident in the US²⁴. Close EU-US cooperation to address common security challenges should be mirrored by efforts to ensure that citizens benefit from the same rights when the same data is processed for the same purposes on both sides of the Atlantic. It is also important that derogations based on national security needs are narrowly defined. Safeguards and limitations should be agreed in this respect.

These negotiations provide an opportunity to clarify that personal data held by private companies and located in the EU will not be directly accessed by or transferred to US law enforcement authorities outside of formal channels of co-operation, such as Mutual Legal Assistance agreements or sectoral EU-US Agreements authorising such transfers. Access by other means should be excluded, unless it takes place in clearly defined, exceptional and judicially reviewable situations. The US should undertake commitments in that regard²⁵.

An “umbrella agreement” agreed along those lines, should provide the general framework to ensure a high level of protection of personal data when transferred to the US for the purpose of preventing or combating crime and terrorism. Sectoral agreements should, where necessary due to the nature of the data transfer concerned, lay down additional rules and safeguards, building on the example of the EU-US PNR and TFTP Agreements, which set strict conditions for transfer of data and safeguards for EU citizens.

²⁴ See the relevant passage of the Joint Press Statement following the EU-US-Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington: “We are therefore, as a matter of urgency, committed to advancing rapidly in the negotiations on a meaningful and comprehensive data protection umbrella agreement in the field of law enforcement. The agreement would act as a basis to facilitate transfers of data in the context of police and judicial cooperation in criminal matters by ensuring a high level of personal data protection for U.S. and EU citizens. We are committed to working to resolve the remaining issues raised by both sides, including judicial redress (a critical issue for the EU). Our aim is to complete the negotiations on the agreement ahead of summer 2014.”

²⁵ See the relevant passage of the Joint Press Statement following the EU-US Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington: “We also underline the value of the EU-U.S. Mutual Legal Assistance Agreement. We reiterate our commitment to ensure that it is used broadly and effectively for evidence purposes in criminal proceedings. There were also discussions on the need to clarify that personal data held by private entities in the territory of the other party will not be accessed by law enforcement agencies outside of legally authorized channels. We also agree to review the functioning of the Mutual Legal Assistance Agreement, as contemplated in the Agreement, and to consult each other whenever needed.”

3.4. Addressing European concerns in the on-going US reform process

US President Obama has announced a review of US national security authorities' activities, including of the applicable legal framework. This on-going process provides an important opportunity to address EU concerns raised by recent revelations about US intelligence collection programmes. The most important changes would be extending the safeguards available to US citizens and residents to EU citizens not resident in the US, increased transparency of intelligence activities, and further strengthening oversight. Such changes would restore trust in EU-US data exchanges, and promote the use of Internet services by Europeans.

With respect to extending the safeguards available to US citizens and residents to EU citizens, legal standards in relation to US surveillance programmes which treat US and EU citizens differently should be reviewed, including from the perspective of necessity and proportionality, keeping in mind the close transatlantic security partnership based on common values, rights and freedoms. This would reduce the extent to which Europeans are affected by US intelligence collection programmes.

More transparency is needed on the legal framework of US intelligence collection programmes and its interpretation by US Courts as well as on the quantitative dimension of US intelligence collection programmes. EU citizens would also benefit from such changes.

The oversight of US intelligence collection programmes would be improved by strengthening the role of the Foreign Intelligence Surveillance Court and by introducing remedies for individuals. These mechanisms could reduce the processing of personal data of Europeans that are not relevant for national security purposes.

3.5. Promoting privacy standards internationally

Issues raised by modern methods of data protection are not limited to data transfer between the EU and the US. A high level of protection of personal data should also be guaranteed to any individual. EU rules on collection, processing and transfer of data should be promoted internationally.

Recently, a number of initiatives have been proposed to promote the protection of privacy, particularly on the internet²⁶. The EU should ensure that such initiatives, if pursued, fully take into account the principles of protecting fundamental rights, freedom of expression, personal data and privacy as set out in EU law and in the EU Cyber Security Strategy, and do not undermine the freedom, openness and security of cyber space. This includes a democratic and efficient multi stakeholder governance model.

The on-going reforms of data protection laws on both sides of the Atlantic also provide the EU and the US a unique opportunity to set the standard internationally. Data exchanges across the Atlantic and beyond would greatly benefit from the strengthening of the US domestic legal framework, including the passage of the "Consumer Privacy Bill of Rights" announced by President Obama in February 2012 as part of a comprehensive blueprint to improve consumers' privacy protections. The existence of a set of strong and enforceable data protection rules enshrined in both the EU and the US would constitute a solid basis for cross-border data flows.

In view of promoting privacy standards internationally, accession to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), which is open to countries which are not member of the Council of Europe²⁷, should also be favoured. Safeguards and guarantees agreed in international fora should result in a high level of protection compatible with what is required under EU law.

²⁶ See in this respect the draft resolution proposed to the UN General Assembly by Germany and Brazil – calling for the protection of privacy online as offline.

²⁷ The US is already party to another Council of Europe convention: the 2001 Convention on Cybercrime (also known as the "Budapest Convention").

4. CONCLUSIONS AND RECOMMENDATIONS

The issues identified in this Communication require action to be taken by the US as well as by the EU and its Member States.

The concerns around transatlantic data exchanges are, first of all, a wake-up call for the EU and its Member States to advance swiftly and with ambition on the data protection reform. It shows that a strong legislative framework with clear rules that are enforceable also in situations when data are transferred abroad is, more than ever, a necessity. The EU institutions should therefore continue working towards the adoption of the EU data protection reform by spring 2014, to make sure that personal data is effectively and comprehensively protected.

Given the significance of transatlantic data flows, it is essential that the instruments on which these exchanges are based appropriately address the challenges and opportunities of the digital era and new technological developments like cloud computing. Existing and future arrangements and agreements should ensure that the continuity of a high level of protection is guaranteed over the Atlantic.

A robust Safe Harbour scheme is in the interests of EU and US citizens and companies. It should be strengthened by better monitoring and implementation in the short term, and, on this basis, by a broader review of its functioning. Improvements are necessary to ensure that the original objectives of the Safe Harbour Decision – i.e. continuity of data protection, legal certainty and free EU-US flow of data – are still met.

These improvements should focus on the need for the US authorities to better supervise and monitor the compliance of self-certified companies with the Safe Harbour Privacy Principles. It is also important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary and proportionate.

In the area of law enforcement, the current negotiations of an “umbrella agreement” should result in a high level of protection for citizens on both sides of the Atlantic. Such an agreement would strengthen the trust of Europeans in EU-US data exchanges, and provide a basis to further develop EU-US security cooperation and partnership. In the context of the negotiation, commitments should be secured to the effect that procedural safeguards, including judicial redress, are available to Europeans who are not resident in the US.

Commitments should be sought from the US administration to ensure that personal data held by private entities in the EU will not be accessed directly by US law enforcement agencies outside of formal channels of co-operation, such as Mutual Legal Assistance agreements and sectoral EU-US Agreements such as PNR and TFTP authorising such transfers under strict conditions, except in clearly defined, exceptional and judicially reviewable situations.

The US should also extend the safeguards available to US citizens and residents to EU citizens not resident in the US, ensure the necessity and proportionality of the programmes, greater transparency and oversight in the legal framework applicable to US national security authorities.

Areas listed in this communication will require constructive engagement from both sides of the Atlantic. Together, as strategic partners, the EU and the US have the ability to overcome the current tensions in the transatlantic relationship and rebuild trust in EU-US data flows. Undertaking joint political and legal commitments on further cooperation in these areas will strengthen the overall transatlantic relationship.

Dokument 2014/0034385

Von: BMWi Bölhoff, Corinna
Gesendet: Mittwoch, 22. Januar 2014 16:22
An: Spitzer, Patrick, Dr.
Cc: PGDS_; AA Oelfke, Christian; AA Kinder, Kristin; AA Wendel, Philipp; BMJ Henrichs, Christoph; BMJ Harms, Katharina; VI4_; IT1_; OESIII1_; 'ref132@bk.bund.de'; BK Rensmann, Michael; Bender, Ulrike; Merz, Jürgen; Schlender, Katharina; Marscholleck, Dietmar; OESI3AG_; Stöber, Karlheinz, Dr.; Weinbrenner, Ulrich; RegOeSI3; Kotira, Jan; Stang, Rüdiger; BMWi Scholl, Kirsten; BMWi Bölhoff, Corinna; Tageskopien-EA2@bmwi.bund.de
Betreff: AW: Frist 22.01., 17:00 Uhr: Anforderung eines Berichtsbogens zur Unterrichtung des Deutschen Bundestages (17067/13)
Anlagen: 140122_Berichtsb_Rebuilding Trust_BMWi.doc

Lieber Herr Spitzer,

BMWi zeichnet ohne inhaltliche Anmerkungen mit. Eine winzige redaktionelle Änderung habe ich eingefügt.

Mit freundlichen Grüßen,
 Corinna Bölhoff

Dr. Corinna Bölhoff

Referat EA2 - Zukunft der EU, Justiz und Inneres, Bessere Rechtsetzung
 Bundesministerium für Wirtschaft und Energie
 Scharnhorststr. 34-37, 10115 Berlin
 Telefon: +49 (0)30 18615-6937
 Fax: +49 (0)30 18615-50-6937
 E-Mail: corinna.boelhoff@bmwi.bund.de
 Internet: <http://www.bmwi.de>

Von: Patrick.Spitzer@bmi.bund.de [mailto:Patrick.Spitzer@bmi.bund.de]

Gesendet: Mittwoch, 22. Januar 2014 12:08

An: BUERO-EA2; e05-2@auswaertiges-amt.de; e05-3@auswaertiges-amt.de; 200-4@auswaertiges-amt.de; henrichs-ch@bmj.bund.de; harms-ka@bmj.bund.de

Cc: PGDS@bmi.bund.de; VI4@bmi.bund.de; IT1@bmi.bund.de; OESIII1@bmi.bund.de; Bölhoff, Corinna, Dr., EA2; 'ref132@bk.bund.de'; Michael.Rensmann@bk.bund.de; Ulrike.Bender@bmi.bund.de; Juergen.Merz@bmi.bund.de; Katharina.Schlender@bmi.bund.de; Dietmar.Marscholleck@bmi.bund.de; OESI3AG@bmi.bund.de; Karlheinz.Stoeber@bmi.bund.de; Ulrich.Weinbrenner@bmi.bund.de; RegOeSI3@bmi.bund.de; Jan.Kotira@bmi.bund.de; Ruediger.Stang@bmi.bund.de

Betreff: Frist 22.01., 17:00 Uhr: Anforderung eines Berichtsbogens zur Unterrichtung des Deutschen Bundestages (17067/13)

Wichtigkeit: Hoch

ÖS I 3-52000/4#1

Liebe Kolleginnen und Kollegen,

ich bitte um Mitzeichnung zum als **Anlage 1** beigefügten Berichtsbogen zur Unterrichtung des Deutschen Bundestages **bis heute, 22. Januar 2014, 17.00 Uhr** (Rückmeldungen bitte auch an das Postfach oesi3ag@bmi.bund.de). Grundlage der Berichterstattung ist das als **Anlage 2** beigefügte Dokument „Rebuilding Trust in EU US Data Flows“.

Freundliche Grüße

Patrick Spitzer

im Auftrag
Dr. Patrick Spitzer

Bundesministerium des Innern
Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,
BKA-Gesetz, Datenschutz im Sicherheitsbereich)
Alt-Moabit 101D, 10559 Berlin
Telefon: +49 (0)30 18681-1390
E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

B E R I C H T S B O G E N

gemäß Anlage zu § 6 Absatz 2 EUZBBG und Ziffer II. 3. der Anlage zu § 9 EUZBLG

Ressort/Referat:	AG ÖS I 3	Datum:	20.01.2014
Referatsleiterin/ Referatsleiter:	MinR Weinbrenner MinR Taube	Telefon:	030 186811300
Bearbeiterin/ Bearbeiter:	RR Dr. Spitzer	Telefon:	030 186811390
abgestimmt mit:	BMJV; BMWi, AA	Telefax:	

Thema:	Mitteilung der Kommission an das Europäische Parlament und den Rat über die Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA
Sachgebiet:	Europäische Justiz- und Innenpolitik
Ratsdok.-Nummer:	17067/13
KOM-Nummer:	COM(2013) 846 final
Nummer des interinstitutionellen Dossiers:	nicht bekannt
Nummer der Bundesratsdrucksache:	nicht bekannt
Nachweis der Zulässigkeit für europäische Regelungen: (Prüfung der Rechtsgrundlage)	entfällt, da kein Rechtsakt
Subsidiaritätsprüfung:	entfällt, da kein Rechtsakt
Verhältnismäßigkeitsprüfung:	entfällt, da kein Rechtsakt
Zielsetzung:	Ausarbeitung von Maßnahmen zur Berücksichtigung beim Datenaustausch zwischen den USA und der EU vor dem Hintergrund der Veröffentlichungen zur Überwachungstätigkeit der NSA.
Inhaltliche Schwerpunkte:	Die Mitteilung ist ein politisches Strategiepapier über die transatlantischen Datenströme, in dem die sich aus den Enthüllungen über die umfangreichen Programme der US-Nachrichtendienste zur Sammlung von Informationen ergebenden Herausforderungen und Risiken aus Sicht der KOM beschrieben und die nach Auffassung der KOM erforderlichen Maßnahmen zur Ausräumung der genannten

- 2 -

Bedenken dargelegt werden. Das Papier fasst verschiedene weitere Veröffentlichungen der EU zu Einzelthemen, wie die Analyse über die Funktionsweise des „Safe Harbor Abkommens“ und den Bericht über das TFTP-Abkommen (auch SWIFT-Abkommen genannt), zusammen.

Folgende Maßnahmen werden von der KOM aufgegriffen:

Datenschutzreformpaket

KOM sieht das von ihr Anfang 2012 vorgeschlagene Datenschutzreformpaket als ein Schlüsselement in Bezug auf den Schutz personenbezogener Daten an. Als Begründung werden fünf Elemente, die aus ihrer Sicht insoweit entscheidend sind, angeführt: das Marktortprinzip, Regelungen zu Drittstaatenübermittlungen, Sanktionen, Regelungen zu Verantwortlichkeiten und die Regelungen im Bereich Polizei und Justiz.

