Interceptability of telecommunications: Is US and Dutch law prepared for the future?

Bert-Jaap Koops[a] and Rudi Bekkers[b, c]

[a]Tilburg Institute for Law, Technology, and Society, Tilburg University, P.O. Box 90153, NL-5000 LE Tilburg, The Netherlands

[b]Eindhoven Centre for Innovation Studies (ECIS), Technische Universiteit Eindhoven, P.O. Box 513, NL-5600 BM Eindhoven, The Netherlands

[c]Dialogic Innovatie and Interactie, Wilhelminapark 20, NL-3581 ND Utrecht, The Netherlands

Abstract

Already for many decades, governments successfully intercept telecommunications to collect information about – potential – criminals and terrorists. A crucial part of interception policy is legislation that requires telecommunications providers to make their networks and services interceptable. This paper discusses two examples of interceptability legislation: the Communications Assistance for Law Enforcement Act (CALEA) in the US and the Telecommunications Act in the Netherlands, in order to show basic questions, considerations, and trade-offs relevant to designing legal interceptability laws.

In particular, the sustainability of interceptability policies as laid down in these laws is questioned, since they are under significant pressure. Technical and market developments challenge their effectiveness and costs. These developments include IP-based services, seamless roaming, default encryption at various telecommunications layers, and the 'identity boom'. Market challenges include substantial shifts in the value chain and the explosion of traffic volumes. This paper aims to determine which interceptability policy is best suited to cope with the challenges that lie ahead.

Abbreviated title

Interceptability of telecommunications

This is the preprint of a paper that has been published as:

Bert-Jaap Koops & Rudi Bekkers (2007). Interceptability of telecommunications: Are U.S. and Dutch law prepared for the future? Telecommunications Policy 31 (2007) 45–67.

It is available from the following digital object identifier (DOI) :
http://dx.doi.org/10.1016/j.telpol.2006.11.006

1. Introduction

Interception of telecommunications is one of the most vital methods for governments to collect information about – potential – criminals and terrorists. In the course of the twentieth century, it became an investigation power that government agencies call indispensable, and it is, particularly in some European countries, by far the most widely used special investigation power.[1]

Historically, wiretapping[2] has been easy. You plug in on the right telephone line, and you can immediately listen in on the communications. In the 1990s, however, with several changes in telecommunications taking place, including liberalization, privatization and developments in technology and markets, governments were forced to pass legislation in order to make sure that they would continue to have the ability to wiretap. The U.S. Communications Assistance for Law Enforcement Act (CALEA) of 1994 and Chapter 13 of the Dutch Telecommunications Act of 1998, for example, imposed obligations on telecommunications carriers[3] to ensure interceptability.

'Interceptability' means that telecommunications can be intercepted technically on the telecommunications networks or services that transport the communications (technical interceptability).[4] It also includes the ability of telecommunications providers to deliver traffic data[5] or user data, since these may be necessary before a wiretap can be ordered. Interceptability thus means, in short, the ability to investigate telecommunications.

Interceptability legislation is a classic example of the trade-off between public and private interests: obligations – including financial ones – are imposed on private parties, in order to safeguard a public interest. The interest of the private parties – the telecommunications providers – to develop and maintain telecom networks and services as they and the market see fit clashes with the public interest of government agencies who desire to intercept telecommunications and therefore require interceptability. The scope of the obligations imposed within this trade-off, and particularly their financial consequences, which differ from country to country, make this a particularly sensitive and politically heated topic.

This is a good occasion to take a fresh look at interceptability laws. Most of these date from the mid-1990s, an era in which the internet was only just emerging on a larger scale and in which liberalization was only just starting in Europe. Since then, significant developments have taken place in telecommunications, both in the

[1] See *infra*, section 3.

[2] In this article, the terms 'wiretapping' and 'interception of telecommunications' will be used interchangeably. In the U.S., a distinction is usually made between wire, electronic, and oral interception, following the distinction made in criminal-procedure law; the term wiretapping in this article includes the U.S. wire and electronic interception, but excludes oral interception (which roughly means direct interception, with a bug or directional microphone, of voice communication).

[3] In this article, the terms 'carrier', 'operator', and 'provider' will be used interchangeably for someone who operates telecommunications networks and/or services.

[4] 'Interceptability' also includes the obligation that telecommunications carriers comply with legal orders to intercept or to provide traffic data or user data (organisational interceptability). Since this aspect is less vulnerable to developments in telecommunications, this article will be confined to technical interceptability.

[5] Besides interception of telecommunications, which means the content of these communications, governments also have powers to access 'traffic data': data about the communications, such as who called whom when (and perhaps where). In the U.S., the methods to request access to traffic data are called pen registers and trap-and-trace devices; the term 'traffic-data collection' will be used here.

technology and in the market, and these developments continue steadily – for instance with Fiber to the Home (FttH) and Voice over IP (VoIP) – to put pressure on the interceptability of telecommunications. These developments are such that it must be questioned whether the fixation of governments on a sweeping ability to wiretap, as entrenched in legislation, can be continued at all, and if it can, what the costs would be – both financially and in terms of immaterial costs such as privacy and other forms of legal protection.

In light of this, the following questions are posed in this article: How do developments in telecommunications challenge the future interceptability of telecommunications, and how can governments respond to these challenges? Can a balance be maintained between, on the one hand, the ability to counter crime and terrorism through interception and, on the other, the protection against overintrusive government interference?

These questions shall be answered by looking at two countries, the United States and the Netherlands. The former is chosen because the U.S. enacted one of the earliest, if not the first, interceptability laws, and because it has an interesting set of provisions that make the law rather flexible to include or exclude new telecommunications. The second is chosen as a representative of a European legal system that provides an interesting counterexample to the U.S. law. The Dutch law is less elaborate and seems more rigid, with an all-or-nothing approach to new telecommunications; it turns out to be broader in scope than the U.S. law. The Netherlands is also interesting to include because very few publications cover it, so that this article takes the opportunity of opening up the Dutch law to an international audience.[6]

After a glimpse of the historical context that triggered interceptability laws (section 2), the U.S. and the Dutch legislation are described in general (section 3) and subtsequently in more detail, through a comparative analysis of the major policy decisions that underlie these laws (section 4). Then, major developments in telecommunications are described that are taking place now or that will surface in the near future, with an indication how these put pressure on the interceptability laws (section 5). Then, the research questions are answered by analyzing the sustainability of U.S. and Dutch law in view of these developments (section 6). The article ends with a conclusion (section 7).

It should be stressed that this article is restricted to laws regarding *interceptability* of telecommunications. The much broader issue of *interception* legislation, i.e., under what conditions the police can intercept telecommunications, cannot be addressed within the scope of this article. As a consequence, regulatory instruments such as the Council of Europe's Convention on Cybercrime and the U.S. Patriot Act are not discussed, since these do not regard interceptability.[7]

---

[6] Academic literature in English is often limited to a comparison between U.S. and UK Law, see for instance Yeates (2001) and Sutter (2001). A comparative description of the interceptability laws in the G7 countries is available in German, see Büllingen and Hillebrand (2003). There is no academic international literature that pays substantial attention to the Dutch interceptability law; in Dutch literature, only Koops, et al. (2005) and Smits (2006) cover the subject.

[7] The Convention on Cybercrime (ETS 185) contains an investigation power to order preservation and partial disclosure of traffic data (art. 17). This implies an obligation of telecom providers to disclose traffic data, but does not imply technical interceptability obligations. Cf. Explanatory Report, available at http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, §§ 165-169. The U.S. Patriot Act (Public Law 107-56) 'is not intended to affect obligations under Communications Assistance for Law Enforcement Act, nor does the act impose any additional technical obligation or requirement on a provider of wire or electronic communication

2. Historical context

The interceptability of telecommunications is influenced to a large degree by technical and market developments. It is therefore useful to first look at the context of past telecommunications developments that have triggered interceptability laws. This covers the period roughly until the late 1990s.

In many respects, the telecommunications sector has been a relatively stable field with few changes. This certainly holds true for the period up to the late 1980s. In most countries, all telecommunications services were offered by one single, usually public, provider, often designated as the national PTT. In the US, the largest operator AT&T was a private firm but can nevertheless be characterized as a monopolist, which at its peak employed one million people.

The offer of services changed little over the years. Voice telephony was in all respects the most important service. Although technical developments took place, such as the invention and – much later – general adoption of the fax, the automation and later digitization of telephone exchanges, the rise of data transport, and the introduction of car telephony, the impact of these new services was fairly limited. The main challenge for PTTs up to the late 1980s was to meet the growing demand for voice telephony, including the issue of bringing telephony to all homes, even in lonely places, at acceptable costs. In terms of interceptability, there were hardly any problems.

This changed in the course of the 1990s, as a result of market, policy and technical developments that had their roots in the 1980s. The following may be mentioned.

- The *number of market parties* grew significantly: In the US, new entrants such as Microwave Communications, Inc (MCI) and Sprint captured important submarkets. AT&T's local operations were split into seven independent Regional Bell Operating Companies (RBOC's) known as 'Baby Bells'. Competition further increased, by new entrants as well as cable tv companies offering a wider range of telecommunications services. Europe saw a gradual liberalization in various partial telecommunications markets, leading to full-scale liberalisation of the entire sector by January 1st, 1998, with increasing competition as a result.[8]
- The broad introduction of *new services*, including mobile telephony.
- The increasing importance of the internet, partly through the ever growing popularity of the World Wide Web.

These developments were not immediately disastrous for interceptability, because fixed telephony continued to be interceptable without problems, and because, despite liberalization, the market share of the former incumbent continued to be high in almost all partial markets. However, as new services, such as GSM telephony, increased in importance and as the market share of new market parties grew, wiretapping threatened to become less feasible. It was then that governments started to create policies and legislation to ensure interceptability.

---

service or other person to furnish facilities or technical assistance.' H.R.Rep. No. 107-236 (2001), at 62-3.

[8] See Directive 90/388/EEC from June 1990, which eliminated some particular, exclusive rights in the telecoms sector, with the exception, however, of voice telephony and mobile services and infrastructures. These exceptions were subsequently removed by later directives: 96/2/EC of January 1996 (liberalizing mobile and personal telecommunications), and 96/19/EC of March 1996, which determined that the entire telecommunications market should be liberalized in member states by January 1st, 1998.

3. Legal background: interceptability laws in U.S. and Europe

Before going into the interceptability laws, it is relevant to point out that, although the statutory frameworks to intercept in the U.S. and the Netherlands were introduced at about the same time, in 1968 and 1971 respectively,[9] and have developed in quite similar ways (for an extensive review, see Smits 2006), the use made of these powers differs significantly.

In the U.S., law enforcement uses interception relatively infrequently: in 2004, 1710 law-enforcement interception warrants were given. Note that one warrant may cover a long time and numerous connections; the average number of intercepts per order was 3,017 (Administrative Office of the United States Courts 2005). In the Netherlands, wiretap figures are not published, but occasionally, figures filter through. In 1999, 10,000 law-enforcement intercept warrants were given, 3000 for fixed telephony and 7000 for mobile telephones.[10] Since multiple warrants need to be given if a user has different telecommunications connections, the number of warrants may not be compared directly with that of the U.S. Still, the interception density in the Netherlands is certainly much higher, given that interception has been soaring since 2000 (Beijer et al. 2004), and given that the Netherlands has about 17 times fewer inhabitants than the U.S. In Europe, only the interception rate in Italy seems to be higher.[11]

This means that wiretapping is altogether a more important investigation power in the Netherlands than it is in the U.S., where for instance bugging and infiltration are more common. This fact should be borne in mind when the respective interceptability laws are looked at.

3.1. United States: CALEA

In the United States, the FBI launched two far-reaching legislative proposals in the early 1990s to mandate interceptability. Neither gained support by the legislature. A third, somewhat more palatable, proposal was made by the Clinton administration in February 1994. This proposal led, in a watered-down version, to the enactment in October 1994 of the Communications Assistance for Law Enforcement Act of 1994 (CALEA) (see for the legislative history, BeVier 1999). CALEA is set out in Title 47 of the U.S. Code (U.S.C.) under the title 'Interception of Digital and Other Communications'.[12] Its purpose is 'to preserve the ability of law enforcement to conduct electronic surveillance in the face of rapid advances in telecommunications technology'.[13] It has obligations for telecommunications carriers to ensure both the capability to intercept and a minimum capacity to intercept.

---

[9] U.S.: Omnibus Crime Control and Safe Streets Act 1968, Pub. L. No. 90-351, title III (note, however, that interception had been possible before this based on case law, since *Olmstead* v. *United States*, 277 U.S. 438 (1928)). Netherlands: Law of 7 April 1971 on Criminal Provisions for the Protection of Privacy [*Wet van 7 april 1971, houdende enige strafbepalingen tot bescherming van de persoonlijke levenssfeer*], *Staatsblad* 1971, 180. The *Staatsblad* is the Dutch official journal in which laws and regulations are published.

[10] *Kamerstukken II* 2000/01, 27591, nr. 2.

[11] See the table and figures mentioned in Albrecht, et al. (2003), p. 104.

[12] Pub. L. No. 103-414, 108 Stat. 4279, available at <http://www.askcalea.net/>. For Title 47 U.S.C., see <http://www4.law.cornell.edu/uscode/html/uscode47/usc_sup_01_47_10_9_20_I.html>. For an overview and critical analysis of CALEA, see BeVier (1999), Yeates (2001).

[13] <http://www.askcalea.net/faqs.html#05>.

Telecommunication carriers are common carriers of transmission or switching services for hire; CALEA explicitly excludes information services (47 U.S.C. §1001(8)).

The 'capability requirements' mean that equipment, facilities, and services are capable of, among other things, enabling the government to intercept communications content and to access call-identifying information (47 U.S.C. §1002 (a)). The 'capacity requirements' demand, *inter alia*, a certain number of simultaneously interceptable lines (47 U.S.C. §1003). The law provides a 'safe harbor' for telecom carriers if they comply with publicly available technical requirements or standards adopted by an industry association or standard-setting organization (47 U.S.C. §1006).[14] And, in turn, manufacturers of telecommunications equipment and providers of support services are required to make available to telecom carriers equipment and services that comply with the interceptability requirements (47 U.S.C. §1005(b)).

The CALEA obligations were originally intended to be in force by October 1998. However, the release of more detailed capacity and capability requirements by the Federal Communications Commission (FCC) was slower than expected, as well as fiercely debated, and the original capability compliance date was extended to 30 June 2000, and then again extended to 30 June 2002.[15] Subsequently, carriers could still apply for extensions of at most two years at a time, on the basis of 47 U.S.C. §1006(c). These extensions were liberally granted, particularly for carriers participating in the FBI's Flexible Deployment Program, wherein the carrier and the FBI work together to develop mutually agreeable solutions (Yeates 2001). In fact, significant exceptions relating to sparse funding in relation to the standards that have to be met (see *infra*, section 4) may mean that 'CALEA will probably never be fully implemented' (Yeates 2001).

3.2. Europe

3.2.1. EU Resolution on lawful interception

Interceptability legislation in Europe has been initiated within the European Union. The Council of Ministers of Justice and Home Affairs, on 17 January 1995, adopted a resolution 'on the lawful interception of telecommunications',[16] allegedly at the initiative of the Netherlands (Statewatch 1997).

This resolution requests EU member states to establish legislation that imposes interceptability requirements on telecommunications providers. The core text of the resolution is as follows:

> 1. The Council notes that the requirements of Member States to enable them to conduct the lawful interception of telecommunications, annexed to this Resolution ('the Requirements'), constitute an important summary of the needs of the competent authorities

---

[14] See <http://www.askcalea.net/standards.html> for an overview of available standards. Although "publicly available", the standards are not cheap: e.g., it costs USD352 to download standard J-STD-025-B-2003, <https://www.atis.org/atis/docstore/doc_display.asp?ID=2570>.

[15] Only for packet-mode communications, an earlier deadline of 19 November 2001 existed, see <http://www.askcalea.net/faqs.html#14>.

[16] Council Resolution of 17 January 1995 on the lawful interception of telecommunications (96/C329/01), *Official Journal* 4 November 1996, *available at* <http://www.privacy.org/pi/activities/tapping/eu_tap_resolution_1995.html>.

> for the technical implementation of legally authorized interception in modern telecommunications systems.
>
> 2. The Council considers that the aforementioned Requirements should be taken into account in the definition and implementation of measures which may affect the legally authorized interception of telecommunications and requests Member States to call upon the Ministers responsible for telecommunications to support this view and to cooperate with the Ministers responsible for Justice and Home Affairs with the aim of implementing the Requirements in relation to network operators and service providers.

The resolution contains an annex with the requirements of law-enforcement agencies for telecommunications to be intercepted. These requirements are actually very similar to the CALEA requirements[17] and the requirements drafted by ILETS, the International Law Enforcement Telecommunications Seminar.[18] This suggests a considerable degree of – informal – cooperation between the EU and the U.S. in the area of interceptability.

It took a remarkably long time for the resolution to be published in the *Official Journal* of the European Community – almost two years, suggesting perhaps a wish to let sleeping dogs lie. Indeed, very little public discussion took place in Europe about the resolution, which is often the case with decisions taken in the third pillar of the EU's decision-making structure.[19] This is in striking contrast with the U.S. situation, where CALEA was fiercely debated in Congress with significant publicity, academic criticism, and lobbying from privacy groups (BeVier 1999).

A resolution is less directly binding than another instrument that can be used in the EU third pillar, a framework decision. Moreover, the wording of the resolution is cautious. It only 'requests' the member states to 'call upon' its telecommunications ministers to 'support' the importance of interceptability requirements and to 'cooperate' to implement the requirements – altogether a remarkably non-binding statement.

Nevertheless, most if not all member states have passed interceptability legislation as a consequence of the EU resolution (cf. Büllingen and Hillebrand 2003). The Dutch legislation shall now be described as a different example of interceptability legislation.

3.2.2. Dutch law: Ch. 13 Telecommunications Act

The main interceptability legislation in the Netherlands was enacted in 1998, based on a policy document written in 1996. However, even before 1996, a start had been made with establishing interceptability requirements. When concessions for mobile telecommunications were granted in 1994, concession holders were obliged to ensure technical interceptability.[20] When it subsequently became clear

[17] On 29-30 November 1993, the Justice and Home Affairs Council adopted a resolution that aimed at comparing the interception requirements of the member states with those of the FBI. A *Memorandum of Understanding* that was sent to third parties to adopt the EU requirements, gave the contact addressess of the director of the FBI and the Secretary-General of the European Council (Statewatch, 1997). This suggests that there was a close collaboration between the EU and the U.S. in setting requirements, or at least significant influence from the U.S. on the EU.

[18] *See* <http://cryptome.org/ilets-snoop.htm>.

[19] The third pillar concerns police and justice affairs. Decisions in this pillar are taken by the Council of Ministers, i.e., the assembly of Ministers of the member states, and the European Parliament has little say over these decisions.

[20] Mobile Telecommunications Act [*Wet van 16 juni 1994 (mobiele telecommunicatie)*], *Staatsblad* 1994, 628, inserting art. 13g in the Telecommunications Facilities Act [*Wet op de telecommunicatievoorzieningen*] that

that making GSM interceptable required considerable investments, a law was passed in 1995 that stipulated that concession holders themselves had to pay for the investment, exploitation, and maintenance costs for ensuring interceptability.[21]

These laws paved the road for a telecommunications-wide interceptability policy. In 1996, the government launched the *Policy proposal lawful interception of telecommunications*.[22] Reasons to formulate a policy were liberalization, internationalization, and the pace of developments in telecommunications, and an increase in interception-related costs. Most of all, the policy referred to the EU resolution as a collection of requirements that must be implemented in Dutch law without fail.[23] Taking the resolution as a starting point, the document basically formulated six policy principles, the main ones being:

- All public telecommunications networks and services must be interceptable from the moment of introduction.
- Also service providers have to co-operate with interception and data delivery.
- The investment, exploitation, and maintenance costs for interceptability and security are borne by telecommunications providers. The operational costs for intercepts are borne by the government.

This policy was subsequently implemented in the Dutch Telecommunications Act (*Telecommunicatiewet*) of 1998 (hereafter: DTA), which replaced the Telecommunications Facilities Act, and in underlying regulations.[24] Chapter 13 of this act contains requirements for ensuring technical interceptability (art. 13.1), co-operation with law enforcement and national-security services (art. 13.2, 13.2a, 13.4), a provision on costs (art. 13.6), as well as provisions on dispute resolution (art. 13.3), information security (art. 13.5), and exemption in exceptional cases (art. 13.8). Existing networks and services that were not yet interceptable had to comply within nine months after the law took effect, that is, they had to be interceptable by 15 September 1999 (art. 20.13 DTA).

A major issue in the parliamentary debate on the Act concerned internet: the law stipulated that internet providers also had to ensure interceptability, but in 1998, no standards or tools were readily available for internet interception. Therefore, it was decided that Internet Service Providers (ISPs) could request exemption from the requirements until 15 April 2001.[25] In 2002, a group of ISPs established a central organization with movable interception devices that could be plugged in on members' infrastructures, so that not each and every single – small – ISP had to buy equipment on its own.