Verbesserung von Safe Harbor

KOM identifiziert als Schwachstellen der Safe-Harbor-Regelung Defizite bei der Transparenz und der Durchsetzung der Vereinbarung (insbesondere Inhalt und Veröffentlichung der Datenschutzerklärung der Safe-Harbor-registrierten Unternehmen, Verfügbarkeit alternativer Konfliktlösungsmechanismen für EU-Bürger, Durchsetzung durch die zuständigen US-Behörden, Zugang zu den Daten durch US-Sicherheitsbehörden) und gibt Empfehlungen zur verbesserten Umsetzung von Safe Harbor ab. Darüber hinaus kündigt KOM Gespräche mit den US-Behörden an, die der gemeinsamen Identifizierung von Schwachstellen und deren Abhilfe bis Sommer 2014 dienen sollen.

Abschluss eines EU-US Datenschutzabkommens

KOM strebt den Abschluss eines Rahmenabkommens zum Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen an. Ein solches Abkommen solle den Rahmen für eine möglichst hohes Datenschutzniveau vorgeben und u.a. auch für einen effektiven Rechtsschutz für EU-Bürger außerhalb der USA geben und ggf. durch fachspezifische Einzelabkommen, wie das EU-US PNR- und das TFTP- Abkommen ergänzt werden.

Berücksichtigung von EU-Interessen im laufenden US-Reformprozess

Die von US-Präsident Obama initiierte Evaluierung der US-Sicherheitsbehörden soll genutzt werden, um eine Anhebung der Standards für EU-Bürger zu erreichen. Der Bericht spricht u.a. die Ungleichbehandlung von US- und EU-Bürgern, unterschiedliche Auffassungen über die Auslegung des Verhältnismäßigkeitsgrundsatzes und die mangelnden Rechtsschutzmöglichkeiten für EU-Bürger in den USA als zentrale Punkte an.

- 3 -

<p>Politische Bedeutung:</p>	<p>Die politische Bedeutung ist vor dem Hintergrund der andauernden Veröffentlichungen zu Aktivitäten amerikanischer Nachrichtendienste und der öffentlichen Diskussion in DEU und auf internationaler Ebene als hoch zu bewerten.</p>
<p>Was ist das besondere deutsche Interesse?</p>	<p>Aufgrund der unmittelbaren Betroffenheit Deutschlands durch die Veröffentlichungen Edward Snowdens besteht an allen diesbezüglichen Maßnahmen/Empfehlungen grundsätzlich ein besonderes Interesse. Generell ist dabei zu beachten, dass die EU zwar eine Kompetenz für den Datenschutz, nicht jedoch für die Tätigkeit der Nachrichtendienste hat. Im Einzelnen:</p> <p><u>Datenschutzreformpaket</u></p> <p>Der dargestellte Zusammenhang zwischen den Überwachungsmaßnahmen und der Datenschutz-Grundverordnung (DSGVO) vermag nur teilweise zu überzeugen. Zutreffend ist, dass das Marktortprinzip zu einer Verbesserung des Datenschutzes im transatlantischen Verhältnis beitragen dürfte, weil US-Unternehmen in Europa unmittelbar an EU-Recht gebunden werden können. Bei den Drittstaatenregelungen ist zu differenzieren. Allgemein dürften die von der KOM vorgeschlagenen Regelungen kaum zu einer Verbesserung führen. Dies gilt insbesondere für Übermittlungen von Unternehmen an US-Behörden. Hierzu hatte DEU einen neuen Art. 42a vorgeschlagen. Die bisher formulierten Anforderungen an die Übermittlung personenbezogener Daten in Drittstaaten werden auch der technischen Entwicklung und Vernetzung noch nicht gerecht. Entgegen den Behauptungen der KOM bleiben insbesondere zentrale Fragen der Übermittlung, z.B. beim „Cloud computing“, ungelöst. Zu begrüßen ist, dass die KOM Ideen der US-Seite aufgegriffen hat, die das Weiße Haus in seinem Papier „Consumer Data Privacy in a Networked World („Consumer Bill of Rights“) im Februar 2012 entwickelt hat. Allerdings lässt KOM offen, wie sich diese Ideen in die DSGVO inkorporieren lassen.</p> <p><u>Safe Harbor</u></p> <p>Die Bundesregierung hat sich wiederholt für eine Verbesserung der Safe-Harbor-Regelung ausgesprochen, die schnellstmögliche Vorlage des KOM-Berichts zu Safe Harbor gefordert und drängt in der EU auf Nachverhandlungen des Safe-Harbor-Abkommens. Sie unterstützt die Vorschläge der KOM zur Verbesserung von Safe Harbor. Darüber hinaus setzt sie sich dafür ein, für Modelle wie Safe Harbor in der europäischen Datenschutz-Grundverordnung einen robusten Rechtsrahmen mit klaren Vorgaben für Garantien der Bürgerinnen und Bürger zu schaffen und hat bereits einen entsprechenden Vorschlag in die Verhandlungen in der Ratsarbeitsgruppe DAPIX eingebracht. Ziel ist es, die Individualrechte der Bürgerinnen und Bürger zu</p>

- 4 -

	<p>stärken und ihnen bessere Rechtsschutzmöglichkeiten zur Verfügung zu stellen, die Registrierung der Unternehmen in der EU vorzunehmen und die staatliche Kontrolle seitens der EU-Datenschutzaufsichtsbehörden in Modellen wie Safe-Harbor zu stärken.</p> <p><u>EU-US-Datenschutzabkommen</u></p> <p>Deutschland hat sich für einen baldigen Abschluss des Abkommens unter der Voraussetzung, dass damit mit Blick auf den Schutz personenbezogener Daten und den Individualrechtsschutz ein wirklicher Mehrwert geschaffen wird, ausgesprochen.</p> <p>Bislang haben sich die Verhandlungen schwierig gestaltet. In wichtigen Punkten herrscht weiterhin keine Einigkeit so bei der Speicherdauer, der unabhängigen Aufsicht, den Individualrechten und dem Rechtsschutz. Auch wollen die USA weiterhin das Abkommen als sog. „executive agreement“ abschließen; ein solches kann US-Recht nicht abändern. Bei EU/US Justice and Home Affairs Ministerial Treffen am 18.11.2013 haben beide Seiten das Ziel bekräftigt, die Verhandlungen bis zum Sommer 2014 abzuschließen.</p> <p><u>Berücksichtigung von EU-Interessen im laufenden US-Reformprozess</u></p> <p>Deutschland hat sich auch auf EU-Ebene in den Prozess zur Aufklärung des Sachverhalts im Zusammenhang mit den Veröffentlichungen von Edward Snowden und zur Erarbeitung konkreter Empfehlungen der EU und der MS zur Berücksichtigung in der laufenden US-internen Evaluierung der Überwachungsprogramme intensiv eingebracht. Ein Dokument der EU und der MS mit Vorschlägen zur Anwendung des Verhältnismäßigkeitsprinzips, zum verbesserten Individualrechtsschutz und zur Gleichstellung von EU- und US-Bürgern wurde am 6. Dezember 2013 im Rahmen des <u>JI-Ministertreffens</u> <u>Ministerrats</u> in Brüssel behandelt.</p>
bisherige Position des Deutschen Bundestages:	nicht bekannt
Position des Bundesrates:	nicht bekannt
Position des Europäischen Parlaments:	nicht bekannt
Meinungsstand im Rat:	keine Behandlung durch den Rat
Verfahrensstand: (Stand der Befassung)	
Finanzielle Auswirkungen:	

- 5 -

Zeitplan für die Behandlung im

a) Bundesrat:	nicht bekannt
b) Europäischen Parlament:	nicht bekannt
c) Rat:	nicht bekannt

Dokument 2014/0035967

Von: Spitzer, Patrick, Dr.
Gesendet: Donnerstag, 23. Januar 2014 12:23
An: BMWI BUERO-EA2; AA Oelfke, Christian; AA Kinder, Kristin; AA Wendel, Philipp; BMJ Henrichs, Christoph; BMJ Harms, Katharina; BMJ Deffaa, Ulrich; PGDS_; VI4_; IT1_; OESIII1_
Cc: BMWI Bölhoff, Corinna; 'ref132@bk.bund.de'; BK Rensmann, Michael; Bender, Ulrike; Merz, Jürgen; Schlender, Katharina; Marscholleck, Dietmar; OESI3AG_; Stöber, Karlheinz, Dr.; Weinbrenner, Ulrich; RegOeSI3; Kotira, Jan; Stang, Rüdiger; B3_; Wenske, Martina; Schlender, Katharina
Betreff: WG: Frist 22.01., 17:00 Uhr: Anforderung eines Berichtsbogens zur Unterrichtung des Deutschen Bundestages (17067/13)
Anlagen: 17067.EN13.pdf; 140123_Berichtsb_Rebuilding Trust.doc
Wichtigkeit: Hoch

ÖS I 3-52000/4#1

Liebe Kolleginnen und Kollegen,

für Ihre Anmerkungen möchte ich mich bedanken. Die als Anlage beigefügte fortgeschriebene Fassung des Berichtsbogens übermittele ich zur finalen Durchsicht und mit der Bitte um Mitzeichnung bis heute, **23. Januar 2014, 16:00 Uhr (Verschweigen)**.

Freundliche Grüße

Patrick Spitzer
 (-1390)

Von: Spitzer, Patrick, Dr.
Gesendet: Mittwoch, 22. Januar 2014 12:08
An: BMWI BUERO-EA2; AA Oelfke, Christian; AA Kinder, Kristin; AA Wendel, Philipp; BMJ Henrichs, Christoph; BMJ Harms, Katharina
Cc: PGDS_; VI4_; IT1_; OESIII1_; BMWI Bölhoff, Corinna; 'ref132@bk.bund.de'; BK Rensmann, Michael; Bender, Ulrike; Merz, Jürgen; Schlender, Katharina; Marscholleck, Dietmar; OESI3AG_; Stöber, Karlheinz, Dr.; Weinbrenner, Ulrich; RegOeSI3; Kotira, Jan; Stang, Rüdiger
Betreff: Frist 22.01., 17:00 Uhr: Anforderung eines Berichtsbogens zur Unterrichtung des Deutschen Bundestages (17067/13)
Wichtigkeit: Hoch

ÖS I 3-52000/4#1

Liebe Kolleginnen und Kollegen,

ich bitte um Mitzeichnung zum als **Anlage 1** beigefügten Berichtsbogen zur Unterrichtung des Deutschen Bundestages **bis heute, 22. Januar 2014, 17.00 Uhr** (Rückmeldungen bitte auch an das Postfach oesi3ag@bmi.bund.de). Grundlage der Berichterstattung ist das als **Anlage 2** beigefügte Dokument „Rebuilding Trust in EU US Data Flows“.

Freundliche Grüße

Patrick Spitzer

im Auftrag
Dr. Patrick Spitzer

Bundesministerium des Innern
Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,
BKA-Gesetz, Datenschutz im Sicherheitsbereich)
Alt-Moabit 101D, 10559 Berlin
Telefon: +49 (0)30 18681-1390
E-Mail: patrick.spitzer@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 29 November 2013

17067/13

**JAI 1095
USA 64
DATAPROTECT 190
COTER 154**

COVER NOTE

from: Secretary-General of the European Commission,
signed by Mr Jordi AYET PUIGARNAU, Director

date of receipt: 28 November 2013

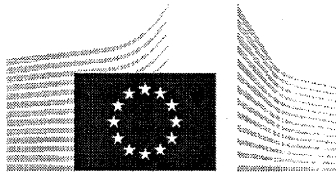
to: Mr Uwe CORSEPIUS, Secretary-General of the Council of the European
Union

No Cion doc.: COM(2013) 846 final

Subject: Communication from the Commission to the European Parliament and the
Council
Rebuilding Trust in EU-US Data Flows

Delegations will find attached Commission document COM(2013) 846 final.

Encl.: COM(2013) 846 final



**EUROPEAN
COMMISSION**

Brussels, 27.11.2013
COM(2013) 846 final

**COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN
PARLIAMENT AND THE COUNCIL**

Rebuilding Trust in EU-US Data Flows

1. INTRODUCTION: THE CHANGING ENVIRONMENT OF EU-US DATA PROCESSING

The European Union and the United States are strategic partners, and this partnership is critical for the promotion of our shared values, our security and our common leadership in global affairs.

However, trust in the partnership has been negatively affected and needs to be restored. The EU, its Member States and European citizens have expressed deep concerns at revelations of large-scale US intelligence collection programmes, in particular as regards the protection of personal data¹. Mass surveillance of private communication, be it of citizens, enterprises or political leaders, is unacceptable.

Transfers of personal data are an important and necessary element of the transatlantic relationship. They form an integral part of commercial exchanges across the Atlantic including for new growing digital businesses, such as social media or cloud computing, with large amounts of data going from the EU to the US. They also constitute a crucial component of EU-US co-operation in the law enforcement field, and of the cooperation between Member States and the US in the field of national security. In order to facilitate data flows, while ensuring a high level of data protection as required under EU law, the US and the EU have put in place a series of agreements and arrangements.

Commercial exchanges are addressed by Decision 2000/520/EC² (hereafter “the Safe Harbour Decision”). This Decision provides a legal basis for transfers of personal data from the EU to companies established in the US which have adhered to the Safe Harbour Privacy Principles.

Exchange of personal data between the EU and the US for the purposes of law enforcement, including the prevention and combating of terrorism and other forms of serious crime, is governed by a number of agreements at EU level. These are the Mutual Legal Assistance Agreement³, the Agreement on the use and transfer of Passenger Name Records (PNR)⁴, the Agreement on the processing and transfer of Financial Messaging Data for the purpose of the Terrorist Finance Tracking Program (TFTP)⁵, and the Agreement between Europol and the US. These Agreements respond to important security challenges and meet the common security interests of the EU and US, whilst providing a high level of protection of personal data. In addition, the EU and the US are currently negotiating a framework agreement on data protection in the field of police and judicial cooperation (“umbrella agreement”)⁶. The aim is to ensure a high level of data protection for citizens whose data is exchanged thereby further

¹ For the purposes of this Communication, references to EU citizens include also non-EU data subjects which fall within the scope of European Union's data protection law.

² Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25.8.2000, p. 7.

³ Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 291, 7.11. 2009, p. 40.

⁴ Council Decision 2012/472/EU of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L 215, 11.8.2012, p. 4.

⁵ Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195, 27.7.2010, p. 3.

⁶ The Council adopted the Decision authorising the Commission to negotiating the Agreement on 3 December 2010. See IP/10/1661 of 3 December 2010.

advancing EU-US cooperation in the combating of crime and terrorism on the basis of shared values and agreed safeguards.

These instruments operate in an environment in which personal data flows are acquiring increasing relevance.

On the one hand, the development of the digital economy has led to exponential growth in the quantity, quality, diversity and nature of data processing activities. The use of electronic communication services by citizens in their daily lives has increased. Personal data has become a highly valuable asset: the estimated value of EU citizens' data was €315bn in 2011 and has the potential to grow to nearly €1tn annually by 2020⁷. The market for the analysis of large sets of data is growing by 40% per year worldwide⁸. Similarly, technological developments, for example related to cloud computing, put into perspective the notion of international data transfer as cross-border data flows are becoming a day to day reality.⁹

The increase in the use of electronic communications and data processing services, including cloud computing, has also substantially expanded the scope and significance of transatlantic data transfers. Elements such as the central position of US companies in the digital economy¹⁰, the transatlantic routing of a large part of electronic communications and the volume of electronic data flows between the EU and the US have become even more relevant. On the other hand, modern methods of personal data processing raise new and important questions. This applies both to new means of large-scale processing of consumer data by private companies for commercial purposes, and to the increased ability of large-scale surveillance of communications data by intelligence agencies.

Large-scale US intelligence collection programmes, such as PRISM affect the fundamental rights of Europeans and, specifically, their right to privacy and to the protection of personal data. These programmes also point to a connection between Government surveillance and the processing of data by private companies, notably by US internet companies. As a result, they may therefore have an economic impact. If citizens are concerned about the large-scale processing of their personal data by private companies or by the surveillance of their data by intelligence agencies when using Internet services, this may affect their trust in the digital economy, with potential negative consequences on growth.

These developments expose EU-US data flows to new challenges. This Communication addresses these challenges. It explores the way forward on the basis of the findings contained in the Report of the EU Co-Chairs of the ad hoc EU-US Working Group and the Communication on the Safe Harbour.

It seeks to provide an effective way forward to rebuild trust and reinforce EU-US cooperation in these fields and strengthen the broader transatlantic relationship.

This Communication is based on the premise that the standard of protection of personal data must be addressed in its proper context, without affecting other dimensions of EU-US relations, including the on-going negotiations for a Transatlantic Trade and Investment Partnership. For this reason, data protection standards will not be negotiated within the Transatlantic Trade and Investment Partnership, which will fully respect the data protection rules.

⁷ See Boston Consulting Group, "The Value of our Digital Identity", November 2012.

⁸ See McKinsey, "Big data: The next frontier for innovation, competition, and productivity", 2011

⁹ Communication on Unleashing the potential of cloud computing in Europe, COM(2012) 529 final

¹⁰ For example, the combined number of unique visitors to Microsoft Hotmail, Google Gmail and Yahoo! Mail from European countries in June 2012 totalled over 227 million, eclipsing that of all other providers. The combined number of unique European users accessing Facebook and Facebook Mobile in March 2012 was 196.5 million, making Facebook the largest social network in Europe. Google is the leading internet search engine with 90.2% of worldwide internet users. US mobile messaging service What's App was used by 91% of iPhone users in Germany in June 2013.

It is important to note that whilst the EU can take action in areas of EU competence, in particular to safeguard the application of EU law¹¹, national security remains the sole responsibility of each Member State¹².

2. THE IMPACT ON THE INSTRUMENTS FOR DATA TRANSFERS

First, as regards data transferred for commercial purposes, the Safe Harbour has proven to be an important vehicle for EU-US data transfers. Its commercial importance has grown as personal data flows have taken on greater prominence in the transatlantic commercial relationship. Over the past 13 years, the Safe Harbour scheme has evolved to include more than 3.000 companies, over half of which have signed up within the last five years. Yet concerns about the level of protection of personal data of EU citizens transferred to the US under the Safe Harbour scheme have grown. The voluntary and declaratory nature of the scheme has sharpened focus on its transparency and enforcement. While a majority of US companies apply its principles, some self-certified companies do not. The non-compliance of some self-certified companies with the Safe Harbour Privacy Principles places such companies at a competitive advantage in relation to European companies operating in the same markets.

Moreover, while under the Safe Harbour, limitations to data protection rules are permitted where necessary on grounds of national security¹³, the question has arisen whether the large-scale collection and processing of personal information under US surveillance programmes is necessary and proportionate to meet the interests of national security. It is also clear from the findings of the ad hoc EU-US Working Group that, under these programmes, EU citizens do not enjoy the same rights and procedural safeguards as Americans.

The reach of these surveillance programmes, combined with the unequal treatment of EU citizens, brings into question the level of protection afforded by the Safe Harbour arrangement. The personal data of EU citizens sent to the US under the Safe Harbour may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the EU and the purposes for which it was transferred to the US. A majority of the US internet companies that appear to be more directly concerned by these programmes are certified under the Safe Harbour scheme.

Second, as regards exchanges of data for law enforcement purposes, the existing Agreements (PNR, TFTP) have proven highly valuable tools to address common security threats linked to serious transnational crime and terrorism, whilst laying down safeguards that ensure a high level of data protection¹⁴. These safeguards extend to EU citizens, and the Agreements provide for mechanisms to review their implementation and to address issues of concern related thereto. The TFTP Agreement also establishes a system of oversight, with EU independent overseers checking how data covered by the Agreement is searched by the US.

Against the backdrop of concerns raised in the EU about US surveillance programmes, the European Commission has used those mechanisms to check how the agreements are applied. In the case of the PNR Agreement, a joint review was conducted, involving data protection

¹¹ See Judgment of the Court of Justice of the European Union in Case C-300/11, ZZ v Secretary of State for the Home Department.

¹² Article 4(2) TEU.

¹³ See e.g. Safe Harbour Decision, Annex I.

¹⁴ See Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data pursuant to Article 6 (6) of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program.

experts from the EU and the US, looking at how the Agreement has been implemented¹⁵. That review did not give any indication that US surveillance programmes extend to or have impact on the passenger data covered by the PNR Agreement. In the case of the TFTP Agreement, the Commission opened formal consultations after allegations were made of US intelligence agencies directly accessing personal data in the EU, contrary to the Agreement. These consultations did not reveal any elements proving a breach of the TFTP Agreement, and they led the US to provide written assurance that no direct data collection has taken place contrary to the provisions of the Agreement.

The large-scale collection and processing of personal information under US surveillance programmes call, however, for a continuation of very close monitoring of the implementation of the PNR and TFTP Agreements in the future. The EU and the US have therefore agreed to advance the next Joint Review of the TFTP Agreement, which will be held in Spring 2014. Within that and future joint reviews, greater transparency will be ensured on how the system of oversight operates and on how it protects the data of EU citizens. In parallel, steps will be taken to ensure that the system of oversight continues to pay close attention to how data transferred to the US under the Agreement is processed, with a focus on how such data is shared between US authorities.

Third, the increase in the volume of processing of personal data underlines the importance of the legal and administrative safeguards that apply. One of the goals of the Ad Hoc EU-US Working Group was to establish what safeguards apply to minimise the impact of the processing on the fundamental rights of EU citizens. Safeguards are also necessary to protect companies. Certain US laws such as the Patriot Act, enable US authorities to directly request companies access to data stored in the EU. Therefore, European companies, and US companies present in the EU, may be required to transfer data to the US in breach of EU and Member States' laws, and are consequently caught between conflicting legal obligations. Legal uncertainty deriving from such direct requests may hold back the development of new digital services, such as cloud computing, which can provide efficient, lower-cost solutions for individuals and businesses.

3. ENSURING THE EFFECTIVENESS OF DATA PROTECTION

Transfers of personal data between the EU and the US are an essential component of the transatlantic commercial relationship. Information sharing is also an essential component of EU-US security cooperation, critically important to the common goal of preventing and combating serious crime and terrorism. However, recent revelations about US intelligence collection programmes have negatively affected the trust on which this cooperation is based. In particular, it has affected trust in the way personal data is processed. The following steps should be taken to restore trust in data transfers for the benefit of the digital economy, security both in the EU and in the US, and the broader transatlantic relationship.

3.1. The EU data protection reform

The data protection reform proposed by the Commission in January 2012¹⁶ provides a key response as regards the protection of personal data. Five components of the proposed Data Protection package are of particular importance.

¹⁵ See on the Commission report "Joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security".

¹⁶ COM(2012) 10 final: Proposal for a Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25.1.2012, and COM(2012) 11 final: Proposal for a Regulation of the European Parliament and the Council on the protection of individuals

First, as regards territorial scope, the proposed regulation makes clear that companies that are not established in the Union will have to apply EU data protection law when they offer goods and services to European consumers or monitor their behaviour. In other words, the fundamental right to data protection will be respected, independently of the geographical location of a company or of its processing facility¹⁷.

Secondly, on international transfers, the proposed regulation establishes the conditions under which data can be transferred outside the EU. Transfers can only be allowed where these conditions, which safeguard the individuals' rights to a high level of protection, are met¹⁸.

Thirdly, concerning enforcement, the proposed rules provide for proportionate and dissuasive sanctions (up to 2% of a company's annual global turnover) to make sure that companies comply with EU law¹⁹. The existence of credible sanctions will increase companies' incentive to comply with EU law.

Fourthly, the proposed regulation includes clear rules on the obligations and liabilities of data processors such as cloud providers, including on security²⁰. As the revelations about US intelligence collection programmes have shown, this is critical because these programmes affect data stored in the cloud. Also, companies providing storage space in the cloud which are asked to provide personal data to foreign authorities will not be able to escape their responsibility by reference to their status as data processors rather than data controllers.

Fifth, the package will lead to the establishment of comprehensive rules for the protection of personal data processed in the law enforcement sector.

It is expected that the package will be agreed upon in a timely manner in the course of 2014²¹.

3.2. Making Safe Harbour safer

The Safe Harbour scheme is an important component of the EU-US commercial relationship, relied upon by companies on both sides of the Atlantic.

The Commission's report on the functioning of Safe Harbour has identified a number of weaknesses in the scheme. As a result of a lack of transparency and of enforcement, some self-certified Safe Harbour members do not, in practice, comply with its principles. This has a negative impact on EU citizens' fundamental rights. It also creates a disadvantage for European companies compared to those competing US companies that are operating under the scheme but in practice not applying its principles. This weakness also affects the majority of US companies which properly apply the scheme. Safe Harbour also acts as a conduit for the

with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

¹⁷ The Commission takes note that the European Parliament confirmed and strengthened this important principle, enshrined in Art. 3 of the proposed Regulation, in its vote of 21 October 2013 on the data protection reform reports of MEPs Jan-Philipp Albrecht and Dimitrios Droutsas in the Committee for Civil Liberties, Justice and Home Affairs (LIBE).

¹⁸ The Commission takes note that in its vote of 21 October 2013, the LIBE Committee of the European Parliament proposed to include a provision in the future Regulation that would subject requests from foreign authorities to access personal data collected in the EU to the obtaining of a prior authorisation from a national data protection authority, where such a request would be issued outside a mutual legal assistance treaty or another international agreement.

¹⁹ The Commission takes note that in its vote of 21 October 2013, the LIBE Committee proposed strengthening the Commission's proposal by providing that fines can go up to 5% of the annual worldwide turnover of a company.

²⁰ The Commission takes note that in its vote of 21 October 2013, the LIBE Committee endorsed the strengthening of the obligations and liabilities of data processors, in the particular with regard to Art. 26 of the proposed Regulation.

²¹ The Conclusions of the October 2013 European Council state that: "It is important to foster the trust of citizens and businesses in the digital economy. The timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015".

transfer of the personal data of EU citizens from the EU to the US by companies required to surrender data to US intelligence agencies under the US intelligence collection programmes. Unless the deficiencies are corrected, it therefore constitutes a competitive disadvantage for EU business and has a negative impact on the fundamental right to data protection of EU citizens.

The shortcomings of the Safe Harbour scheme have been underlined by the response of European Data Protection Authorities to the recent surveillance revelations. Article 3 of the Safe Harbour Decision authorises these authorities to suspend, under certain conditions, data flows to certified companies.²² German data protection commissioners have decided not to issue new permissions for data transfers to non-EU countries (for example for the use of certain cloud services). They will also examine whether data transfers on the basis of the Safe Harbour should be suspended.²³ The risk is that such measures, taken at national level, would create differences in coverage, which means that Safe Harbour would cease to be a core mechanism for the transfer of personal data between the EU and the US.

The Commission has the authority under Directive 95/46/EC to suspend or revoke the Safe Harbour decision if the scheme no longer provides an adequate level of protection. Furthermore, Article 3 of the Safe Harbour Decision provides that the Commission may reverse, suspend or limit the scope of the decision, while, under article 4, it may adapt the decision at any time in the light of experience with its implementation.

Against this background, a number of policy options can be considered, including:

- Maintaining the *status quo*;
- Strengthening the Safe Harbour scheme and reviewing its functioning thoroughly;
- Suspending or revoking the Safe Harbour decision.

Given the weaknesses identified, the current implementation of Safe Harbour cannot be maintained. However, its revocation would adversely affect the interests of member companies in the EU and in the US. The Commission considers that Safe Harbour should rather be strengthened.

The improvements should address both the structural shortcomings related to transparency and enforcement, the substantive Safe Harbour principles and the operation of the national security exception.

More specifically, for Safe Harbour to work as intended, the monitoring and supervision by US authorities of the compliance of certified companies with the Safe Harbour Privacy Principles needs to be more effective and systematic. The transparency of certified companies' privacy policies needs to be improved. The availability and affordability of dispute resolution mechanisms also needs to be ensured to EU citizens.

As a matter of urgency, the Commission will engage with the US authorities to discuss the shortcomings identified. Remedies should be identified by summer 2014 and implemented as soon as possible. On the basis thereof, the Commission will undertake a complete stock taking of the functioning of the Safe Harbour. This broader review process should involve open consultation and a debate in the European Parliament and the Council as well as discussions with the US authorities.