4. Basic questions in legal interceptability

An interceptability policy has to answer several basic questions. The most fundamental questions concern first which types of telecommunications have to be

---

included an obligation for concession holders to ensure interceptability.

[21] Intercepting GSM Act [*Wet van 23 november 1995 (aftappen van GSM)*], *Staatsblad* 1995, 594, inserting art. 64a in the Telecommunications Facilities Act [*Wet op de telecommunicatievoorzieningen*].

[22] *Beleidsvoornemen bevoegd aftappen telecommunicatie,* Parliamentary Series [*Kamerstukken II*] 1995/96, 24 679, nr. 1.

[23] *Kamerstukken II* 1995/96, 24 679, nr. 1, p. 7.

[24] Telecommunications Act [*Wet van 19 oktober 1998 (Telecommunicatiewet)*], *Staatsblad* 1998, 610.

[25] *Beleidsregels ontheffingsverlening aftapbaarheid Internetdiensten*, Stcrt. 1999, 86, p. 9; *Beleidsregels ontheffingsverlening aftapbaarheid Internetdiensten*, Stcrt. 2000, 133, p. 37.

interceptable, second what is the scope of the interceptability requirements, and third who bears the costs for the interceptability. In this section, the U.S. and Dutch answers to these questions are compared.

4.1. Who shall comply?

4.1.1. Networks and/or services?

The first question is whether interception should take place at the network level, at the service level, or at both. Interception at the network level implies that all data passing the network are intercepted and are subsequently to be sorted out – to retrieve only those data coming from or going to the interception target – and interpreted, i.e., to put the raw signals in the right format. This has the advantage that all communications from the interception target that pass the network are intercepted, which is particularly advantageous if the target uses numerous services from different providers; it has the drawbacks, however, of overcollection, since data from non-targets passing the network might be intercepted as well, and of the extra effort of interpreting the raw signals. Intercepting services has the opposite advantages and drawbacks. It is hard to make an *a priori* choice between the two: a service interception will often be preferable but may not always be workable, and so, network interception may sometimes be the only possibility. It is not surprising, therefore, that both the U.S. and the Netherlands have opted for dual interceptability. However, the Dutch law seems to be further-reaching, since it includes all telecommunications services, including those offered by Internet Service Providers (ISPs, see also the following section). CALEA excludes information services and certain ISPs and in that respect seems to rely somewhat more on network interception.

4.1.2. What networks and services?

Given that both network providers and service providers may in principle be required to ensure interceptability, the main issue is how to define the relevant networks and services.

The definitions in the Netherlands tag on to the definitions in the general telecommunications regulation of the DTA, except that they exclude the media services that are also covered by this act. Public network providers and public service providers fall under the scope of Chapter 13 DTA. The first are defined as electronic communication networks that are wholly or partly used for offering public telecommunications services. These services are defined as services available to the public that consist of transferring signals across an electronic communications network, except media broadcasts (art. 1.1 sub ee and ff DTA). This includes all service providers who transfer signals. The argumentation for this broad applicability to service providers was that, in modern systems, also service providers can exploit switches, according to the Explanatory Memorandum.[26] The obligations are restricted to 'public' telecommunications, which means that there is a public offer that, in principle, everyone can accept against the conditions mentioned in the offer. For private telecommunications, another provision was constructed. On the basis of art. 13.7 DTA, the Minister could designate specific private networks or services that

[26] *Kamerstukken II* 1996/97, 25 533, nr. 3, p. 124.

have to meet one or more interceptability requirements, in the interest of national security or law enforcement; in such a case, the government will have to pay for the costs of interceptability. However, art. 13.7 has not entered into force, and it is doubtful that it ever will. Therefore, private telecommunications are – for the time being – completely excluded.

CALEA uses definitions of its own, separate from the Communications Act of 1934 that regulates telecommunications. CALEA covers telecommunications carriers, i.e., 'a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire'. Explicitly included are mobile service providers, and explicitly excluded are information service providers[27] (47 U.S.C. §1001(8)). The definition fairly closely resembles the Dutch definition. Both cover communications transfer and switching at the network and service level, and both exclude storage services.

There are some small but significant differences, however. Dutch law includes electronic messaging services which CALEA excludes. Moreover, all ISPs fall under the Dutch law, whereas some kinds of ISPs are exempt from CALEA. BeVier 1999 mentions internet access providers such as AOL and Compuserve to be exempt, although that may be a far-fetched interpretation since access services involve transmission of communications.

Another difference is that the DTA has a more fixed definition: all public networks and services are included. There is considerable confusion over the interpretation of the term 'public' (Koops et al. 2005), but once the supervising authority OPTA has decided that a network or service is public (or private), it falls definitively within (or without) the scope of the law. CALEA, which in its 'for hire' uses a similar element as the Dutch 'public', contains a flexible element for closed telecommunications: it also covers services 'to the extent that the Commission [FCC] finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this subchapter' (47 U.S.C. §1001(8)(B)(ii)). In other words, when a service is not a common carrier for hire, but in practice substitutes local telephony, it can be designated by the FCC as an interceptability service.[28] In this respect, the U.S. law seems broader than the Dutch law, although perhaps the Dutch National Regulatory Authority OPTA might just as well deem a service that significantly substitutes local telephony a 'public' service. The main difference is that the U.S. definition is more precise and to the point, since it refers to 'substantial use' and the public need to intercept as a criterion, whereas the Dutch element 'public' merely relates to an offer 'to the public' as interpreted in the telecommunications market, largely in view of antitrust regulation. The evaluation of Ch. 13 DTA recommended to look for a better criterion than 'public' (Koops et al. 2005); perhaps CALEA may serve as an example here.

These subtle differences in the scope of the laws may turn out to be significant when new telecommunications services are considered (see section 6).

---

[27] The term "information services" means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; this includes information storage facilities, electronic publishing, and electronic messaging services, but excludes any capability for a telecommunications carrier's internal management, control, or operation of its telecommunications network (47 U.S.C. §1001(6)).

[28] This provision was invoked by the FCC to bring facilities-based broadband Internet access providers and interconnected VoIP providers under the scope of CALEA (FCC 2004; FCC 2005).

4.2. What must telecom operators do?

The obligations for telecom operators under the interceptability laws concern both the capability to intercept and a sufficient capacity to intercept.

4.2.1. Capability

The Dutch Telecommunications Act uses a very generic description of capability: providers offer telecommunications only if these are ‘interceptable’; what is interceptable in a technical sense can be detailed in an Order in Council or subordinate regulations (art. 13.1 DTA). These latter legal instruments can be established by the Minister without discussion in parliament or formal consultation with affected parties.

The relevant Order in Council was published simultaneously with the Telecommunications Act and was effective at the same date, 15 December 1998.[29] It describes functional requirements: interception must be possible without delay, undetectable to the users, and with a quality comparable to the original communication; it must be transported without delay to the requesting government agency or agencies, in accordance with a technical protocol to be determined by regulation; and the provider must undo encryption that he applied himself. Moreover, telecommunications transferred via a switch to another public telecommunications network must be interceptable.

The requirements of the Order in Council can be further specified in a ministerial regulation. An interim regulation was in effect since 15 December 1998, subsequently extended, only to be replaced by a definitive regulation on 15 June 2001.[30] The hassle of the interim regulations was caused by the fact that the technical protocols for transferring intercepts to the government agencies (often referred to as handover protocols) were not forthcoming rapidly. In fact, the final 2001 regulation did not designate a protocol but referred, like the interim regulations, to protocols then ‘in use’ with the agencies. In order to create at least a semblance of legal certainty, some requirements were specified in the regulations, notably that all signals have to be forwarded, including activation of telephone conferencing and call forwarding, and that call-identifying information (connection numbers, date and time) must be provided along with the intercept itself.[31]

Besides capability to intercept, the capability of providing call-identifying information is also relevant to government agencies, who after all have legal powers to request user data or traffic data. Art. 13.4 DTA contains obligations for telecom providers to provide user data, that is, name, address, number, and the kind of services used. Art. 13.2a DTA, in force since 1 September 2004, requires providers to deliver traffic data. However, there is no real requirement *to be able* to deliver user or traffic data. The one exception is that mobile operators have to retain certain

[29] Decree on intercepting public telecommunications networks and services [*Besluit aftappen openbare telecommunicatienetwerken en -diensten*], *Staatsblad* 1998, 642, amended by *Staatsblad* 2001, 262.

[30] Temporary regulation on intercepting public telecommunications networks and services [*Tijdelijke regeling aftappen openbare telecommunicatienetwerken en -diensten*], *Staatscourant* 1998, nr. 238, p. 10; Temporary regulation on intercepting public telecommunications networks and services 2000, *Staatscourant* 2000, nr. 41, p. 8; Regulation on intercepting public telecommunications networks and services [*Regeling aftappen openbare telecommunicatienetwerken en -diensten*], *Staatscourant* 2001, nr. 107, p. 20.

[31] The second interim regulation also specified that ‘real-time’ transfer to the government implied a delay of at most 300 ms for circuit-switched services and 1 s for packet-switched services, but this was dropped in the final regulation.

data for three months – time, number, and cell location of calls –,[32] because in this way, the number of prepaid-card holders that need to be intercepted can be traced.[33] There are no other data retention requirements, at least not yet.[34] For telephony user data, which are presumed to be available anyway, there are further requirements to keep these available in an interconnected database called CIOT, to be updated every 24 hours, which can be accessed by the investigation officers; a similar obligation is envisioned for internet user data in 2006,[35] even though that is fundamentally a different situation since internet numbers, such as dynamic IP addresses, are much more volatile than telephony numbers.

CALEA lists four functional capability requirements in 47 U.S.C. §1002(a):

1. to expeditiously isolate and enable the government to intercept the wire or electronic communications of a subscriber, in real-time ('concurrently') or so much later as is acceptable to the government;
2. to expeditiously isolate and enable the government to access call-identifying information that is reasonably available to the carrier; this excludes location data if the government only has authority to collect traffic data;[36]
3. to deliver the intercepts and information to the government in such a format that government equipment can transfer these outside the carrier's;
4. to keep the interception secret from the subscriber, and to protect communications that are not included in the intercept warrant.

As to encryption, carriers have to decrypt communications encrypted by users only if the carrier provided the encryption and has the means to decrypt (47 U.S.C. §1002(b)(3)); the law is silent on encryption used by the carrier himself, but by implication of the foregoing, he will likely have to decrypt in those cases as well. This is somewhat further-reaching than the Dutch provision, which requires only decryption of self-applied encryption, but since the Netherlands have a general requirement of decryption by people likely to know the decryption means (art. 125k Dutch Code of Criminal Procedure),[37] there is no material difference.

---

[32] Art. 13.4 para. 2 DTA *juncto* art. 7 Decree on special collection of number data [*Besluit bijzondere vergaring nummergegevens telecommunicatie*], *Staatsblad* 2002, 31.

[33] Supposing that the police observes the prepaid-card interception target to call on two or more occasions, they can then request mobile operators to do a search on which – presumably unique – number phoned at these specific times on these locations.

[34] In the EU, a measure is forthcoming to require telecommunications providers to store all their traffic data ('data retention') for a period of six months to two years. See the proposal for a *Directive on the retention of data processed in connection with the provision of public electronic communication services*, COM(2005) 438final, 21.9.2005, accepted by the European Parliament on 14 December 2005, available at <http://www.europarl.eu.int/oeil/file.jsp?id=5275032>. The Directive is likely to replace the European Council's *Draft Framework Decision on the retention of data (...) for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism*, launched 28 April 2004, <http://register.consilium.eu.int/pdf/en/04/st08/st08958.en04.pdf>, with numerous later revisions, see the October 2005 version <http://www.statewatch.org/news/2005/oct/council-data-ret-draft-10-oct-05.pdf>.

[35] Decree on delivering telecommunications data [*Besluit verstrekking gegevens telecommunicatie*], *Staatsblad* 2000, 71, in force since 1 September 2004. The CIOT is the Central Information Point for Telecommunications Investigation (*Centraal informatiepunt onderzoek telecommunicatie*).

[36] Note, however, that the location of the cell in which a mobile phone is calling was later added as call-identifying information, see *infra*.

[37] Art. 125k CCP is usable if law enforcement copies encrypted communications when in storage, e.g., e-mail stored on a user's computer in a search. For encrypted communications intercepted in transport, there is currently no decryption order, but the Computer Crime II Bill (*Wetsvoorstel computercriminaliteit II*) proposes such a power in art. 126m para. 6 and art. 126t para. 6 CCP; *Kamerstukken I* 2005/06, 26 671, nr. A.

Finally, there is a specific requirement for mobile services, requiring carriers to provide identifying information in real-time of other carriers to which the mobile communication is switching when an intercept is taking place (47 U.S.C. §1002(d)).

There are several limitations to the requirements. First, it is explicitly stated that the requirements do not authorize law enforcement to require specific equipment or configurations to be used, nor to prohibit specific equipment, services, or features (47 U.S.C. §1002(b)(1)). More importantly, the requirements can only be enforced if law enforcement has no reasonable alternative for intercepting or accessing traffic data, and if technology is reasonably available to comply with the requirements (47 U.S.C. §1007(a)). Similarly, carriers can request one or more extensions of the compliance date for a period of maximum two years, which may be granted if timely compliance is not reasonably achievable (§1006(c)). Also, telecommunications in operation before 1 January 1995 are exempted, unless they are replaced, significantly upgraded or changed afterwards (47 U.S.C. §1007(c)(3)). And most crucially, telecommunications installed or deployed after 1 January 1995 need only be made interceptable if the FCC determines, upon a carrier's request, that compliance is reasonably achievable, taking into account a non-exhaustive list of ten factors (47 U.S.C. §1008(b)). What is reasonably achievable is closely related to the issue of cost (see *infra*, section 4.3).

The capability requirements as listed above have to be detailed in interception equipment and standards.[38] 47 U.S.C. §1006(a) stipulates, somewhat optimistically, that the Attorney General, in coordination with law enforcement, shall consult with industry, standard-setting organizations, user groups, and state utility commissions to 'ensure the efficient and industry-wide implementation of the assistance capability requirements'. A standard was proposed in 1997 by the Telecommunications Industry Association, called the 'J-Standard', but the FBI was not satisfied and proposed nine more requirements, often termed the 'punch list'. The FCC, in its role as arbiter (47 U.S.C. §1006(b)), accepted six of these in a Final Implementation Order. This was challenged in court, however, and four more punch-list items were removed, leaving only a requirement to include cell-location data in call-identifying information, and a requirement to access traffic data in packet-switched services on the basis of an authority to collect traffic data.[39] The extended J-Standard now forms a technical standard, which provides a 'safe harbor' for carriers who comply with it (47 U.S.C. §1006(a)(2)); it is not a mandatory standard, however – carriers may use other means to achieve the same end.

The capability requirements in U.S. and Dutch law turn out by and large to be similar. They share the major requirement that relevant networks and services must be able to isolate communications to be intercepted and to transfer these in a proper format to the government.

CALEA has more explicit provisions on traffic data, however: call-identifying data have to be isolatable and transferable as well, as far as they are reasonably available. This means that technical measures may have to be taken to be able to

[38] The following description of the standard-setting process is based on Yeates (2001), pp. 146-9, where references to the standards can be found.

[39] This was contested since in packet mode, communications content and traffic data are both contained in the same packets, raising doubts that law enforcement would be able to access content on the basis of a traffic-data order, for which no court warrant is needed.

isolate traffic data, notably in packet-switched networks. Dutch law basically only has a requirement for certain traffic data in mobile communications, but otherwise apparently assumes that the carrier is able to provide traffic data anyway; the carrier need take no measures to ensure this. CALEA also has an explicit requirement for mobile carriers to provide identifying information of other carriers to which mobile communication is switching during an intercept, so that roaming (the use as a visitor of mobile networks other than the home network) does not hamper the interception. This is quite understandable, since roaming within the national footprint is a much more regular event in the U.S. than it is in any European country. Dutch law, nevertheless, has a somewhat similar requirement that telecommunications transferred to another network be interceptable, but this is much vaguer than giving real-time information about the following provider.

A major difference between the two is the treatment of existing equipment. In the U.S., pre-1995 equipment need not be adapted, unless and to the extent that the government decides to pay for this. In the Netherlands, pre-1998 equipment had to meet the requirement in any case, regardless of whether or not the one-off reimbursement (see section 4.3) was given or not. The same difference holds with new telecommunications: new Dutch networks or services have to meet the requirements in any case, whereas U.S. equipment need do so only after it has been decided to be reasonably achievable in the particular case (cf. *infra*, sections 4.3 and 4.4).

4.2.2. Capacity

Currently, Dutch law does not have specific capacity requirements, although it did so in the past. In the Order in Council of 1998 and the interim regulations, capacity requirements were included: simultaneous intercepts had to be possible for 0.01 per cent of the number of users, with a minimum of 30 (with telephony), for 0.02 per cent of the number of users (with leased lines), and 0.15 per cent of active SIM (Subscriber Identity Module) cards (with GSM).[40] However, they were dropped in the amended Order in Council and the final regulation of 2001, which now merely says that a provider has to comply with each order without delay.[41] This means that providers have to decide themselves how much capacity they want to reserve; the risk of not being able to comply if too many simultaneous intercepts are required, is theirs.[42]

In contrast to the Dutch law, CALEA presupposes specific capacity requirements for simultaneous interception. 47 U.S.C. §1003(a)(1), again rather optimistically, stipulates that the Attorney General, after consultation, issue within a year after 1 October 1994 notices of capacity requirements, including both the actual number of simultaneous intercepts expected and a maximum capacity. However, such notices were not proposed until March 1998 for certain types of telecommunications, leaving providers another three years to comply with these. Even more than the capability requirements, the capacity requirements relate to costs: carriers have to be reimbursed for costs ‘directly associated’ with meeting the capacity requirements,

[40] Artt. 3-5 Temporary regulations 1998 and 2000, *supra*, note 30, *juncto* art. 2(b) Decree, *supra*, note 29.

[41] Artt. 3-5 Regulation 2001, *supra*, note 30; art. 2(b) was struck from the Decree by amendment, *Staatsblad* 2001, 262.

[42] Regulation on intercepting public telecommunications networks and services [*Regeling aftappen openbare telecommunicatienetwerken en -diensten*], Explanation, section 4, *Staatscourant* 2001, nr. 107, p. 20.

and they are considered to be in compliance until they are actually reimbursed (47 U.S.C. §1003(e)).

Here a major difference between U.S. and Dutch law can be perceived. The U.S. has explicit – if heavily contested – capacity requirements, where the Netherlands does not. This means that CALEA ensures legal certainty in this respect – the carriers know just what they have to do – whereas Dutch law leaves the carriers in the dark, so that they run the risk of infringing the law if they do not invest in sufficient capacity, even if the government does not tell what is considered sufficient.

4.3. Who pays?

In an area where public and private interests meet so intensely as here, the question who bears the burden of costs is crucial. The distribution of costs was a central issue in both the Dutch and the U.S. legislative processes.

In the Netherlands, the policy proposed that all investment, exploitation, and maintenance costs for interceptability are borne by the providers.[43] Although some opposition was voiced in parliament, the proposal was implemented in the law: providers have to pay for interceptability (art. 13.6 para. 1 DTA). The main reasons given for this cost allocation were that the government's costs for interception were snowballing already, and that it is more cost-effective to let the providers pay, because they will look for the cheapest solutions; if the government were to pay, they could hardly determine whether a provider charged reasonable costs. The argument that may have ultimately convinced parliament to go along with this, was an estimate by the minister that the investment costs for interceptability would be no more than 1% of the total investment made by operators, and usually less, if the operator knows beforehand that he has to build in interceptability.[44] The law's evaluation suggested that the actual costs turn out to be substantially more than this 1% (Koops et al. 2005), but there is no way for providers to request reimbursement. The provision is currently being challenged in court by internet provider XS4ALL, notoriously critical of law enforcement powers.[45]

The one exception made is a one-off reimbursement that providers of telecommunications already in use before 1998 could request; 2.9 million guilders (roughly 1.5 million US$) were allocated for this from the government budget, being half of the estimated total investment costs.[46] It cannot be determined whether this money has actually been paid; no records of this exist (Koops et al. 2005).

CALEA has more liberal reimbursement provisions.[47] 500 million US$ were appropriated from the government budget for paying interceptability costs (47 U.S.C. §1009). As in the Netherlands, it is difficult to determine exactly how much

---

[43] The operational costs for intercepts are borne by the government, but that issue is left aside here.

[44] See notably *Kamerstukken II* 1997/98, 25 533, nr. 82, p. 5, *Handelingen II* 31 maart 1998, 67-5008; *Kamerstukken I* 1997/98, nr. 309b, p. 21, and nr. 309d, p. 5; *Handelingen I* 13 oktober 1998, 3-45, 3-63, and 3-67. The estimate was based on a rough estimate for GSM, but it was somehow subsequently extrapolated as an estimate for any kind of telecommunications.