²² Specifically, pursuant to Art. 3 of the Safe Harbour Decision, such suspensions may take place in cases where there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

²³ Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, press release of 24 July 2013.

It is also important that the national security exception foreseen by the Safe Harbour Decision, is used only to an extent that is strictly necessary and proportionate.

3.3. Strengthening data protection safeguards in law enforcement cooperation

The EU and the US are currently negotiating a data protection “umbrella” agreement on transfers and processing of personal information in the context of police and judicial co-operation in criminal matters. The conclusion of such an agreement providing for a high level of protection of personal data would represent a major contribution to strengthening trust across the Atlantic. By advancing the protection of EU data citizens' rights, it would help strengthen transatlantic cooperation aimed at preventing and combating crime and terrorism.

According to the decision authorising the Commission to negotiate the umbrella agreement, the aim of the negotiations should be to ensure a high level of protection in line with the EU data protection *acquis*. This should be reflected in agreed rules and safeguards on, *inter alia*, purpose limitation, the conditions and the duration of the retention of data. In the context of the negotiation, the Commission should also obtain commitments on enforceable rights including judicial redress mechanisms for EU citizens not resident in the US²⁴. Close EU-US cooperation to address common security challenges should be mirrored by efforts to ensure that citizens benefit from the same rights when the same data is processed for the same purposes on both sides of the Atlantic. It is also important that derogations based on national security needs are narrowly defined. Safeguards and limitations should be agreed in this respect.

These negotiations provide an opportunity to clarify that personal data held by private companies and located in the EU will not be directly accessed by or transferred to US law enforcement authorities outside of formal channels of co-operation, such as Mutual Legal Assistance agreements or sectoral EU-US Agreements authorising such transfers. Access by other means should be excluded, unless it takes place in clearly defined, exceptional and judicially reviewable situations. The US should undertake commitments in that regard²⁵.

An "umbrella agreement" agreed along those lines, should provide the general framework to ensure a high level of protection of personal data when transferred to the US for the purpose of preventing or combating crime and terrorism. Sectoral agreements should, where necessary due to the nature of the data transfer concerned, lay down additional rules and safeguards, building on the example of the EU-US PNR and TFTP Agreements, which set strict conditions for transfer of data and safeguards for EU citizens.

²⁴ See the relevant passage of the Joint Press Statement following the EU-US-Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington: "We are therefore, as a matter of urgency, committed to advancing rapidly in the negotiations on a meaningful and comprehensive data protection umbrella agreement in the field of law enforcement. The agreement would act as a basis to facilitate transfers of data in the context of police and judicial cooperation in criminal matters by ensuring a high level of personal data protection for U.S. and EU citizens. We are committed to working to resolve the remaining issues raised by both sides, including judicial redress (a critical issue for the EU). Our aim is to complete the negotiations on the agreement ahead of summer 2014."

²⁵ See the relevant passage of the Joint Press Statement following the EU-US Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington: "We also underline the value of the EU-U.S. Mutual Legal Assistance Agreement. We reiterate our commitment to ensure that it is used broadly and effectively for evidence purposes in criminal proceedings. There were also discussions on the need to clarify that personal data held by private entities in the territory of the other party will not be accessed by law enforcement agencies outside of legally authorized channels. We also agree to review the functioning of the Mutual Legal Assistance Agreement, as contemplated in the Agreement, and to consult each other whenever needed."

3.4. Addressing European concerns in the on-going US reform process

US President Obama has announced a review of US national security authorities' activities, including of the applicable legal framework. This on-going process provides an important opportunity to address EU concerns raised by recent revelations about US intelligence collection programmes. The most important changes would be extending the safeguards available to US citizens and residents to EU citizens not resident in the US, increased transparency of intelligence activities, and further strengthening oversight. Such changes would restore trust in EU-US data exchanges, and promote the use of Internet services by Europeans.

With respect to extending the safeguards available to US citizens and residents to EU citizens, legal standards in relation to US surveillance programmes which treat US and EU citizens differently should be reviewed, including from the perspective of necessity and proportionality, keeping in mind the close transatlantic security partnership based on common values, rights and freedoms. This would reduce the extent to which Europeans are affected by US intelligence collection programmes.

More transparency is needed on the legal framework of US intelligence collection programmes and its interpretation by US Courts as well as on the quantitative dimension of US intelligence collection programmes. EU citizens would also benefit from such changes.

The oversight of US intelligence collection programmes would be improved by strengthening the role of the Foreign Intelligence Surveillance Court and by introducing remedies for individuals. These mechanisms could reduce the processing of personal data of Europeans that are not relevant for national security purposes.

3.5. Promoting privacy standards internationally

Issues raised by modern methods of data protection are not limited to data transfer between the EU and the US. A high level of protection of personal data should also be guaranteed to any individual. EU rules on collection, processing and transfer of data should be promoted internationally.

Recently, a number of initiatives have been proposed to promote the protection of privacy, particularly on the internet²⁶. The EU should ensure that such initiatives, if pursued, fully take into account the principles of protecting fundamental rights, freedom of expression, personal data and privacy as set out in EU law and in the EU Cyber Security Strategy, and do not undermine the freedom, openness and security of cyber space. This includes a democratic and efficient multi stakeholder governance model.

The on-going reforms of data protection laws on both sides of the Atlantic also provide the EU and the US a unique opportunity to set the standard internationally. Data exchanges across the Atlantic and beyond would greatly benefit from the strengthening of the US domestic legal framework, including the passage of the "Consumer Privacy Bill of Rights" announced by President Obama in February 2012 as part of a comprehensive blueprint to improve consumers' privacy protections. The existence of a set of strong and enforceable data protection rules enshrined in both the EU and the US would constitute a solid basis for cross-border data flows.

In view of promoting privacy standards internationally, accession to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), which is open to countries which are not member of the Council of Europe²⁷, should also be favoured. Safeguards and guarantees agreed in international fora should result in a high level of protection compatible with what is required under EU law.

²⁶ See in this respect the draft resolution proposed to the UN General Assembly by Germany and Brazil – calling for the protection of privacy online as offline.

²⁷ The US is already party to another Council of Europe convention: the 2001 Convention on Cybercrime (also known as the "Budapest Convention").

4. CONCLUSIONS AND RECOMMENDATIONS

The issues identified in this Communication require action to be taken by the US as well as by the EU and its Member States.

The concerns around transatlantic data exchanges are, first of all, a wake-up call for the EU and its Member States to advance swiftly and with ambition on the data protection reform. It shows that a strong legislative framework with clear rules that are enforceable also in situations when data are transferred abroad is, more than ever, a necessity. The EU institutions should therefore continue working towards the adoption of the EU data protection reform by spring 2014, to make sure that personal data is effectively and comprehensively protected.

Given the significance of transatlantic data flows, it is essential that the instruments on which these exchanges are based appropriately address the challenges and opportunities of the digital era and new technological developments like cloud computing. Existing and future arrangements and agreements should ensure that the continuity of a high level of protection is guaranteed over the Atlantic.

A robust Safe Harbour scheme is in the interests of EU and US citizens and companies. It should be strengthened by better monitoring and implementation in the short term, and, on this basis, by a broader review of its functioning. Improvements are necessary to ensure that the original objectives of the Safe Harbour Decision – i.e. continuity of data protection, legal certainty and free EU-US flow of data – are still met.

These improvements should focus on the need for the US authorities to better supervise and monitor the compliance of self-certified companies with the Safe Harbour Privacy Principles. It is also important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary and proportionate.

In the area of law enforcement, the current negotiations of an “umbrella agreement” should result in a high level of protection for citizens on both sides of the Atlantic. Such an agreement would strengthen the trust of Europeans in EU-US data exchanges, and provide a basis to further develop EU-US security cooperation and partnership. In the context of the negotiation, commitments should be secured to the effect that procedural safeguards, including judicial redress, are available to Europeans who are not resident in the US.

Commitments should be sought from the US administration to ensure that personal data held by private entities in the EU will not be accessed directly by US law enforcement agencies outside of formal channels of co-operation, such as Mutual Legal Assistance agreements and sectoral EU-US Agreements such as PNR and TFTP authorising such transfers under strict conditions, except in clearly defined, exceptional and judicially reviewable situations.

The US should also extend the safeguards available to US citizens and residents to EU citizens not resident in the US, ensure the necessity and proportionality of the programmes, greater transparency and oversight in the legal framework applicable to US national security authorities.

Areas listed in this communication will require constructive engagement from both sides of the Atlantic. Together, as strategic partners, the EU and the US have the ability to overcome the current tensions in the transatlantic relationship and rebuild trust in EU-US data flows. Undertaking joint political and legal commitments on further cooperation in these areas will strengthen the overall transatlantic relationship.

B E R I C H T S B O G E N

gemäß Anlage zu § 6 Absatz 2 EUZBBG und Ziffer II. 3. der Anlage zu § 9 EUZBLG

Ressort/Referat:	AG ÖS I 3	Datum:	20.01.2014
Referatsleiterin/ Referatsleiter:	MinR Weinbrenner MinR Taube	Telefon:	030 186811300
Bearbeiterin/ Bearbeiter:	RR Dr. Spitzer	Telefon:	030 186811390
abgestimmt mit:	BMJV; BMWi, AA	Telefax:	

Thema:	Mitteilung der Kommission an das Europäische Parlament und den Rat über die Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA
Sachgebiet:	Europäische Justiz- und Innenpolitik
Ratsdok.-Nummer:	17067/13
KOM-Nummer:	COM(2013) 846 final
Nummer des interinstitutionellen Dossiers:	nicht bekannt
Nummer der Bundesratsdrucksache:	nicht bekannt
Nachweis der Zulässigkeit für europäische Regelungen: (Prüfung der Rechtsgrundlage)	entfällt, da kein Rechtsakt
Subsidiaritätsprüfung:	entfällt, da kein Rechtsakt
Verhältnismäßigkeitsprüfung:	entfällt, da kein Rechtsakt
Zielsetzung:	Ausarbeitung von Maßnahmen zur Berücksichtigung beim Datenaustausch zwischen den USA und der EU vor dem Hintergrund der Veröffentlichungen zur Überwachungstätigkeit der NSA.
Inhaltliche Schwerpunkte:	Die Mitteilung ist ein politisches Strategiepapier über die transatlantischen Datenströme, in dem die sich aus den Enthüllungen über die umfangreichen Programme der US-Nachrichtendienste zur Sammlung von Informationen ergebenden Herausforderungen und Risiken aus Sicht der KOM beschrieben und die nach Auffassung der KOM erforderlichen Maßnahmen zur Ausräumung der genannten

- 2 -

Bedenken dargelegt werden. Das Papier fasst verschiedene weitere Veröffentlichungen der EU zu Einzelthemen, wie die Analyse über die Funktionsweise des „Safe Harbor Abkommens“ und den Bericht über das TFTP-Abkommen (auch SWIFT-Abkommen genannt), zusammen.

Folgende Maßnahmen werden von der KOM aufgegriffen:

Datenschutzreformpaket

KOM sieht das von ihr Anfang 2012 vorgeschlagene Datenschutzreformpaket als ein Schlüsselement in Bezug auf den Schutz personenbezogener Daten an. Als Begründung werden fünf Elemente, die aus ihrer Sicht insoweit entscheidend sind, angeführt: das Marktortprinzip, Regelungen zu Drittstaatenübermittlungen, Sanktionen (u.a. von Cloud-Anbietern), Regelungen zu Verantwortlichkeiten und die Regelungen im Bereich Polizei und Justiz.

Verbesserung von Safe Harbor

KOM identifiziert als Schwachstellen der Safe-Harbor-Regelung Defizite bei der Transparenz und der Durchsetzung der Vereinbarung (insbesondere Inhalt und Veröffentlichung der Datenschutzerklärung der Safe-Harbor-registrierten Unternehmen, Verfügbarkeit alternativer Konfliktlösungsmechanismen für EU-Bürger, Durchsetzung durch die zuständigen US-Behörden, Zugang zu den Daten durch US-Sicherheitsbehörden) und gibt Empfehlungen zur verbesserten Umsetzung von Safe Harbor ab. Darüber hinaus kündigt KOM Gespräche mit der US-Regierung an, die der gemeinsamen Identifizierung von Schwachstellen und deren Abhilfe bis Sommer 2014 dienen sollen.

Abschluss eines EU-US Datenschutzabkommens

KOM strebt den Abschluss eines Rahmenabkommens zum Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen an. Ein solches Abkommen solle den Rahmen für eine möglichst hohes Datenschutzniveau vorgeben und u.a. auch für einen effektiven Rechtsschutz für EU-Bürger außerhalb der USA geben und ggf. durch bereits bestehende fachspezifische Einzelabkommen, wie bspw. das EU-US PNR- und das TFTP-Abkommen ergänzt werden.