[45] Summons submitted on 7 March 2005, <http://www.xs4all.nl/nieuws/pdf/XS4ALLdagvaarding.pdf>. An overview of the case is available in Dutch at <http://www.xs4all.nl/nieuws/overzicht.php?dos=Aftapkosten&taal=nl&msect=nieuws>.

[46] *Beleidsvoornemen bevoegd aftappen telecommunicatie,* Parliamentary Series [*Kamerstukken II*] 1995/96, 24 679, nr. 1, p. 11 and 21.

[47] See also <http://www.askcalea.net/cost.html>.

money has been paid to telecommunications carriers, but it is clear that the available budget is significantly higher in the U.S. It can be spent in the following ways. First, as mentioned above, the government must pay for direct costs made to meet capacity requirements; if not, the carrier is deemed to be compliant. Second, for adapting telecommunications in use before 1 January 1995 to meet capability requirements, reimbursement may be requested, and if this is not forthcoming, the carrier is understood to be compliant (47 U.S.C. §1008(a) and (d)). Third, and most importantly, the costs for making new telecommunications meet the capability requirements need only be paid by the carrier as far as they are 'reasonable'. A carrier can petition the FCC to determine whether interceptability is 'reasonably achievable' for his telecommunications; the Commission must then 'determine whether compliance would impose significant difficulty *or expense* on the carrier or on the users of the carrier's systems' (emphasis added), taking into account at least ten factors, including the effect on rates for basic residential telephone service; the effect on the nature and cost of the equipment, facility, or service at issue; and the financial resources of the telecommunications carrier (47 U.S.C. §1008(b)(1), factors (B), (E), and (H)). That is, the burden of the financial cost for interceptability has to be weighed against the needs of law enforcement and national security to make this particular telecommunications network or service interceptable (which is factor (A)). If the cost is deemed too high by the FCC, the government must pay the additional costs (i.e., above the reasonable costs) or else the carrier is deemed to be compliant (47 U.S.C. §1008(b)(2)).

The cost provisions in CALEA have also encouraged the government to actively engage in a process to develop and make available cost-effective interception equipment. As a result, in the FBI's reimbursement strategy, carriers can – according to the FBI – often receive CALEA-compliant software at no charge or at nominal costs.[48]

It is in the cost allocation that the major difference between the U.S. and the Dutch laws is perceivable. The Dutch approach is to allocate all costs for investments to the carriers, where the U.S. approach is to allocate only reasonable costs to carriers.

For equipment already in use, the Dutch government offered to pay about 1.5 million US$, being half of the estimated costs; the U.S. allocated 500 million US$ for this (but also for other things), and has to pay for all real costs for pre-1995 equipment. The U.S. thus appropriated relatively more to fund interceptability, 333 times as much as the Netherlands, which is roughly a factor 20 more than the population ratio or telephone-line ratio would suggest.[49] This is understandable, since Dutch carriers are required to pay more themselves. A major difference, however, is that Dutch carriers had to adapt first and could request reimbursement only afterwards, if still available, whereas U.S. carriers could wait for the government to explicitly allocate money to them and only then to adapt the equipment. Similarly, capacity requirements also have to be funded by the U.S. government, whereas Dutch carriers have to pay for capacity themselves. And most

[48] <http://www.askcalea.net/faqs.html#12>.

[49] ITU statistics for 1998, available at <http://www.itu.int/ITU-D/ict/statistics/at_glance/basic98.pdf>, indicate a population ratio of 17:1 (270 million U.S. inhabitants, 16 million in the Netherlands), and a telephone-line ratio of 19:1 (180 million U.S. telephone lines, 67 per 100), against 9.3 million Dutch ones, 59 per 100).

significantly, for new telecommunications, U.S. carriers – in contrast to Dutch carriers – only have to pay reasonable costs, to be determined in advance before they start an interceptability process. Of course, the proof of this pudding is in the eating of deciding what is 'reasonable', but the law lists ten factors and thus requires the FCC to weigh the interest of law enforcement (which is one factor) with the interests of carriers, users, and the market (as set out in nine factors). Therefore, the FCC is forced to go into explicit consideration of the interests of carriers and the market and must therefore provide strong arguments if it gives more weight to the law-enforcement interest in a particular case. (In the current climate, of course, the threat of terrorism is likely to be seen as a strong argument in this respect.)

Moreover, a significant difference is that in the U.S., efforts are made to ensure that CALEA-compliant equipment is available, partly through CALEA obligations for manufacturers (47 U.S.C. §1005) and partly through the financial incentive for the FBI to engage manufacturers in standard-setting, so that it is more likely that reasonably cheap CALEA solutions are available in the market. In the Netherlands, equipment manufacturers are left out of the picture, and it is left to carriers to negotiate with manufacturers for cost-effective solutions. Since the Dutch telecommunications market is small, and since Dutch standards diverge somewhat from international standards – if available, there is little incentive for manufacturers, who often operate globally, to offer affordable interceptability equipment tailored to the Dutch market.

4.4. Checks and balances

Where public and private interests clash, checks and balances are of prime importance. The scope of interceptability obligations, including public and private funding, is the result of political decision-making; as such, the scope is laid down in law. However, this law can never be definitive and unequivocal: the definitions of just which carriers have to comply with the law, of exactly what 'interceptability' means, and of exactly when private parties have to pay, are bound to require interpretation. A vital question in analyzing the scope of the laws, therefore, is what checks and balances are laid down in the law itself to deal with its interpretation.

The Dutch law has few real checks and balances built-in. There is one provision on dispute resolution, but this only relates to disputes over the technical specifications of how to transport intercepts to the government. Disputes over when a carrier is deemed 'public', what 'real-time' is, what capacity is needed, etcetera, are not regulated and hence left to be decided in court. What is more, no indications are given how to decide in future when a new network or service falls under the scope of the law. It is left to the national regulatory authority, OPTA, to decide whether it concerns an offer to the general public, with few guidelines for interpreting this (Koops et al. 2005). As soon as this is answered affirmatively, all obligations of the Telecommunications Act must be met. There is no escape clause if, for instance, the new network or service is not directly relevant to law enforcement or if it is very expensive to build in interceptability.

The Dutch absence of specific[50] checks and balances is particularly noticeable when CALEA is considered. As was noted above, a major balance has been built-in

[50] Of course, general checks and balances apply, such as the framework of the EU Treaty, under which it might perhaps be argued that the Dutch law has been based upon an unlawful EU decision since the matter should be

by allowing the FCC to determine, when requested by a carrier, whether it is reasonable to require this carrier to implement interceptability. The FCC must not only look at financial consequences for the carrier, but also at other factors that may be at stake (47 U.S.C. §1008(b)(1) under C, F, G, I, and K):

- The need to protect the privacy and security of communications not authorized to be intercepted.
- The effect on the operation of the equipment, facility, or service at issue.
- The policy of the United States to encourage the provision of new technologies and services to the public.
- The effect on competition in the provision of telecommunications services.
- Such other factors as the Commission determines are appropriate.

That is to say, the scope of CALEA also depends on the impact of interceptability on privacy and security, innovation, and competition. Privacy and security are also mentioned in § 1002(a)(4)(A): interceptability must be built-in in such a way that only communications are intercepted for which authorization has been given; that is, the prevention of over-collection is an explicit requirement for interception technology.

Two more checks and balances are relevant. The first is that a financial incentive is built-in for the government to spend the money on those networks or services where the government need for interception is highest. For carriers with pre-1995 equipment and with newer telecommunications for which interceptability is not reasonably achievable, a fund of 500 million dollars is available to pay for interceptability. Since these carriers are in a safe harbor from which they can only be removed if the government funds their costs, it is up to law enforcement to decide where they will spend CALEA funding. This ensures that only those networks or services are targeted where law enforcement reasonably expects to make the most interceptions. This is in striking contrast to the Netherlands, where telecommunications have to be made interceptable even if the government is not likely to use interception there in the foreseeable future.

The other safeguard worth mentioning is that the standard-setting process for detailing the interceptability requirements is explicitly made a joint and public effort in the U.S.[51] Both the capability requirements (§ 1006(a)(1)) and the capacity requirements (§ 1003(a)(1)) require the Attorney General to consult not only with law enforcement, but also with standard-setting organizations and telecommunications users, or with carriers and equipment manufacturers, respectively. The debate over the J-Standard shows that this consultation is not quite a friendly tea-party – which can never be the case where interests clash so clearly – but at least it takes place in public. The ensuing court procedure also adds a public element to the whole process. And it is this element of openness that provides an extra safeguard, in that public scrutiny can protect against over-intrusive or unreasonable government decisions. Here as well, the U.S. situation differs ostensibly from the Dutch one, where consultation is limited to standard setting for intercept transfer protocols, hidden from the public, and where all other interpretative choices of what constitutes interceptability are either one-way

---

regulated in the first rather than the third pillar (see note 19), or that it hampers fair competition because the financial implications are larger for Dutch companies than for companies in other EU countries with different interceptability policies.

[51] CALEA 'contains a number of provisions to guarantee accountability and provide opportunities for public scrutiny of and participation in the implementation process', notes BeVier (1999).

decisions by the government or, if these are challenged by carriers, results of invisible discussion between government agencies and – often only the large – carriers. No court procedures have been initiated so far – the case of *XS4ALL* v. *the Netherlands* will be the first to bring some public visibility to decisions about the scope of the Dutch law.

5. Future developments in telecommunications

The interceptability policy in the Netherlands is largely based on the telecommunications landscape of the mid-1990s. An evaluation of the Dutch policy and legislation that we have conducted in 2004-2005 shows that several policy choices create problems now that this landscape has radically changed. In the U.S., the debate over facilities-based broadband access and VoIP shows that the interpretation of CALEA – what exactly is an 'information service' or 'switching'? – is also raising questions (Adrian 2005).[52] At the time of writing (June 2006), the D.C. Court of Appeals has upheld the FCC's decision to bring both under the scope of CALEA,[53] and facilities-based broadband access providers and interconnected VoIP providers will have to comply by 14 May 2007 (FCC 2006). The FCC's interpretation of CALEA is still contested, however, and the debate is likely to continue.[54]

This may be the first instance of a battle between law enforcement and the market over telecommunications innovations in the years to come. Are the laws prepared for the future in that they will ensure an on-going ability to intercept telecommunications? In this section, some of the major developments in telecommunications that put pressure on the interceptability legislation shall be examined. First technical developments are discussed, and then market developments.

5.1. Technical developments

There are numerous technical developments that pose challenges to interceptability. Figure 1 presents a selection of nine of the most important ones. Each of these developments will be discussed below.