Berücksichtigung von EU-Interessen im laufenden US-Reformprozess

Die von US-Präsident Obama initiierte Evaluierung der US-Sicherheitsbehörden soll genutzt werden, um eine Anhebung der Standards für EU-Bürger zu erreichen. Die Mitteilung spricht u.a. die Ungleichbehandlung von US- und EU-Bürgern, unterschiedliche Auffassungen über die Auslegung des Verhältnismäßigkeitsgrundsatzes und die mangelnden Rechtsschutzmöglichkeiten für EU-Bürger in

- 3 -

	den USA als zentrale Punkte an.
Politische Bedeutung:	Die politische Bedeutung ist vor dem Hintergrund der andauernden Veröffentlichungen zu Aktivitäten amerikanischer Nachrichtendienste und der öffentlichen Diskussion in DEU, im EP und auf internationaler Ebene als sehr hoch zu bewerten.
Was ist das besondere deutsche Interesse?	<p>Aufgrund der unmittelbaren Betroffenheit Deutschlands durch die in den Veröffentlichungen Edward Snowdens dargelegten Aktivitäten und dem hohen Maß öffentlicher Aufmerksamkeit besteht an allen diesbezüglichen Maßnahmen/Empfehlungen grundsätzlich ein besonderes Interesse. In anderen EU-Mitgliedstaaten ist dies nicht im gleichen Maß der Fall. Generell ist zu beachten, dass die EU zwar eine Kompetenz für den Datenschutz, nicht jedoch für die Tätigkeit der Nachrichtendienste hat. Im Einzelnen:</p> <p><u>Datenschutzreformpaket</u></p> <p>Der dargestellte Zusammenhang zwischen den Überwachungsmaßnahmen und der Datenschutz-Grundverordnung (DSGVO) vermag nur teilweise zu überzeugen. Zutreffend ist, dass das Marktortprinzip zu einer Verbesserung des Datenschutzes im transatlantischen Verhältnis beitragen dürfte, weil US-Unternehmen in Europa unmittelbar an EU-Recht gebunden werden können. Bei den Drittstaatenregelungen ist zu differenzieren. Allgemein dürften die von der KOM vorgeschlagenen Regelungen kaum zu einer wesentlichen Verbesserung führen. Dies gilt insbesondere für Übermittlungen von Unternehmen an US-Behörden. Hierzu hatte DEU einen neuen Art. 42a vorgeschlagen, der besondere Anforderungen an die Übermittlung von Daten an Behörden und Gerichte in Drittstaaten stellt. Die bisher formulierten Anforderungen an die Übermittlung personenbezogener Daten in Drittstaaten werden jedenfalls der technischen Entwicklung und Vernetzung noch nicht gerecht. So bleiben insbesondere zentrale Fragen der Übermittlung, z.B. beim „Cloud computing“, ungelöst. Zu begrüßen ist, dass die KOM Ideen der US-Seite erwähnt, die das Weiße Haus in seinem Papier „Consumer Data Privacy in a Networked World („Consumer Bill of Rights“) im Februar 2012 entwickelt hat. Allerdings lässt KOM offen, wie sich diese Ideen in die DSGVO inkorporieren lassen. Die Datenschutzrichtlinie enthält zwar Regelungen für die Datenübermittlung an Drittstaaten und macht grundsätzlich ein angemessenes Datenschutzniveau zur Übermittlungsbedingung. Sie kann aber das Datenschutzniveau in den USA nicht beeinflussen.</p> <p><u>Safe Harbor</u></p> <p>Die Bundesregierung hat sich wiederholt für eine Verbesserung und Nachverhandlung der Safe-Harbor-Regelung ausgesprochen. Sie unterstützt die Vorschläge der KOM zur Verbesserung von Safe Harbor. Darüber hinaus setzt</p>

- 4 -

	<p>sie sich dafür ein, für Modelle wie Safe Harbor in der europäischen Datenschutz-Grundverordnung einen robusten Rechtsrahmen mit klaren Vorgaben für Garantien der Bürgerinnen und Bürger zu schaffen und hat dies auch in die Verhandlungen in der Ratsarbeitsgruppe DAPIX eingebracht. Ziel ist es, die Individualrechte der Bürgerinnen und Bürger zu stärken und ihnen bessere Rechtsschutzmöglichkeiten zur Verfügung zu stellen, die Registrierung der Unternehmen in der EU vorzunehmen und die staatliche Kontrolle seitens der EU-Datenschutzaufsichtsbehörden in Modellen wie Safe-Harbor zu stärken.</p> <p><u>EU-US-Datenschutzabkommen</u></p> <p>Deutschland hat sich für einen baldigen Abschluss des Abkommens unter der Voraussetzung, dass damit mit Blick auf den Schutz personenbezogener Daten und den Individualrechtsschutz ein wirklicher Mehrwert geschaffen wird, ausgesprochen.</p> <p>Bislang haben sich die Verhandlungen schwierig gestaltet. In wichtigen Punkten herrscht weiterhin keine Einigkeit so bei der Speicherdauer, der unabhängigen Aufsicht, den Individualrechten und dem Rechtsschutz. Auch wollen die USA weiterhin das Abkommen als sog. „executive agreement“ abschließen; ein solches muss nicht vom Kongress ratifiziert werden, hat aber auch nur eingeschränkte rechtliche Wirkung. Bei EU/US Justice and Home Affairs Ministerial Treffen am 18.11.2013 haben beide Seiten das Ziel bekräftigt, die Verhandlungen bis zum Sommer 2014 abzuschließen.</p> <p><u>Berücksichtigung von EU-Interessen im laufenden US-Reformprozess</u></p> <p>Deutschland hat sich auch auf EU-Ebene in den Prozess zur Aufklärung des Sachverhalts im Zusammenhang mit den Veröffentlichungen von Edward Snowden und zur Erarbeitung konkreter Empfehlungen der EU und der MS zur Berücksichtigung in der laufenden US-internen Evaluierung der Überwachungsprogramme intensiv eingebracht. Ein Dokument der EU und der MS mit Vorschlägen zur Anwendung des Verhältnismäßigkeitsprinzips, zum verbesserten Individualrechtsschutz und zur Gleichstellung von EU- und US-Bürgern wurde am 6. Dezember 2013 im Rahmen des JI- Ministerrats in Brüssel behandelt.</p>
bisherige Position des Deutschen Bundestages:	nicht bekannt
Position des Bundesrates:	nicht bekannt
Position des Europäischen Parlaments:	Bislang noch keine formale EP-Befassung mit der Mitteilung.
Meinungsstand im Rat:	keine Behandlung durch den Rat

- 5 -

Verfahrensstand: (Stand der Befassung)	
Finanzielle Auswirkungen:	

Zeitplan für die Behandlung im

a) Bundesrat:	nicht bekannt
b) Europäischen Parlament:	nicht bekannt
c) Rat:	nicht bekannt

Dokument 2014/0068742

Von: Spitzer, Patrick, Dr.
Gesendet: Montag, 10. Februar 2014 17:18
An: RegOeSI3
Betreff: WG: EU-AL am 13.02.; hier: Einladung und Anforderung der Beiträge
Anlagen: 140213 EKR EU-AL Einladung.pdf; 140210_EUAL_TOP2_fin.doc

Bitt z Vg OesI3-52000/4#1
Gruß

Patrick Spitzer

Von: Spitzer, Patrick, Dr.
Gesendet: Montag, 10. Februar 2014 17:09
An: Treber, Petra
Cc: GII2_; OESI3AG_; Weinbrenner, Ulrich; Taube, Matthias; Schlender, Katharina; Papenkort, Katja, Dr.
Betreff: WG: EU-AL am 13.02.; hier: Einladung und Anforderung der Beiträge

Liebe Frau Treber,

anbei nun auch Teil 2 der Vorbereitung (Anlage). Hinweis: Billigung durch AL V steht noch aus. Sie wird, sobald sie vorliegt, nachgereicht. Ich bitte deshalb, von einer Übersendung an die Ressorts vorerst abzusehen.

Freundliche Grüße

Patrick Spitzer
(-1390)

Von: Lesser, Ralf
Gesendet: Montag, 10. Februar 2014 16:50
An: GII2_; Treber, Petra
Cc: OESI3AG_; RegOeSI3; Weinbrenner, Ulrich; Taube, Matthias; Spitzer, Patrick, Dr.
Betreff: WG: EU-AL am 13.02.; hier: Einladung und Anforderung der Beiträge

Liebe Frau Treber,

beigefügt übersende ich Ihnen einen Teil der Vorbereitung für TOP 2 betreffend das EU-US-Datenschutzabkommen. Ich erinnere nochmals daran, dass die Einladung des AA an dieser Stelle äußerst missverständlich formuliert ist (siehe bereits meine Mail anbei) und sich unter TOP 2 zwei weitestgehend unabhängige Themen wiederfinden. Mein Kollege Herr Dr. Spitzer wird Ihnen die Vorbereitung für den zweiten Gesprächsteil gesondert zukommen lassen.

Beste Grüße
Ralf Lesser

im Auftrag

Ralf Lesser, LL.M.
Bundesministerium des Innern

Arbeitsgruppe ÖS I 3 (Polizeiliches Informationswesen,
BKA-Gesetz, Datenschutz im Sicherheitsbereich)

Alt-Moabit 101D, 10559 Berlin

Telefon: +49 (0)30 18681-1998

E-Mail: ralf.lesser@bmi.bund.de, oesi3ag@bmi.bund.de

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

Von: Jergl, Johann

Gesendet: Dienstag, 4. Februar 2014 15:34

An: Lesser, Ralf

Cc: Weinbrenner, Ulrich; Spitzer, Patrick, Dr.

Betreff: WG: EU-AL am 13.02.; hier: Einladung und Anforderung der Beiträge

Aus der Referatspost z.w.V. (Übersendung eines Vermerks, TOP 2: Datenschutz EU-USA). Haben wir weitere Themen?

Viele Grüße,

Johann Jergl

AG ÖS I 3, Tel. -1767

Von: GII2_

Gesendet: Dienstag, 4. Februar 2014 14:40

An: OESI3AG_; Arhelger, Roland; RegGII2; B3_; B4_; D1_; GII1_; GII3_; GII4_; GII5_; IT1_; IT3_; KM1_; MI5_; O1_; OESI4_; SP2_; SP6_; VI4_; ZI2_

Cc: OESII1_; PGDS_; GII2_

Betreff: EU-AL am 13.02.; hier: Einladung und Anforderung der Beiträge

GII2-20200/3#11

Hiermit übersende ich die Tagesordnung für o. g. Sitzung mit der Bitte um Kenntnisnahme.

Sollten aus Ihrer Sicht **dringender Gesprächsbedarf** zu **weiteren Themen** bestehen, bitte ich

bis Freitag, 7.2.2014 - 15:00 Uhr um Mitteilung (mit kurzer Begründung) an Referatspostfach G II 2.

Die Grundsatz- und Koordinierungsreferate bitte ich hier um Abfrage in der Abteilung. Fehlanzeige ist **nicht** erforderlich.

Gleichzeitig bitte ich um Übermittlung eines Vermerks (Anlage Formatvorlage) wie nachstehend aufgeführt:

VI 4	Top 1 Bankenunion Top 6 Monitoring VVW und RL-Umsetzung
ÖS I 3 unter Beteiligung von ÖS II 1 und PG DS	Top 2 Datenschutz EU-USA
G II 2, H. Arhelger	Top 9 Verschiedenes (iii) (ggf.) Dt.-brit. EStS-Konsultationen

Bitte senden Sie Ihren Beitrag **bis spätestens Montag, 10.2.2014 – 17:00 Uhr** an das Referatspostfach G II 2.

Mit freundlichem Gruß
i. A. Petra Treber
Referat G II 2
Tel: 2402

2) RegGII2: z.Vg. (Anlagen nicht gesondert)

Von: EKR-S Scholz, Sandra Maria [<mailto:ekr-s@auswaertiges-amt.de>]

Gesendet: Montag, 3. Februar 2014 14:52

An: zzzzz EKR EU-AL-EXTERN (extern)

Cc: EKR-L Schieb, Thomas; AA Brökelmann, Sebastian

Betreff: EU-AL am 13.02. -- hier: Einladung

Sehr geehrte Damen und Herren,

anbei erhalten Sie die Einladung zur nächsten Sitzung der EU-Abteilungsleiter am 13. Februar 2014, die um 8:30 Uhr im Auswärtigen Amt stattfinden wird.

Über eine Rückmeldung bezüglich Ihrer Teilnahme bis zum 11. Februar würde ich mich sehr freuen.

Mit freundlichen Grüßen

Sandra Scholz

EU-Koordinierungsreferat
Auswärtiges Amt
Werderscher Markt 1
10117 Berlin

Tel.: +49-(0)30-1817-2336

Fax: +49-(0)30-1817-52336

E-Mail: ekr-s@auswaertiges-amt.de



Auswärtiges Amt

Ministerialdirigent
Arndt Freytag von Loringhoven
- Stellvertretender Leiter der Europaabteilung -

Werderscher Markt 1
11013 Berlin
Telefon (01888) 17 - 2580
Telefon Sekretariat: (01888) 17 - 2336
Telefax Sekretariat: (01888) 17 - 4175
E-Mail: E-D@auswaertiges-amt.de

Bundesministerium
für Wirtschaft
und Technologie

Ministerialdirektorin
Claudia Dörr-Voß
- Leiterin der Europaabteilung -

Scharnhorststr. 34-37
10115 Berlin
Telefon (01888) 2014 - 7720
Telefon Sekretariat: (01888) 2014-7721
Telefax Sekretariat: (01888) 2014-5481
E-Mail: claudia.doerr-voss@bmwi.bund.de

Nur per E-Mail

Berlin, den 3. Februar 2014

Herrn MDg Dr. Franz Neueder, Abtlg. 5, BKAm
Herrn MD Thomas Westphal, Leiter Abtlg. E, BMF
Herrn MD Dr. Jörg Bentmann, Abtlg. G, BMI
Herrn MDg Klaus Jörg Meyer-Cabri van Amelrode, Leiter EU-Koordination, BMJV
Herrn MD Heinz Koller, Leiter Abtlg. VI, BMAS
Herrn MD Dr. Dietrich Guth, Leiter Abtlg. 6, BMEL
Herrn Udo Scholten, Leiter Unterabtlg. Z3, BMG
Herrn MDg Franzjosef Schafhausen, Leiter Abtlg. KI, BMUB
Herrn MR Dr. Veit Steinle, Leiter der Abteilung UI, BMVI
Herrn MD Volker Rieke, Leiter Abtlg. 2, BMBF
Frau MR'in Dr. Uta Böllhoff, Leiterin Abtlg. 4, BMZ
Herrn MD Uwe Spindeldreier, Leiter Abtlg. 3, BPA
Herrn MDg Christoph Linzbach, Leiter Unterabtlg. 31, BMFSFJ
Herrn Dr. Ulrich Stefan Schlie, AL Pol, BMVg
Herrn Dr. Günter Winands, BKM
Herrn Botschafter Peter Tempel, StäV Brüssel
Herrn Botschafter Dr. Guido Peruzzo, StäV Brüssel

nachrichtlich:

BKAm	z.Hd. Herrn VLR I Georg Felsheim
AA	z.Hd. Herrn VLR I Thomas Schieb
BMWi	z.Hd. Herrn MR Klaus-Peter Leier
BMF	z.Hd. Herrn MR Ralph Müller
BMI	z.Hd. Herrn RD Dr. Christoph Hübner
BMAS	z.Hd. Herrn MR Holger Winkler
BMEL	z.Hd. Herrn MR Rolf Burbach
BMVg	z.Hd. Herrn KzS Axel Deertz
BMFSFJ	z.Hd. Frau Nicole Elping
BMG	z.Hd. Frau Birte Langbein
BMUB	z.Hd. Frau RD'in Dr. Eva Kracht
BMVI	z. Hd. Frau RD'in Heike Seefried
BMBF	z.Hd. Herr MR Andreas Drechsler
BMZ	z.Hd. Herrn RD Bernd Gruschinski
BKM	z.Hd. Frau MR'in Elisabeth Gorecki-Schöberl
BPA	z.Hd. Herrn MR Ulrich Köhn
StäV	z.Hd. Herrn BR I Robert Dieter/ Herrn OAR Werner Langhals

Betr.: Koordinierung der Europapolitik innerhalb der Bundesregierung

Sehr geehrte Kolleginnen und Kollegen,

wir laden Sie hiermit zu einer Besprechung zur Koordinierung der Europapolitik ein am

Donnerstag, den 13. Februar, um 08:30 Uhr
im AA, Saal des 20. Juli (Raum 1.12.13, Erdgeschoss Neubau).