[52] The FCC's struggle to define which VoIP services should fall within the scope of CALEA is revealing in this respect. First, a distinction was made between 'managed VoIP' (inside CALEA scope) and 'non-managed VoIP' (outside CALEA scope). The distinction was subsequently abandoned as being unmanageable, being replaced by a distinction between 'interconnected VoIP' (inside CALEA scope) and 'non-interconnected VoIP' (outside CALEA scope). See Adrian (2005) and FCC (2005). This illustrates that determining the scope of interceptability legislation with respect to new networks or services requires careful analysis not only of the technology but also of the business models and market positions at issue.

[53] *ACE* v. *FCC*, 9 June 2006 (D.C. Cir.), available at <http://www.epic.org/privacy/wiretap/ace_v_fcc.pdf>.

[54] Cf. the statement of senator Patrick Leahy, chief sponsor of CALEA in Congress in 1994: 'Stretching a law written for the telephone system of 1994 to cover the Internet of 2006 is simply inconsistent with congressional intent.' Available at <http://leahy.senate.gov/press/200606/060906.html>. Compare also the rather fierce dissenting opinion of Judge Edwards in *ACE* v. *FCC*, 9 June 2006 (D.C. Cir.), calling the FCC's reasoning 'utter gobbledygook, and it certainly cannot be what Congress intended'.

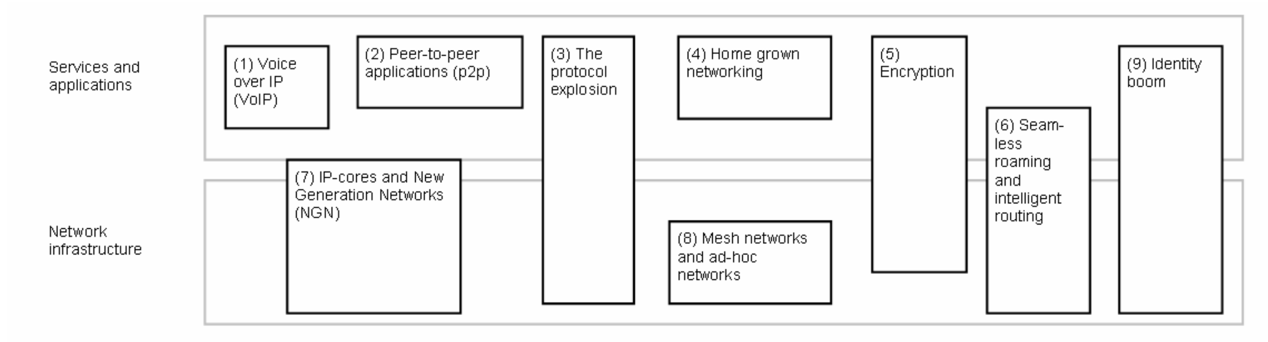

Figure 1. Overview of selected technical developments

(1) **Voice over IP services (VoIP)** services are clearly on the rise. Using packet-switched technologies (as opposed to the circuit-switched technologies in traditional telephone networks), they promise substantial economies on operating expenses to network operators. Although there are still a few pending issues such as the quality of service and emergency calls (Chong and Matthews 2004), many observers expect that these services may eventually replace all circuit-switched telephony services. VoIP services can be easily deployed on a wide array of underlying broadband access networks, including those on the basis of Digital Subscriber Line (DSL) and cable TV technologies. In recent years, such services have been introduced by operators all around the world, both by incumbents and by new entrants. They are often accompanied by new tariff structures, such as unmetered (unlimited) national calls. VoIP comes in many flavors, including the popular H.323, Multimedia Gateway Control Protocol (MGCP) and Session Initiation Protocol (SIP) protocols. They do not only vary on the technical protocol level, but they also have different overall architectures (Durkin 2003; Davidson and Peters 2000). One challenge that VoIP poses to interceptability is that the setup of calls and the actual traffic are typically totally separated. A service provider might be involved in setting up the call, but the actual data traffic between the two calling parties may be handled by totally different firms with whom the VoIP provider might not even have any relation. As a result, the actual call data are never seen by the VoIP provider. In the Netherlands, for instance, this fact poses serious difficulties for service providers, as the Dutch law obliges them to intercept traffic if requested to do so (see above). Alternatively, a service provider could route all voice traffic via its own switching facilities, but this is less efficient in many respects and in fact undoes many of the particular advantages of VoIP. As a result, if the innovative potential of VoIP is to be maintained, building in interceptability raises serious security concerns (Bellovin et al. 2006). Another particular problem is that new formats have to be developed to deal with the specific nature of VoIP and to cope with differences between the various VoIP flavors. A straightforward mapping of the various VoIP protocols to the traditional Public Switched Telephone Network (PSTN) telephony functions is simply not possible, no matter how much authorities would like it to be that way.

(2) In recent years, a remarkable increase in the use of **peer-to-peer (p2p)** applications can be observed (Oram, 2001). Starting with the – often illegal - exchange of music files, p2p applications are now aiming at a wide array of legal

telecommunications services, including telephony, messaging and chatting (Verma, 2004). A popular example is the p2p telephony program Skype. Now, instant messaging programs such as MSN Messenger, Yahoo Messenger, and Triton offer p2p telephony services as well. In fact, all three have added video chatting to their latest releases too. From the perspective of interception legislation, p2p systems may pose various problems. If the law relies on obligations to service providers, the issue is that with p2p applications there simply is no service provider. Instead, all technical functionalities are performed by the programs that are installed on the computers of the individual participants. One could attempt to intercept p2p telecommunications on the underlying telecommunications infrastructure network, but the problem there is that peer-to-peer applications enable encryption by default, possibly making the data stream indecipherable to authorities. Also, suspects may be using the same p2p service from different networks and different IP-addresses. Moreover, p2p systems are still under development and with the more advanced file-sharing versions, bits of information do not come from one single source, but small bits of information are gathered from numerous other users, further complicating interception.

(3) A further relevant development is what could be referred to as the **protocol explosion** in telecommunications. Each day, numerous new protocols are being put into service. These could be for existing types of service, but also for totally newly devised applications. Also, the diversity of peripheral equipment is increasing at a great pace. Not only gaming consoles but also a large variety of domestic equipment will probably be equipped with telecommunications ports. One example is an internet-enabled fridge that automatically compiles a shopping list of necessities and communicates that to a on-line shop. Very often, such new types of device use unique protocols. A game console can even use different protocols for every different game or application it runs. Another complication is that protocols are more and more frequently subject to changes (Bekkers 2005). Especially web-based applications (such as those used for Hotmail, Gmail and Outlook Web Access) may change their protocols without requiring changes at the client side. Many new protocols do not have the strict revision and change management that is associated with formal standards. Often, new protocols or new versions of protocols are not fully documented and, in the case of proprietary protocols, no documentation may be available at all. All of this challenges the ability of the authorities to translate data streams into comprehensible information.

(4) Yet another development is known as **home-grown networking**. Whereas in the past users had to rely on telecommunications providers in order to use services, they can now often create these themselves. It is not too complicated for an advanced user to install a private email server or hosting server at home. It is envisaged that, in the near future, standard software will allow almost every user to do so. This obviously affects the degree to which authorities can turn to service providers for intercepts.

(5) The issue of **encryption** has of course long been on the agenda of those involved in interception (cf. Koops 1999). It is not a new fact that people aware of the risks of being intercepted may protect themselves with advanced end-to-end

encryption. Publicly available algorithms such as Advanced Encryption Standard (AES), Triple Data Encryption Standard (Triple DES) and RSA (a public-key encryption named after the initials of its inventors) offer a more than substantial protection and are implemented in numerous computer programs. Alternatively, users may hide their communications in larger pieces of data (such as in the least significant bits of graphic files) – a process called steganography.

A new development, however, is that, more and more often, encryption is activated by default, without the end user intentionally switching it on. As data on the internet can potentially be seen by many other parties, it is quite understandable that service providers and end users employ encryption, either on parts of the links or end-to-end. As a consequence, a larger part of the regular telecommunications traffic is becoming unreadable. Keys for decryption can only be requested when the law provides for this, which will take a fair amount of time and may fail, for instance, when users have changed keys in the mean-time. Some examples of emerging encryption problems are the widely used Virtual Private Network (VPN) services that often have encryption turned on, many peer-to-peer applications which encrypt the data they exchange, and internet sites interacting with end users that use encryption protocols such as the Secure HyperText Transfer Protocol (HTTPS). The situation might worsen with the wide adoption of the new **internet protocol IPv6**. This successor to the current IP protocol in fact encompasses the IPsec encryption protocol (Feit, 1997, and Huitema, 1996). This means that all compliant devices must implement this security protocol, and chances are that much of the actual internet traffic will be encrypted, possibly also in the different streams in which it is encapsulated.

(6) Given the advent of many complementary networks, **seamless roaming and intelligent routing** is becoming more and more important. The first phenomenon is best explained by an example: a user might start a phone call in his or her office, using the company's private WiFi network. Walking out of the building, the call is taken over by a 3G cellular network. When leaving the coverage of the 3G cell, the network hands the call over to a GSM network. Finally, the call is transferred onto a public WiFi hotspot when the user walks into a train station. As such, the user can optimize the quality, the performance and the costs of the service, among other things, on the basis of his or her preferences. For a variety of reasons, it is expected that such seamless roaming will become increasingly common in the years to come. Basically, two scenarios can be envisaged. In the first, there is a central service provider that orchestrates the whole process (regardless of the fact whether it actually operates all networks in question). In principle, this operator can fulfill an intercept obligation – even though it might have to bear substantial costs to make this possible. In the second scenario, intelligence is located in the user device, and each operator involved sees only its own contribution to the total call. In this instance, the call can no longer be intercepted through a wiretap order to a single operator. Data may have to be gathered from multiple operators, but here, differences in addressing, user identities and signaling data may arise, as well as difficulties to assemble all data streams back into the original call data. In a more or less similar manner as with seamless roaming, users of fixed networks may dynamically switch between services and networks, depending on the costs, the required performance for a certain application, and so on. Such intelligent routing

facilities also facilitate load balancing. These create problems similar to those posed by seamless roaming.

(7) Currently, much efforts are devoted to the modernization of the network infrastructures. So-called **New Generation Networks (NGNs)** are designed to fully replace existing networks, including circuit-switch telephony switches, which are by now getting obsolete. Depending on their exact design, NGNs may pose less or more problems with regard to interceptability. Those designs that originate from traditional telecommunications standard-setting organizations (such as TIPHON project of the European Telecommunications Standards Institute ETSI) take interceptability as a design requirement, right from the very beginning. However, with designs originating from other organizations, for instance those generating internet standards, such a thing is not self-evident. Interception has never been a basic assumption among internet standard-developing bodies, and the later addition of intercept functionalities might lead to problems or unattractive compromises.

(8) In contrast to traditional networks, where there is a clear distinction between the centralized network infrastructure on the one hand and the user terminals on the other, **mesh networks and ad-hoc networks** have nodes that serve both as infrastructure and as access points. In other words: the user terminals may serve as a kind of relay to serve other users. This allows the construction of very cost-effective networks, especially when low-cost elements such as the Linux operating system and WiFi radio links are utilized. These networks are also highly adaptive; coverage and capacity grow as new users join. The term mesh network is used for fixed wireless types of networks, while in an ad-hoc network, terminals are mobile. In the latter case, the shape of the network is constantly changing. With regard to interception, one of the various challenges is that such networks allow users to exchange messages without data passing a central point, ultimately requiring interception functionalities in each user terminal, which is both unrealistic and insecure. While it is not yet clear whether mesh networks or ad-hoc networks will actually become a dominant means of communications, their nature makes them certainly difficult to intercept.

(9). A final complicating development concerns what can be referred to as the **identity boom**. In days gone by, all users could be simply identified by their telephony number. The structure of these directory numbers is defined on an international level by the International Telecommunication Union (ITU). Later, mobile numbers had to be added (such as the so-called GSM MSISDN numbers, which are often called 'mobile numbers' and are in fact part of the same directory number structure). With the advent of the internet, an IP number structure had to be introduced. This already introduced some complications: quite often, IP numbers are dynamically allocated to users for each specific session, and thus may differ each day, or even each hour. Unlike telephony, there is not necessarily a long-term, stable relation between an individual and the IP-number(s) that he or she uses. More recently, however, many more challenges with regard to numbers surface, including the following.

- Other identities than IP-numbers are being introduced at a great pace, and might even make the IP number arbitrary. Even today, a typical intensive user of

the internet might have dozens of different identities for different services: think of multiple e-mail aliases, MSN-identities, Skype names, a BlackBerry account, and so on. All these identities could be used from various locations (and thus various IP-numbers), including home, the office, a mobile network, a hotspot, a public terminal or a cybercafé.
- Typically, the number of IP-addresses per household is growing. IPv6 clearly caters for this growth. It is foreseen that many domestic devices will have their own IP addresses.
- Technical mechanisms such as tunneling threaten the transparency of IP-addresses. In such systems, a 'container' of data is transmitted, which includes both data and IP addresses of various sessions. There are various reasons to tunnel IP traffic, one of them being to able to transfer IPv6 traffic over IPv4 networks. These containers make it more difficult to observe the IP addresses of the underlying sessions and thus complicate interception.

To continue to be able to wiretap, it will be increasingly important for authorities to have up-to-date lists of all these different identities of users.

5.2. Market developments

Not only technology but also the telecommunications market is changing in significant ways. Not in the least these changes are fostered by the policy of liberalization and privatization that is pursued in all world regions. Below, six developments will be briefly discussed that are relevant in the context of lawful interception.

1) Overturning of the value chain;
2) Speedy adoption of all types of new services;
3) Explosion of traffic volumes;
4) Growing diversity of networks and technologies;
5) Cross-border offering of services;
6) Growing complexity of the value chain.

(1) One of the most important recent market developments in the field of telecommunications is that of the **overturning of the value chain** relating to traditional telecommunications services (see, among others, (Bekkers 2004)). The last two decades have seen many changes in the telecommunications market. To a great extent, however, the major service providers (the incumbent telephony providers) continued to build on a traditional, vertically-oriented market model in which all the providers have an extensive underlying infrastructure for transport and access. Competition creates a number of vertical compartments which provide interconnection to enable each other's customers to communicate with each other. Turnover is generated mainly by the income from circuit-switched voice telephony; a frequently heard statement holds that, in volume, the present telecommunications networks carry twice as much data traffic as voice traffic, but that turnover for voice traffic is seven times as high as that for data. So far, new entrants such as carrier select and carrier preselect telephony providers as well as (A)DSL providers, who can obtain access to the incumbent operators' networks on the basis of European legislation, have not been a great threat to the traditional business model (leaving aside one or two submarkets). Serious indicators, however, now suggest a large-

scale overturning of the business case, with the dominant vertical business model giving way to a horizontal model in which parties concentrate on a particular role in the value chain, such as access provider or service provider. Precisely because voice traffic generates much more income ‘per bit’ than data traffic, however, many traditional operators are grimly holding on to the integrated, vertical business model. Incumbents could be said to indulge – out of necessity – in a form of cross-financing. Abandoning this model will not only result in a heavy fall in income; technologies such as VoIP (see below) will also have major implications for the size of the workforce required; in many countries staff cutbacks at the (former) state enterprises are a thorny political issue.

Developments similar to those discussed above are expected with mobile services (i.e. VoIP services that use flat fee UMTS data subscriptions as a transport link), and with internet services, where less and less users actually use the email service by their access provider but use services such as Hotmail or Gmail instead.

The result of this development is that, more often than not, there will be few or no links between the access provider and the service provider. In the context of interception, this creates problems for authorities, as data from both access provider and service provider are necessary to set up a successful wiretap.

(2) In the past few years, a **speedy adoption of all types of new services** can be observed. For instance, by mid-2004, there were more than 60 million instant messaging (IM) users in Europe, while internet telephony service Skype is claimed to have almost 50 million registered users by July 2005 and to have enabled more than 10 billion minutes of talk time. Both type of services hardly existed a few years ago. Usage patterns are changing fast, and the traffic with new types of services can no longer be neglected from the point of view of interception.

(3) Also, an **explosion in traffic volume** can be observed. For private use, data lines have grown from 56 kbps landline telephony connections to DSL or cable internet offerings that usually support speeds of 0.5 or 1 Mbps. This has already boosted overall internet traffic volumes. Illustrative is traffic at the Amsterdam Internet Exchange, which handles nearly all national and national internet traffic in The Netherlands. In July 2004, this exchange switched approximately 7,100 terabytes of traffic. By July 2005, the volume has grown to more than 16,000 terabytes per month (AMS-IX, 2005). Many observers expect an energetic roll-out of ADSL 2+. With speeds of up to 24 Mbps, it allows triple-play services (television, telephone and internet) as well as new services such as video on demand and High Definition TV. Higher speeds allow content providers to offer more and larger quality content and richer websites, and thus result in larger traffic volumes. The exponential growth of traffic volumes challenges lawful interceptors, both to handle the volumes as such and to select the relevant bits of information.

(4) Next, a **growing diversity of networks and technologies** is perceivable. Increasingly, networks are able to deliver a wide range of services, and the array of access network technologies is still growing. For telephony, an urban user can often choose between many networks and protocols: the regular PSTN service, various mobile telephony services (including GSM and UMTS), telephony via ADSL (both

VoIP-based and a wide array of Voice-over-DSL protocols[55]), telephony via cable (both VOIP-based and via a number of proprietary protocols). In addition, services may be available via WiFi, Fibre-to-the-Home networks, or WiMax networks. For many other telecommunications services, similar examples may be given. To interconnect all these divergent services, a great demand for interoperability is developing (Bekkers 2005). This growing diversity challenges interceptability, as each protocol might require new intercept handover protocols to be developed. Hybrid services are more complex to intercept. Such services may combine Digital Audio Broadcast (DAB) or Terrestrial Digital Video Broadcast (DVB-T) on the downlink and GSM on the uplink (Carter and Stewart 1999), or may combine a fast satellite downlink with a dial-in uplink. Also, users may combine several independent services simultaneously, like sending larger files with the File Transfer Protocol (FTP) while using instant messaging. Such hybrid or simultaneous services are even more difficult to handle, because data from two different handover protocols have to be combined in a meaningful way.

(5) Another trend is the **cross-border offering of services**. In connection with the above-discussed overturning of the value chain and unbundling, network access and services will more often be geographically separated. That is, services are increasingly purchased or used from abroad. These service providers do not necessarily have to be locally established. Even if interceptability laws oblige these operators to provide interception facilities, enforcing such laws may be another issue. With some countries, cooperation with the respective authorities might bring relief, but with others it might not.

(6) Finally, there is a **growing complexity of the value chain**. The number of roles in the value chain is increasing, both in the traditional telecommunications domain and in the services and content domain. Roles are shifting and sometimes move to other actors. With new networks structures, such as Fibre-to-the-Home networks, structurally different roles are defined. Not only does this increase the numbers of actors that the authorities need to deal with, but it also invokes fundamental discussions as to the obligations associated with the various roles. These issues are especially challenging on the lower layers, where the role of the traditional network operator is often cut into two or more roles. All in all, the authorities have to deal with more actors and have to get involved in fundamental discussions what obligations are associated with the new roles, and how these can be operationalized, for instance, by developing appropriate handover protocols).

6. Consequences for interceptability in the future

A number of technical and market developments have been discussed in section 5. These can seriously influence the interceptability of telecommunications, thus challenging lawful interception. The challenges foreseen are summarized in Tables 1 and 2.

---

[55] For an overview, see *Voice over DSL basics* (2002), http://www.pulsewan.com/data101/vodsl_basics.htm, and *Voice over DSL Protocols* (no date), http://www.protocols.com/pbook/vodsl.htm.

Technical developments	*Challenges posed to legal interception*
(1) Voice over IP (VoIP)	Architectures and routing often do not allow service provider to fulfil interceptability obligations.
(2) Peer-to-peer applications (p2p) and (4) Home-grown networking	No service provider may be involved, while the traffic on the network layer is often difficult to decipher.
(3) The protocol explosion	It is increasingly difficult to make and keep all protocols interceptable, and it might be difficult to enforce providers operating from abroad.
(5) Encryption	Increasingly, traffic on networks is encrypted by default, while both legislation and practical problems may prevent authorities from obtaining the necessary keys. Also, calculating criminals have easy means to encrypt end-to-end effectively.
(6) Seamless roaming and intelligent routing	Increasingly, single communications use multiples domains, which makes wiretapping complex.
(7) IP-cores and New Generation Networks (NGN)	The new infrastructure architectures will place new burdens on interceptability, and depending on their origin, they might hardly be interceptable at all.
(8) Mesh networks and ad-hoc networks	The implementation of interceptability might be both unrealistic and insecure on these networks.
(9) Identity boom	It will be increasingly difficult, and perhaps impossible, to keep up-to-date lists of all the different identities of users.