Für die **Bonner Ressorts** besteht die Möglichkeit, im BMBF, Heinemannstr. 2, 53175 Bonn, Haus A/2, Raum 1315 per Videokonferenz an der Besprechung teilzunehmen.

Folgende Tagesordnungspunkte sind vorgesehen:

1. Bankenunion

Ziel: Beratung des weiteren Vorgehens

Verhandlungen - im Rahmen des Trilogs - zur VO über den Einheitlichen Abwicklungsmechanismus sowie über den völkerrechtlichen Vertrag (IGA) zum Einheitlichen Abwicklungsfonds dauern an. Weiteres Thema: Kommission hat am 29.01. Vorschlag zu einem Trennbankensystem vorgelegt.

BMF wird gebeten vorzutragen.

2. Datenschutz EU-USA

Ziel: Festlegung/Bekräftigung der Position der Bundesregierung

Verhandlungen zum Datenschutz-Rahmenabkommen sollen bis Sommer 2014 abgeschlossen werden. EU-US-Ministertreffen in Athen am 25./26.02. terminiert. Erörterung möglicher Implikationen für SWIFT-Abkommen und Safe-Harbor-Vereinbarung. Außerdem sollen mögliche Auswirkungen auf die TTIP-Verhandlungen kurz beleuchtet werden.

BMI wird gebeten vorzutragen, andere Ressorts ergänzen ggf.

3. ETS-Luftverkehr

Ziel: Beratung des weiteren Vorgehens

KOM-Vorschlag für Revision der ETS-RL mit Luftraumansatz findet Zustimmung des EP, aber keine Mehrheit im Rat. BReg gemeinsam mit FRA und GBR für Fortsetzung von „Stop the clock“ bis mind. 2016. Trilog muss bis April (EP-Plenung vrrs. 02.04.) abgeschlossen sein.

BMUB und BMVI tragen vor.

4. Rahmen für Klima- und Energiepolitik 2030

Ziel: Beratung des weiteren Vorgehens

KOM hat am 21.01. Rahmen für Klima- und Energiepolitik bis 2030 vorgelegt. März-ER soll politische Optionen erörtern. RSF bei Umweltrat (03.03.) und Energierat (04.03.) vorgese-

hen. Angesichts heterogenen Meinungsbildes im Rat schwierige Abstimmung der RSF zu erwarten.

BMUB und BMWi tragen vor.

5. Europäisches Semester / Umsetzung länderspezifischer Empfehlungen

Ziel: Information über die Umsetzung der länderspezifischen Empfehlungen (LSE) in DEU sowie zu Verfahren und Zeitplan

Gem. Auftrag der EStS sollen EUAL ab sofort regelmäßiges Monitoring der Umsetzung der LSE vornehmen. Ggf. Einigung auf entsprechendes Verfahren.

BMWi trägt vor, andere Ressorts ergänzen ggf.

6. Monitoring Vertragsverletzungsverfahren und Richtlinien-Umsetzung

Ziel: Übersicht über aktuelle Vertragsverletzungsverfahren wegen Nichtmitteilung der Richtlinienumsetzung mit Zwangsgeldrisiko

BMWi trägt vor; betroffene Ressorts werden gebeten, zu ergänzen (insbes. BMJV zur Nichtmitteilung der Umsetzungen von RL 2011/7 - Zahlungsverzugs-RL und von RL 2011/36 – Menschenhandels-RL sowie BMF, BMVI und BMWi zur Anpassung von RLen zu Steuern, im Bereich Verkehr sowie dem Bereich des Niederlassungsrechts und des freien Dienstleistungsverkehr im Zusammenhang mit dem Beitritt von Kroatien).

7. Wahrnehmung der Ratsformationen

Ziel: Indossierung

Gem. EStS-Beschluss erstellt AA eine Übersicht zur Regelung der Wahrnehmung der unterschiedlichen Ratsformationen in Einklang mit den zum Teil neu zugeschnittenen Ressortzuständigkeiten; Entwurf wurde bereits zirkuliert.

AA trägt vor.

8. EUAL-Vorschauliste

Ziel der Befassung: Indossierung

Turnusmäßige Aktualisierung der EUAL-Vorschau über wichtige europapolitische Dossiers.

AA trägt vor.

9. Verschiedenes

*(i) **Strukturfonds/Absorptionsfähigkeit in den Herkunftsländern:** Follow-up zur Diskussion der EStS am 27.01.; Erörterung möglicher Ansatzpunkte, wie Absorptionsfähigkeit in den betreffenden Ländern verbessert werden kann; ggf. Auftrag zur Erarbeitung einer entsprechenden Unterlage, mit Unterstützung der dt. Auslandsvertretungen; Ergebnisse könnten dann noch in den Zwischenbericht des StS-Ausschusses einfließen. BMWi und BMAS werden gebeten vorzutragen.*

- (ii) **Zusammenarbeit mit Griechenland:** *AA/Vorsitz informiert über Stand des gem. EStS-Beschlusses vom 27.01. zu erstellenden Überblicks über bilaterale Hilfen für GRC.*
- (iii) **(ggf.) Dt.-brit. EStS-Konsultationen** am 27.03. in London: *AA/Vorsitz informiert über Stand der Vorbereitungen.*

Sofern aus Sicht der Ressorts dringender Gesprächsbedarf zu weiteren Themen besteht, bitten wir Sie, diese bis

Montag, den 10. Februar 2014, 13:00 Uhr

an das **AA, Referat E-KR** (LR I Sebastian Brökelmann, Tel. 030-18 17 3945, ekr-4@diplo.de) und **BMWi, Referat E A 1** (ORR'in Julia Grzondziel, Tel. 030-18 615-6915, julia.grzondziel@bmwi.bund.de) zu melden und mit **kurzen schriftlichen Angaben** zum Sachstand zu ergänzen.

Für persönliche Wahrnehmung des Termins und eine Teilnahmebestätigung im Vorfeld wären wir Ihnen dankbar. Wir schlagen vor, dass Sie sich von Ihrer/ Ihrem Europabeauftragten begleiten lassen.

Mit freundlichen Grüßen

gez.

Arndt Freytag von Loringhoven

gez.

Claudia Dörr-Voß

Abteilungsleiterrunde zur Koordinierung der Europapolitik
am Donnerstag, dem 13. Februar 2014 um 08.30 Uhr im BMWi

Referat: AG ÖS I 3
bearbeitet von: Dr. Spitzer

Berlin, den 10.02.2014
HR: 1390

TOP 2: Datenschutz EU-USA

hier: Erörterung möglicher Implikationen für SWIFT-Abkommen und Safe-Harbor-Vereinbarung

Federführendes Ressort: BMI

I. Gesprächsziel lt. TO:

Festlegung/Bekräftigung der Position der Bundesregierung

AA wünscht - auf Nachfrage - folgende inhaltliche Schwerpunktsetzung:

- Darstellung und Erörterung der Haltung der Bundesregierung zum SWIFT-Abkommen und zur Safe Harbor-Vereinbarung vor dem Hintergrund der im Zuge der NSA-Erkenntnisse geführten Datenschutz-Debatte.

II. Sachverhalt/ Sprechpunkte

1 Allgemein

- Meinungsbildung BMI geht u.a. auf verschiedene Analyseberichte KOM zurück. Diese wurden am 27. November 2013 vorgelegt.
- Zu den vorgelegten Analysen gehören u.a.:
 - **Analyse des Funktionierens des Safe-Harbor-Abkommens**
 - **Bericht über das TFTP-Abkommen** (auch SWIFT-Abkommen genannt).
- Beide Berichte und deren Schlussfolgerungen wurden im Rahmen des letzten Treffens der EU-AL am 12. Dezember 2013 behandelt.

2. Safe-Harbor-Abkommens

aktiv

- In ihrer Analyse vom 27. November 2013 spricht KOM sich für eine Verbesserung des Safe Harbor Modells anstelle einer Kündigung aus. Dies entspricht der DEU-Haltung.
- Der Innenausschuss des EP dagegen hat sich zuletzt für eine Aussetzung von Safe-Harbor ausgesprochen.
- Am 31. Januar 2014 tagte der Komitologieausschuss nach Art. 31 der europäischen Datenschutzrichtlinie. KOM stellte den MS ihre Analyse und Empfehlungen vor. Die Empfehlungen wurden von hierzu wortnehmenden

MS im Wesentlichen unterstützt. Allerdings machten neben DEU auch andere MS (NLD, POL, FRA, BUL, AUT und SVN) deutlich, dass die Empfehlungen nicht ausreichend seien.

- Die Bundesregierung ist in den vergangenen Monaten wiederholt für eine Verbesserung von Safe Harbor eingetreten. Neben den Vorschlägen der KOM zur Verbesserung tritt DEU dafür ein, für Modelle wie Safe Harbor in der neuen europäischen Datenschutz-Grundverordnung (DSGVO) einen robusten Rechtsrahmen mit klaren Vorgaben für Garantien der Bürgerinnen und Bürger zu schaffen. Die DSGVO klammert diese Problematik bislang aus. DEU hatte im September 2013 eine entsprechende Note zur Aufnahme in die Verhandlungen in der Ratsarbeitsgruppe DAPIX nach Brüssel übersandt, die auf großes Interesse bei den MS gestoßen ist.
- Ziel sollte es insbesondere sein, die Individualrechte der Bürgerinnen und Bürger zu stärken und ihnen bessere Rechtsschutzmöglichkeiten zur Verfügung zu stellen, die Registrierung der Unternehmen in der EU vorzunehmen und die staatliche Kontrolle seitens der EU-Datenschutzaufsichtsbehörden in Modellen wie Safe Harbor zu stärken.

SWIFT-Abkommen

aktiv

- Im Zusammenhang mit der Veröffentlichung der Snowden-Dokumente wurde in der Presse der Vorwurf erhoben, die NSA habe unter Umgehung des TFTP-Abkommens, das die Weiterleitungsmöglichkeiten von Daten des Finanzdienstleisters SWIFT aus der EU an die USA regelt und begrenzt, direkten Zugriff auf die SWIFT-Server genommen.
- Kommissarin Malmström hat nach Bekanntwerden der Vorwürfe Konsultationen mit den USA eingeleitet. Ende November 2013 wurden diese abgeschlossen und die KOM ist zu dem Schluss gelangt, dass keine Anhaltspunkte für einen Verstoß gegen das Abkommen vorliegen.
- Wir haben stets darauf verwiesen, dass Vertragsparteien des TFTP-Abkommens die EU und die USA sind. Daher war es zunächst Aufgabe der KOM, die gegen die USA erhobenen Vorwürfe aufzuklären.
- Mit Vorliegen des Untersuchungsergebnisses der KOM, dass kein Verstoß gegen das Abkommen vorliegt, besteht derzeit kein Anlass, das Abkommen auszusetzen. Eine Verknüpfung mit anderen Sachverhalten (z.B. Abschluss eines Datenschutzabkommens - wie vom EP gefordert) sollte nicht erfolgen.

reaktiv

- Am 23. Oktober 2013 hat das EP in einer Entschließung KOM aufgefordert, das zwischen der EU und den USA geschlossene Abkommen auszusetzen. Der LIBE-Ausschuss des EP hat auf Grundlage von Expertenbefragungen, Gesprächen mit US- und EU-Behörden sowie Zeitungsartikeln einen Bericht zur NSA-Überwachungsprogrammen verfasst. Dieser kommt zu dem Schluss, dass die NSA z.T. gemeinsam mit Behörden in UK, Kanada und Neuseeland eine massenhafte Überwachung der elektronischen Kommunikation durchführt und dadurch vermutlich auch Rechte von EU-Bürgern und Mitgliedstaaten verletzt. Er schlägt ein breites Maßnahmenbündel vor, u.a. die Aussetzung des TFTP-Abkommens bis zum Abschluss eines Datenschutzabkommens mit den USA.

Projektgruppe NSA

ÖS I 3 - 52000/4#1

AGL: MinR Weinbrenner
AGM: MinR Taube
Ref: ORR Jergl

Berlin, den 28. Februar 2014

Hausruf: 1767

OS-20140304-01

Krings E 5 III

Herrn Parlamentarischen Staatssekretär Dr. Schröder

über

Bundesministerium des Innern	
Stn N	
Eing:	- 4. MRZ. 2014
Uhrzeit:	10:15
Nr:	786

Abdruck(e):

Schröder

Herrn PSt Dr. Krings

Frau Stn Dr. Haber

Herrn Abteilungsleiter ÖS

Herrn Unterabteilungsleiter ÖS I

Bundesministerium des Innern	
PSt K	
Eing.	05. März 2014
Uhrzeit:	9:11
Nr:	87114

1.

2. absenden

3. z. d. A.

8.4.

AP 5/3

PG DS und die Referate ÖS II 1 und IT 3 haben mitgezeichnet.

RegöSIS = Vg. 7-24-3.