Table 1: Challenges posed to legal interception by technical developments

Market developments	***Challenges posed to legal interception***
1) Overturning of the value chain	Among other things, the link between network operators and service providers is loosening, which hampers successful wiretaps.
2) Speedy adoption of all types of new services	New services are often inherently more difficult to intercept, but they may cover such a substantial part of overall traffic that they cannot be neglected.
3) Explosion of traffic volume	The exponential growth in traffic volume challenges intercepting authorities, both to handle the volumes as such and to select the relevant bits of information.
4) Growing diversity of networks and technologies	Each protocol might require new interception handover protocols to be developed, while hybrid systems even call for advanced links between interception systems.
5) Cross-border offering of services	Enforcement of interception obligations is more difficult, especially for operators based in countries or regions without interceptability laws or legal-assistance treaties.
6) Growing complexity of the value chain	Authorities need to deal with more actors and must fundamentally consider the obligations associated with the new roles, and how these can be operationalized.

Table 2: Challenges posed to legal interception by market developments

The precise scope and impact of each of these development remain difficult to assess. At the end of the day, some developments may turn out to be easily addressable within the existing frameworks and mechanisms of interceptability legislation; moreover, new technology developments may also help authorities to cope with these challenges. On the other hand, other developments will surely present serious problems, even if it cannot exactly be predicted which ones. And surely new and unforeseen challenges will arise over time to pose similar or new challenges.

With the caveat that it is difficult to predict, particularly when it regards the future, it is justified to draw at least some conclusions from the developments sketched. It is the combination of numerous technical and market developments that warrant skepticism about future interceptability. It is safe to say that, in terms of building in the technical capability and capacity to intercept, things will not get easier but will surely get more difficult. The telecom landscape is mushrooming, both in volume and in variety, and this holds for telecom providers as well as for networks, protocols, and services. If governments want to retain by and large the same ability to intercept, more efforts must be taken than were needed in the past. This means that more resources are called for: building-in interceptability will definitely be more costly in the future. But even if significantly more resources were allocated, it is not sure that the level of interceptability will remain as high as it is now, given the complexity of the challenges that lie ahead. There are serious threats to the future effectiveness and efficiency of lawful interception.

It should, moreover, be noted that addressing the challenges mentioned is not only a matter of technical ability or financial resources. Investing in order to retain the current level of interceptability will also impact other interests. For example, if interception will be effected more at the network layer than at the service layer, because there is no longer a targetable service provider or because the exact identity of the target can not be determined quickly enough, the risk of over-collection looms large, threatening the privacy of non-suspects.

Telecommunications networks may also become more vulnerable as new interceptability features are built-in, since trade-offs have to be made with network security (e.g., by turning encryption off rather than on as the default option).

Moreover, innovation can be hampered because finding interceptability solutions will take large amounts of time and work, thus delaying the introduction of innovative services.

In short, governments must seriously study the future of interceptability in view of technical and market developments in telecommunications. In doing so, they will have to determine how many resources will be needed to safeguard a minimum level of interceptability, who will have to pay for these resources, and how addressing the current and future problems in interceptability is going to impact on privacy, security, and innovation.

This means that a trade-off is called for. Exactly which new telecom networks and services will have to be made interceptable, to what degree and at what price, and who will have to pay which share of the costs, is a matter that depends on the technology at issue, the government need to make that particular network or service interceptable, and the consequences for privacy, security, and innovation.

It is here that the U.S. approach, as laid down in CALEA, is essentially more flexible and future-proof than is the Dutch approach, enshrined in Ch. 13 Telecommunications Act. CALEA already presumes some form of trade-off, through the crucial provision of 47 U.S.C. §1008(b)(1), which lists ten factors to be taken into account in determining the reasonableness of requiring a particular telecom provider to build in interceptability, flanked by several other checks and balances that ensure enhanced cost-effectiveness (see sections 4.4 and 4.3). The rigid Dutch law cannot handle such a trade-off, since it requires *tout court* that new telecommunications networks and services are made interceptable and that the providers must fund this, regardless of the costs or the effects on security, privacy, or innovation. This “we want it all” approach that aims for 100% interceptability of public telecommunications will be under increasing pressure to become more flexible, and the U.S. approach may be a good example of a way in which a balance between the competing interests can be enshrined in the law itself.

Admittedly, however, this is easier said than done. As noted in section 3, wiretapping is a much more important criminal-investigation tool in the Netherlands than it is in the U.S. Being able to retain this tool will therefore matter more to the Dutch authorities, so that they cannot be expected to simply copy the system of CALEA. Nevertheless, given the scale and scope of the technical and market developments that lie ahead, holding on to an interceptability policy as established by the current Dutch legislation does not seem to us a feasible option. With increasing complexity and diversification in technical solutions and with rising costs, not only is innovation at stake, but also competition issues will surface, given the diverging effects of CALEA and the Dutch Telecommunications Act on the investment burden of telecom providers.

7. Conclusion

There are many reasons to hold on to lawful interception. Over the past decades, this instrument has proved a useful and reliable tool in criminal investigation and in gathering intelligence. Interceptability policy and legislation is a helpful and important means to safeguard this instrument. With an adequate system of checks and balances, a good balance may be achieved between the competing public and private interests in interceptability.

However, legal systems that implement an interceptability policy solely or mainly by placing obligations upon telecom intermediaries (i.e., the network and/or service providers) are likely to lose much of their effectiveness over the next decade. Given technical progress and market developments – the latter often infused by policy measures –, ever larger parts of telecommunications traffic may disappear out of reach of lawful interception. Substantial investments will be required to address this, and even so, the level of interceptability can be expected only to decrease over the next decades.

Particularly since not only financial resources, but also immaterial interests such as privacy, security, innovation, and competition are at stake, careful thought must be given to the scope and scale of interceptability obligations. The competing interests of investigating authorities, telecom providers, consumers, and the market must be taken into account. Given the complexity and variety of the telecom landscape, the trade-off can hardly be made at the level of the legislation itself. Rather, a flexible approach that allows trading off the competing interests on a case-by-case basis is the most likely to succeed. The interceptability policy as laid down in U.S. legislation, CALEA, has such a flexible approach, with a good number of checks and balances. In contrast, the Dutch policy as enshrined in the Telecommunications Act, is more rigid and lacks serious checks and balances that can be relied on to meet the challenges of telecommunications technology and market developments that lie ahead.

References

Administrative Office of the United States Courts (2005), 2004 Wiretap Report. Washington, D.C.: U.S. Courts, April 2005 <http://www.uscourts.gov/wiretap04/contents.html>.

Adrian, J. E. (2005), 'VoIP on Tap: Whether the FCC Should Apply Wiretapping Standards to Voice over Internet Protocol', Administrative Law Review 57(Spring), pp. 647-668.

Albrecht, H.-J., C. Dorsch and C. Krüpe (2003), Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§100a, 100b StPO und anderer verdeckter Ermittlungsmassnahmen. Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht, Juni 2003, 480 p., <http://www.iuscrim.mpg.de/verlag/online/Band_115.pdf>.

AMS-IX (2005), AMS-IX Monthly Reporting: Cumulative Report 2005, <http://www.ams-ix.net/>.

Beijer, A., R. J. Bokhorst, M. Boone, et al. (2004), De Wet bijzondere opsporingsbevoegdheden - eindevaluatie. Meppel, WODC/Boom Juridische uitgevers, 305 p.

Bekkers, R. N. A. (2004), New challenges for telecommunications standardization as a result of a changing environment. Nice: ETSI General Assembly. Report commissioned by the Dutch Ministry of Economic Affairs, 29-30 November 2004.

Bekkers, R. N. A. (2005), On the increasing importance of technical interoperability and ETSI's role in it. Discussion document ETSI/GA45(05)21, offered to the ETSI General Assembly on behalf of the Dutch members of ETSI.

Bellovin, S. et al., Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, 13 June 2006, <http://www.itaa.org/news/docs/CALEAVOIPreport.pdf>.

BeVier, L. R. (1999), 'The Communications Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Break Up of AT&T', Stanford Law Review 51, pp. 1049-1125.

Büllingen, F. and A. Hillebrand (2003), Sicherstellung der Überwachbarkeit der Telekommunikation. Ein Vergleich der Regelungen in den G7-Staaten. Bad Honnef: wik, Juli 2003, 104 p.

Carter, W. and H. Stewart (1999), 'Multimedia on the move', EBU Technical Review (Autumn), pp. 8-17.

Chong, H. M. and H. S. Matthews (2004). Comparative analysis of traditional telephone and Voice-over-Internet Protocol (VoIP) systems. IEEE International Symposium on Electronics and the Environment.

Davidson, J. and J. Peters (2000), Voice over IP fundamentals. Indianapolis (IN), Cisco.

Durkin, J. F. (2003), Voice-enabling the data network: H.232, MGCP, SIP, QoS, SLA's and security. Indianapolis (IN), Cisco.

FCC (2004), Notice of Proposed Rulemaking and Declaratory Ruling, FCC 04-187, Washington, D.C., 9 August 2004, <http://www.askcalea.net/docs/20040809.fcc.04-187.pdf>.

FCC (2005), First Report and Order and Further Notice of Proposed Rulemaking, FCC 05-153, Washington, D.C., 23 September 2005, <http://www.askcalea.org/docs/20050923-fcc-05-153.pdf>.

FCC (2006), Second Report and Order and Memorandum Opinion and Order, FCC 06-56, Washington, D.C., 3 May 2006, <http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-56A1.pdf>.

Feit, S. (1997). TCP/IP: Architecture, Protocols, and Implementation with IPv6 and IP Security. Second Edition. New York: McGraw-Hill.

Huitema, C. (1996) IPv6: The New Internet Protocol. New Jersey: Prentice Hall.

Koops, B. J. (1999), The Crypto Controversy. A Key Conflict in the Information Society. The Hague etc., Kluwer Law International, 301 p.

Koops, B.-J., R. Bekkers, F. Bongers, et al. (2005), Aftapbaarheid van telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet. Tilburg: TILT, November 2005. Study commissioned by the Ministry of Economic Affairs. Available from http://www.minez.nl/content.jsp?objectid=39177.

Oram, A. (ed) (2001) Peer-to-Peer: Harnessing the Power of Disruptive Technologies. O'Reilly.

Smits, A. H. H. (2006), Strafvorderlijk onderzoek van telecommunicatie. Nijmegen, Wolf Legal Publishers, 466 p.

Statewatch (February 1997), 'European Union and FBI launch global surveillance system'.

Sutter, G. (2001). A Tale of Two Interception Regimes: RIP v CALEA, a comparison. 16th BILETA Annual Conference, Edinburgh.

Verma, D.C. (2004). Legitimate Applications of Peer-to-Peer Networks. John Wiley.

Yeates, J. (2001), 'CALEA and the RIPA: The U.S. and the U.K. Responses to Wiretapping in an Increasingly Wireless World', Albany Law Journal of Science and Technology 12, pp. 125-166.