Betr.: Entwurf eines konsolidierten Berichts des LIBE-Komitees zu Überwachungsprogrammen u.a. der US-amerikanischen NSA

Anlagen: - 3 -

1. Votum

- Billigung der anl. Stellungnahme zu dem konsolidierten Bericht des LIBE-Komitees
- Billigung der Zuleitung dieser Stellungnahme an
 - MdEP Axel Voss über Herrn PSt S (Briefentwurf Anlage 2),
 - MdB Hans-Peter Uhl sowie
 - BKAm (wie in Anlage 3)

- 2 -

2. Sachverhalt

Der LIBE-Ausschuss des EP hat auf Grundlage von Expertenbefragungen, Gesprächen mit US- und EU-Behörden sowie Zeitungsartikeln einen Bericht zu Überwachungsprogrammen u.a. der NSA verfasst. Ein Entwurf des nunmehr zugeleiteten konsolidierten Berichts lag dem BMI im Januar 2014 zur Prüfung vor.

Im konsolidierten Bericht wird unverändert festgestellt, dass die NSA z.T. gemeinsam mit Behörden in UK, Kanada und Neuseeland eine massenhafte Überwachung der elektronischen Kommunikation durchführe und dadurch vermutlich auch Rechte von EU-Bürgern und -Mitgliedstaaten verletze. Er beinhaltet ein breites Maßnahmenbündel: Überprüfung und Anpassung von Abkommen mit den USA, Stärkung von ENISA^{*}, dem Europol-Cybercrime-Center (EC3) und dem Europäischen Datenschutzbeauftragten (EDPS), Stärkung der IT-Sicherheit und diverse Appelle an die Kommission und die Mitgliedstaaten. Schwerpunkt ist ein „Digitaler Habeas Corpus“ zum „Schutz der Grundrechte im digitalen Zeitalter“, der nunmehr acht (im Entwurf vom Januar sieben) Punkte beinhaltet.

** EU-Network and Information Security Agency*

Ein Mitarbeiter von MdEP Voss hat Herrn PSt S sowie MdB Uhl um Stellungnahme gebeten. Gleiches begehrt auch Abt. 6 BK-Amt.

3. Stellungnahme

Der Bericht ist im Vergleich zur Entwurfsfassung umfangreich überarbeitet worden (Vergleichsfassung in der Anlage 1). Bereits im Januar geäußerte Bedenken sind jedoch weiterhin überwiegend nicht ausgeräumt. Im Einzelnen:

I. „Digitaler Habeas-Corpus“

1. Abschluss des Datenschutzpakets in 2014

Erscheint nicht aussichtsreich. Es sind noch eine Vielzahl bedeutender Fragen zu klären. Gründlichkeit muss deshalb vor Schnelligkeit gehen.

- 3 -

2. Abschluss des EU-US-Datenschutzabkommens

Keine Bedenken. Zuständig ist KOM.

3. Aussetzung von Safe-Harbour

Die Bundesregierung setzt sich für die Verbesserung von Safe Harbour ein. Neben der zeitnahen Umsetzung der Empfehlungen der KOM aus ihrer Safe Harbour Analyse von November 2013 im Wege der Nachverhandlung sollte in der Datenschutz-Grundverordnung ein rechtlicher Rahmen für Modelle wie Safe Harbour geschaffen werden.

4. Aussetzung des TFTP-Abkommens (betr. Zugang zu SWIFT-Daten zur Terrorismusbekämpfung) bis zum Abschluss des Datenschutzabkommens

Angesichts der Tatsache, dass die Kommission nach Abschluss ihrer Konsultationen zu den Vorwürfen, die USA hätten unter Umgehung des TFTP-Abkommens direkten Zugriff auf den SWIFT-Server genommen, keine Anhaltspunkte für einen Verstoß feststellen konnte, besteht derzeit kein Anlass, das Abkommen auszusetzen.

5. (neu) Evaluierung sämtlicher Abkommen oder des sonstigen Austauschs mit Drittstaaten, auf deren Grundlage es zu einer Verarbeitung personenbezogener Daten kommt

Gegenstand soll die mögliche Verletzung des Schutzes dieser Daten durch Überwachungsmaßnahmen in den Drittstaaten sein. Ein solches Vorhaben würde es erfordern, die Einzelheiten der Überwachungsmaßnahmen von Drittstaaten zu kennen oder diese zumindest belastbar einschätzen zu können. Mit einer Bereitschaft zur Offenlegung von Maßnahmen in der hierfür notwendigen Detaillierung ist nicht zu rechnen. Daher dürfte ein solches Vorhaben nicht aussichtsreich und gleichwohl sehr aufwändig sein.

6. Besserer Schutz der Rechte von EU-Bürgern (ohne Konkretisierung)

Keine Bedenken.

- 4 -

7. Entwicklung einer Strategie für eine Europäische (stärker unabhängige) IT-Industrie („digital new deal“)

Grundsätzlich Zustimmung; der Koalitionsvertrag beinhaltet eine vergleichbare Maßnahme:

„Um Freiheit und Sicherheit im Internet zu schützen, stärken und gestalten wir die Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum. Dazu treten wir für eine europäische Cybersicherheitsstrategie ein, ergreifen Maßnahmen zur Rückgewinnung der technologischen Souveränität, unterstützen die Entwicklung Moderner Staat, innere Sicherheit und Bürgerrechte vertrauenswürdiger IT- und Netz-Infrastruktur sowie die Entwicklung sicherer Soft- und Hardware und sicherer Cloud-Technologie und begrüßen auch Angebote eines nationalen bzw. europäischen Routings.“

8. EU-Politik als Referenz für demokratische und neutrale Internet-Governance

Keine Bedenken.

II. Weitere Punkte

In seiner Bewertung des Berichtsentwurfs vom Januar 2014 hat BMI überdies auf **aus deutscher Sicht besonders kritische Punkte** hingewiesen und deren Streichung angeregt.

Eine diesbezügliche **Verbesserung** kann lediglich in „Main findings“ Nr. 2 des konsolidierten Berichts festgestellt werden, wo nun **nicht mehr unterstellt wird**, auch Deutschland betreibe ähnliche Überwachungsprogramme wie PRISM.

Weiterhin enthalten ist jedoch als „Recommendation“ Nr. 22 (vorher 20) eine **Aufforderung auch an Deutschland** (als angeblicher Teil eines sog. „14-eyes“-Programms), **seine Gesetzgebung zu überprüfen bzw. zu überarbeiten**. Die hier einschlägigen deutschen Vorschriften entsprechen den Vorgaben aus den entsprechenden Urteilen des Bundesverfassungsgerichts und

- 5 -

sind mit den Grundrechten vereinbar. Unabhängig davon liegt die nationale Sicherheitsgesetzgebung außerhalb der Zuständigkeit der EU und damit auch des EP. Deswegen sollte weiterhin die Streichung dieser Empfehlung angestrebt werden.

In Recommendation 99 ist durch neue Einfügungen u.a. die explizite Aufforderung an die KOM aufgenommen worden, die Ausweitung von Zuständigkeiten und Ressourcen bestimmter EU-Einrichtungen mit dem Ziel zu prüfen, dass diese eine Schlüsselrolle bei der Gewährleistung von IT-Sicherheit und der Verhinderung von IT-Angriffen in der EU spielen; ferner soll auch die Einrichtung eines speziellen CERTs für die EU und ihre MS geprüft werden. DEU befürwortet eine Stärkung der Kapazitäten und eine verbesserte Kooperation der MS im Bereich der IT-Sicherheit. Insbesondere im operativen Bereich liegt die Zuständigkeit aber bei den Mitgliedstaaten und auch entsprechende Aktivitäten müssen bei den Mitgliedstaaten verbleiben. Für die diesbezüglichen Einfügungen („play a key role (...)“ und letzter Hs. ab „and to establish within ENISA's structure a Computer Emergency response Team (CERT) for the EU and its Member States“) sollte daher eine Streichung angestrebt werden.



Weinbrenner



Jergl

Briefentwurf PStS

Herrn

Axel Voss, MdEP

Europäisches Parlament

ASP 15 E 150

Rue Wiertz

B-1047 Brüssel

Sehr geehrter Herr Abgeordneter,

für die Zusendung des konsolidierten Berichtsentwurfs des LIBE-Komitees danke ich Ihnen herzlich. Gerne nutze ich die Gelegenheit, aus Sicht des BMI hierzu Stellung zu nehmen, und möchte auf folgende mir besonders wichtig erscheinende Abschnitte eingehen:

I. „Digitaler Habeas-Corpus“

1. Abschluss des Datenschutzpakets in 2014

Es sind noch eine Vielzahl bedeutender Fragen zu klären. Gründlichkeit muss vor Schnelligkeit gehen. Entsprechend hat sich auch der Europäische Rat am 24./25. Oktober 2013 nicht auf eine Verabschiedung in 2014 festgelegt, sondern die „rechtzeitige Verabschiedung eines soliden EU-Datenschutzrahmens für die Vollendung des Digitalen Binnenmarktes bis 2015 als von entscheidender Bedeutung“ bezeichnet.

2. Abschluss des EU-US-Datenschutzabkommens

Gegen dieses Vorhaben im Zuständigkeitsbereich der KOM habe ich keine Einwände.

3. Aussetzung von Safe-Harbour

Die Bundesregierung setzt sich für die Verbesserung von Safe Harbour ein. Neben der zeitnahen Umsetzung der Empfehlungen der KOM aus ihrer Safe Harbour Analyse von November 2013 im Wege der Nachverhandlung sollte in der Datenschutz-Grundverordnung ein rechtlicher Rahmen für Modelle wie Safe Harbour geschaffen werden.

4. Aussetzung des TFTP-Abkommens (betr. Zugang zu SWIFT-Daten zur Terrorismusbekämpfung) bis zum Abschluss des Datenschutzabkommens

Angesichts der Tatsache, dass die Kommission nach Abschluss ihrer Konsultationen zu den Vorwürfen, die USA hätten unter Umgehung des TFTP-Abkommens direkten Zugriff auf den SWIFT-Server genommen, keine Anhaltspunkte für einen Verstoß feststellen konnte, besteht aus meiner Sicht derzeit kein Anlass, das Abkommen auszusetzen.

5. Evaluierung sämtlicher Abkommen oder sonstigen Austauschs mit Drittstaaten, auf deren Grundlage es zu einer Verarbeitung personenbezogener Daten kommt

Gegenstand der Evaluierung soll die mögliche Verletzung des Schutzes dieser Daten durch Überwachungsmaßnahmen in den Drittstaaten sein. Ein solches Vorhaben würde es aus meiner Sicht erfordern, die Einzelheiten der Überwachungsmaßnahmen von Drittstaaten zu kennen oder diese zumindest belastbar einschätzen zu können. Erfahrungsgemäß ist regelmäßig nicht mit einer Bereitschaft zur Offenlegung von Maßnahmen in der hierfür notwendigen Detaillierung zu rechnen. Daher schätze ich dieses Vorhaben nicht als aussichtsreich und gleichwohl sehr aufwändig ein.

6. Besserer Schutz der Rechte von EU-Bürgern (ohne Konkretisierung)

Keine Bedenken.

7. Entwicklung einer Strategie für eine Europäische (stärker unabhängige) IT-Industrie („digital new deal“)

Zustimmung; der Koalitionsvertrag beinhaltet eine vergleichbare Maßnahme: „Um Freiheit und Sicherheit im Internet zu schützen, stärken und gestalten wir die Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum. Dazu treten wir für eine europäische Cybersicherheitsstrategie ein, ergreifen

Maßnahmen zur Rückgewinnung der technologischen Souveränität, unterstützen die Entwicklung Moderner Staat, innere Sicherheit und Bürgerrechte vertrauenswürdiger IT- und Netz-Infrastruktur sowie die Entwicklung sicherer Soft- und Hardware und sicherer Cloud-Technologie und begrüßen auch Angebote eines nationalen bzw. europäischen Routings.“

8. EU-Politik als Referenz für demokratische und neutrale Internet-Governance
Keine Bedenken.

II. Weitere Punkte

In seiner Bewertung des Berichtsentwurfs vom Januar 2014 hat BMI überdies auf **aus deutscher Sicht besonders kritische Punkte** hingewiesen und deren Streichung angeregt.

Eine diesbezügliche Verbesserung kann ich in „Main findings“ Nr. 2 des konsolidierten Berichts feststellen, wo nun nicht mehr unterstellt wird, auch Deutschland betreibe ähnliche Überwachungsprogramme wie PRISM.

Weiterhin enthalten ist jedoch als „Recommendation“ Nr. 22 eine **Aufforderung auch an Deutschland** (als angeblicher Teil eines sog. „14-eyes“-Programms), **seine Gesetzgebung zu überprüfen bzw. zu überarbeiten**. Die hier einschlägigen deutschen Vorschriften entsprechen den Vorgaben aus den entsprechenden Urteilen des Bundesverfassungsgerichts und sind mit den Grundrechten vereinbar. Unabhängig davon liegt die nationale Sicherheitsgesetzgebung außerhalb der Zuständigkeit der EU und damit auch des EP.

In Recommendation 99 ist durch neue Einfügungen u.a. die explizite Aufforderung an die KOM aufgenommen worden, die Ausweitung von Zuständigkeiten und Ressourcen bestimmter EU-Einrichtungen mit dem Ziel zu prüfen, dass diese eine Schlüsselrolle bei der Gewährleistung von IT-Sicherheit und der Verhinderung von IT-Angriffen in der EU spielen; ferner soll auch die Einrichtung eines speziellen CERTs für die EU und ihre MS geprüft werden. DEU befürwortet eine Stärkung der Kapazitäten und eine verbesserte Kooperation der

MS im Bereich der IT-Sicherheit. Insbesondere im **operativen Bereich** liegt die **Zuständigkeit aber bei den Mitgliedstaaten** und auch entsprechende Aktivitäten müssen bei den Mitgliedstaaten verbleiben. Für die diesbezüglichen Einfügungen („play a key role (...)“ und letzter Hs. ab „and to establish within ENISA's structure a Computer Emergency response Team (CERT) for the EU and its Member States“) sollte daher eine Streichung angestrebt werden.

Deswegen erachte ich die Streichung dieser Empfehlungen für notwendig und wäre Ihnen dankbar, wenn Sie dies mit einem entsprechenden Änderungsantrag unterstützen könnten.

Mit freundlichen Grüßen

N.d.H.PStS

Stellungnahme BMI zum Entwurf eines konsolidierten Berichts des LIBE-Komitees zu Überwachungsprogrammen u.a. der US-amerikanischen NSA

I. „Digitaler Habeas-Corpus“

1. Abschluss des Datenschutzpakets in 2014

Erscheint nicht aussichtsreich. Es sind noch eine Vielzahl bedeutender Fragen zu klären. Gründlichkeit muss deshalb vor Schnelligkeit gehen.

2. Abschluss des EU-US-Datenschutzabkommens

Keine Bedenken. Zuständig ist KOM.

3. Aussetzung von Safe-Harbour

Die Bundesregierung setzt sich für die Verbesserung von Safe Harbour ein. Neben der zeitnahen Umsetzung der Empfehlungen der KOM aus ihrer Safe Harbour Analyse von November 2013 im Wege der Nachverhandlung sollte in der Datenschutz-Grundverordnung ein rechtlicher Rahmen für Modelle wie Safe Harbour geschaffen werden.

4. Aussetzung des TFTP-Abkommens (betr. Zugang zu SWIFT-Daten zur Terrorismusbekämpfung) bis zum Abschluss des Datenschutzabkommens

Angeichts der Tatsache, dass die Kommission nach Abschluss ihrer Konsultationen zu den Vorwürfen, die USA hätten unter Umgehung des TFTP-Abkommens direkten Zugriff auf den SWIFT-Server genommen, keine Anhaltspunkte für einen Verstoß feststellen konnte, besteht aus unserer Sicht derzeit kein Anlass, das Abkommen auszusetzen.

5. (neu) Evaluierung sämtlicher Abkommen oder sonstigen Austauschs mit Drittstaaten, auf deren Grundlage es zu einer Verarbeitung personenbezogener Daten kommt

Gegenstand der Evaluierung soll die mögliche Verletzung des Schutzes dieser Daten durch Überwachungsmaßnahmen in den Drittstaaten sein. Ein solches Vorhaben würde es aus unserer Sicht erfordern, die Einzelheiten der Überwachungsmaßnahmen von Drittstaaten zu kennen oder diese zumindest

belastbar einschätzen zu können. Nach unseren Erfahrungen ist regelmäßig nicht mit einer Bereitschaft zur Offenlegung von Maßnahmen in der hierfür notwendigen Detaillierung zu rechnen. Daher schätzen wir dieses Vorhaben nicht als aussichtsreich und gleichwohl sehr aufwändig ein.

6. Besserer Schutz der Rechte von EU-Bürgern (ohne Konkretisierung)

Keine Bedenken.

7. Entwicklung einer Strategie für eine Europäische (stärker unabhängige) IT-Industrie („digital new deal“)

Zustimmung; der Koalitionsvertrag beinhaltet eine vergleichbare Maßnahme: „Um Freiheit und Sicherheit im Internet zu schützen, stärken und gestalten wir die Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum. Dazu treten wir für eine europäische Cybersicherheitsstrategie ein, ergreifen Maßnahmen zur Rückgewinnung der technologischen Souveränität, unterstützen die Entwicklung Moderner Staat, innere Sicherheit und Bürgerrechte vertrauenswürdiger IT- und Netz-Infrastruktur sowie die Entwicklung sicherer Soft- und Hardware und sicherer Cloud-Technologie und begrüßen auch Angebote eines nationalen bzw. europäischen Routings.“

8. EU-Politik als Referenz für demokratische und neutrale Internet-Governance

Keine Bedenken.

II. Weitere Punkte

In seiner Bewertung des Berichtsentwurfs vom Januar 2014 hat BMI überdies auf **aus deutscher Sicht besonders kritische Punkte** hingewiesen und deren Streichung angeregt.

Eine diesbezügliche Verbesserung kann in „Main findings“ Nr. 2 des konsolidierten Berichts festgestellt werden, wo nun nicht mehr unterstellt wird, auch Deutschland betreibe ähnliche Überwachungsprogramme wie PRISM.

Weiterhin enthalten ist jedoch als „Recommendation“ Nr. 22 (vorher 20) eine **Aufforderung auch an Deutschland** (als angeblicher Teil eines sog. „14-eyes“-Programms), **seine Gesetzgebung zu überprüfen bzw. zu überarbeiten**. Die hier einschlägigen deutschen Vorschriften entsprechen den Vorgaben aus den entsprechenden Urteilen des Bundesverfassungsgerichts und sind mit den Grundrechten vereinbar. Unabhängig davon liegt die nationale Sicherheitsgesetzgebung außerhalb der Zuständigkeit der EU und damit auch des EP. Deswegen wird weiterhin die Streichung dieser Empfehlung für notwendig erachtet.

In Recommendation 99 ist durch neue Einfügungen u.a. die explizite Aufforderung an die KOM aufgenommen worden, die Ausweitung von Zuständigkeiten und Ressourcen bestimmter EU-Einrichtungen mit dem Ziel zu prüfen, dass diese eine Schlüsselrolle bei der Gewährleistung von IT-Sicherheit und der Verhinderung von IT-Angriffen in der EU spielen; ferner soll auch die Einrichtung eines speziellen CERTs für die EU und ihre MS geprüft werden. DEU befürwortet eine Stärkung der Kapazitäten und eine verbesserte Kooperation der MS im Bereich der IT-Sicherheit. Insbesondere im **operativen Bereich liegt die Zuständigkeit aber bei den Mitgliedstaaten** und auch entsprechende Aktivitäten müssen bei den Mitgliedstaaten verbleiben. Für die diesbezüglichen Einfügungen („play a key role (...)“ und letzter Hs. ab „and to establish within ENISA's structure a Computer Emergency response Team (CERT) for the EU and its Member States“) sollte daher eine Streichung angestrebt werden.



Bundesministerium
des Innern

ab ca 6.3.14. + Anlage

Bundesministerium des Innern, 11014 Berlin

Herrn
Dr. Hans-Peter Uhl, MdB
Platz der Republik 1
11011 Berlin

Dr. Günter Krings, MdB
Parlamentarischer Staatssekretär

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin

TEL +49 (0)30 18 681-1062

FAX +49 (0)30 18 681-1139

E-MAIL PSIK@bmi.bund.de

INTERNET www.bmi.bund.de

DATUM 6. März 2014

Sehr geehrter Herr Kollege,

*Uhl 7/31
Witz*

Uhl Hans-Peter,

anlegend übersende ich Ihnen wie erbeten die Stellungnahme des Bundesministeriums des Innern zum Entwurf eines konsolidierten Berichts des LIBE-Komitees zu Überwachungsprogrammen u.a. der US-amerikanischen NSA zur Kenntnisnahme.

Mit freundlichen Grüßen

Dr. Krings

Dr. Günter Krings

*RegöSIS z. Vg.
7.24.3*

König, Antje

Von: PStKrings_
Gesendet: Mittwoch, 5. März 2014 12:25
An: 'axel.voss@europarl.europa.de'
Cc: PStKrings_
Betreff: Schreiben PSt Dr. Krings

über BK - Hm. Naas z.k.



Seiten aus
nbenannt-2.PDF - A.

Sehr geehrter Herr Abgeordneter,

im Auftrag von Herrn PSt Dr. Krings übersende ich Ihnen anliegendes Schreiben.

Mit freundlichen Grüßen

Antje König

Büro: Dr. Günter Krings, MdB
Parlamentarischer Staatssekretär
beim Bundesminister des Innern
Alt-Moabit 101 D, 10559 Berlin
Tel.: +49 (0) 30 18 681-1065
Fax: +49 (0) 30 18 681-1139
PC-Fax: +49 (0) 30 18 681-51065
Mail: Antje.Koenig@bmi.bund.de



Bundesministerium
des Innern

Bundesministerium des Innern, 11014 Berlin

Herrn
Axel Voss, MdEP
Europäisches Parlament
ASP 15 E 150
Rue Wiertz
B-1047 Brüssel

Dr. Günter Krings, MdB
Parlamentarischer Staatssekretär

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin

TEL +49 (0)30 18 681-1062

FAX +49 (0)30 18 681-1139

E-MAIL PSIK@bmi.bund.de

INTERNET www.bmi.bund.de

DATUM 5. März 2014

Sehr geehrter Herr Kollege,

Liebes Axel!

für die Zusendung des konsolidierten Berichtsentwurfs des LIBE-Komitees danke ich Ihnen herzlich. Gerne nutze ich die Gelegenheit, aus Sicht des BMI hierzu Stellung zu nehmen, und möchte auf folgende mir besonders wichtig erscheinende Abschnitte eingehen:

I. „Digitaler Habeas-Corpus“

1. Abschluss des Datenschutzpakets in 2014

Es sind noch eine Vielzahl bedeutender Fragen zu klären. Gründlichkeit muss vor Schnelligkeit gehen. Entsprechend hat sich auch der Europäische Rat am 24./25. Oktober 2013 nicht auf eine Verabschiedung in 2014 festgelegt, sondern die „rechtzeitige Verabschiedung eines soliden EU-Datenschutzrahmens für die Vollendung des Digitalen Binnenmarktes bis 2015 als von entscheidender Bedeutung“ bezeichnet.

2. Abschluss des EU-US-Datenschutzabkommens

Gegen dieses Vorhaben im Zuständigkeitsbereich der KOM habe ich keine Einwände.

3. Aussetzung von Safe-Harbour

Die Bundesregierung setzt sich für die Verbesserung von Safe Harbour ein. Neben der zeitnahen Umsetzung der Empfehlungen der KOM aus ihrer Safe Harbour Analyse von November 2013 im Wege der Nachverhandlung sollte in der Datenschutz-Grundverordnung ein rechtlicher Rahmen für Modelle wie Safe Harbour geschaffen werden.



SEITE 2 VON 3

4. Aussetzung des TFTP-Abkommens (betr. Zugang zu SWIFT-Daten zur Terrorismusbekämpfung) bis zum Abschluss des Datenschutzabkommens

Angesichts der Tatsache, dass die Kommission nach Abschluss ihrer Konsultationen zu den Vorwürfen, die USA hätten unter Umgehung des TFTP-Abkommens direkten Zugriff auf den SWIFT-Server genommen, keine Anhaltspunkte für einen Verstoß feststellen konnte, besteht aus meiner Sicht derzeit kein Anlass, das Abkommen auszusetzen.

5. Evaluierung sämtlicher Abkommen oder sonstigen Austauschs mit Drittstaaten, auf deren Grundlage es zu einer Verarbeitung personenbezogener Daten kommt
Gegenstand der Evaluierung soll die mögliche Verletzung des Schutzes dieser Daten durch Überwachungsmaßnahmen in den Drittstaaten sein. Ein solches Vorhaben würde es aus meiner Sicht erfordern, die Einzelheiten der Überwachungsmaßnahmen von Drittstaaten zu kennen oder diese zumindest belastbar einschätzen zu können. Erfahrungsgemäß ist regelmäßig nicht mit einer Bereitschaft zur Offenlegung von Maßnahmen in der hierfür notwendigen Detaillierung zu rechnen. Daher schätze ich dieses Vorhaben nicht als aussichtsreich und gleichwohl sehr aufwändig ein.

6. Besserer Schutz der Rechte von EU-Bürgern (ohne Konkretisierung)

Keine Bedenken.

7. Entwicklung einer Strategie für eine Europäische (stärker unabhängige) IT-Industrie („digital new deal“)

Zustimmung; der Koalitionsvertrag beinhaltet eine vergleichbare Maßnahme:

„Um Freiheit und Sicherheit im Internet zu schützen, stärken und gestalten wir die Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum. Dazu treten wir für eine europäische Cybersicherheitsstrategie ein, ergreifen Maßnahmen zur Rückgewinnung der technologischen Souveränität, unterstützen die Entwicklung Moderner Staat, innere Sicherheit und Bürgerrechte vertrauenswürdiger IT- und Netz-Infrastruktur sowie die Entwicklung sicherer Soft- und Hardware und sicherer Cloud-Technologie und begrüßen auch Angebote eines nationalen bzw. europäischen Routings.“

8. EU-Politik als Referenz für demokratische und neutrale Internet-Governance

Keine Bedenken.

II. Weitere Punkte



Bundesministerium
des Innern

SEITE 3 VON 3

In seiner Bewertung des Berichtsentwurfs vom Januar 2014 hat BMI überdies auf **aus deutscher Sicht besonders kritische Punkte** hingewiesen und deren Streichung angeregt.

Eine diesbezügliche Verbesserung kann ich in „Main findings“ Nr. 2 des konsolidierten Berichts feststellen, wo nun nicht mehr unterstellt wird, auch Deutschland betreibe ähnliche Überwachungsprogramme wie PRISM.

Weiterhin enthalten ist jedoch als „Recommendation“ Nr. 22 eine **Aufforderung auch an Deutschland** (als angeblicher Teil eines sog. „14-eyes“-Programms), **seine Gesetzgebung zu überprüfen bzw. zu überarbeiten**. Die hier einschlägigen deutschen Vorschriften entsprechen den Vorgaben aus den entsprechenden Urteilen des Bundesverfassungsgerichts und sind mit den Grundrechten vereinbar. Unabhängig davon liegt die nationale Sicherheitsgesetzgebung außerhalb der Zuständigkeit der EU und damit auch des EP.

In Recommendation 99 ist durch neue Einfügungen u.a. die explizite Aufforderung an die KOM aufgenommen worden, die Ausweitung von Zuständigkeiten und Ressourcen bestimmter EU-Einrichtungen mit dem Ziel zu prüfen, dass diese eine Schlüsselrolle bei der Gewährleistung von IT-Sicherheit und der Verhinderung von IT-Angriffen in der EU spielen; ferner soll auch die Einrichtung eines speziellen CERTs für die EU und ihre MS geprüft werden. DEU befürwortet eine Stärkung der Kapazitäten und eine verbesserte Kooperation der MS im Bereich der IT-Sicherheit. Insbesondere im **operativen Bereich liegt die Zuständigkeit aber bei den Mitgliedstaaten** und auch entsprechende Aktivitäten müssen bei den Mitgliedstaaten verbleiben. Für die diesbezüglichen Einfügungen („play a key role (...)“ und letzter Hs. ab „and to establish within ENISA's structure a Computer Emergency response Team (CERT) for the EU and its Member States“) sollte daher eine Streichung angestrebt werden.

Deswegen erachte ich die Streichung dieser Empfehlungen für notwendig und wäre Ihnen dankbar, wenn Sie dies mit einem entsprechenden Änderungsantrag unterstützen könnten.

Mit freundlichen Grüßen

Dr. Günter Krings