CONTACT TRACING APPS AND PRIVACY: THE GERMAN EXAMPLE

*By: David W. Opderbeck**

I. INTRODUCTION

Contact tracing is the public health gold standard for managing outbreaks of communicable diseases.[1] Contact tracing allows researchers to trace outbreaks to their sources and implement local quarantines and other selective interventions that can significantly limit the further spread of disease.

At the outset of the COVID-19 pandemic, public health officials around the world hoped that technology would make contact tracing easier and more effective. In the developed world, and even in many parts of the developing world, most people carry phones with geolocation technology. The combination of geolocation, immediate centralized notices, and point-to-point (phone-to-phone) communication capabilities, it was thought, would exponentially amplify traditional contact tracing methods, which required individual interviews.[2]

These hopes were never quite realized. Part of the problem was the speed and scale of the pandemic—it was simply too virulent, fast, and dangerous for contact tracing to contain.[3] Another enormous problem was that contact tracing apps were not widely adopted by the public.[4] There were many reasons for this phenomenon, including differing technological platforms, ineffective

* Professor of Law, Seton Hall University Law School, and Co-Director, Gibbons Institute of Law, Science & Technology and Institute for Privacy Protection. Thanks to Professor Sam Halabi for helpful comments on an earlier draft of this article.

[1] *See, e.g.*, Ken T. D. Eames & Matt J. Keeling, *Contact Tracing and Disease Control*, 270 PROC. BIOL. SCI. 2565, 2565 (2003).

[2] *See* Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, Ludovic Barman, Sylvain Chatel, Kenneth Paterson, Srdjan Čapkun, David Basin, Jan Beutel, Dennis Jackson, Marc Roeschlin, Patrick Leu, Bart Preneel, Nigel Smart, Aysajan Abidin, Seda Gürses, Michael Veale, Cas Cremers, Michael Backes, Nils Ole Tippenhauer, Reuben Binns, Ciro Cattuto, Alain Barrat, Dario Fiore, Manuel Barbosa, Rui Oliveira & José Pereira, *Decentralized Privacy-Preserving Proximity Tracing* 2–9 (May 25, 2020), https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf [https://perma.cc/CYG9-5XFL].

[3] *See* Dyani Lewis, *Where Covid Contact-Tracing Went Wrong*, NATURE 385–86 (Dec. 17, 2020), https://media.nature.com/original/magazine-assets/d41586-020-03518-4/d41586-020-03518-4.pdf [https://perma.cc/UHN2-4KZY].

[4] *Id.*

communications, and glitchy applications, but at the top of the list were concerns about privacy.[5] Contact tracing apps feel creepy. Beyond this visceral feeling, contact tracing apps raise difficult questions about how public health concerns relate to norms and legal rules about personal privacy.

The cultural and legal concerns in the United States differ significantly from those in the European Union (EU). The United States so far has adopted a sectorial approach to privacy, in contrast to the comprehensive approach embodied in the EU's General Data Protection Regulation 2016/679 (GDPR).[6] The United States' sectorial approach reflects United States cultural and legal norms that historically have not viewed most kinds of information about a person as subject to individual dignity or property rights. In the United States, some information collected by contact tracing apps could qualify as health information protected under the Health Insurance Portability and Accountability Act (HIPAA), even if the app provider is not a HIPAA covered entity.[7] The confidentiality of other information collected by a contact tracing app might be subject only to contract law—that is, to the terms of service of an app provider—or in some cases state law. In the EU, the personally identifiable information collected by a contact tracing app is covered by the GDPR.[8]

In Europe, a consortium of researchers called the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) project began studying approaches to contact tracing applications.[9] Members of the consortium disagreed about whether an app should use a centralized contact database.[10] This disagreement spilled over into acrimony, including claims of misgovernance and deception.[11]

---

[5] *Id.* at 387.

[6] *See generally* PETER P. SWIRE & DEBRAE KENNEDY-MAYO, U.S. PRIVATE-SECTOR PRIVACY (IAPP, 3rd ed. 2018).

[7] *See generally id.*

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119); Ashley Thomas & Matthew Buchbinder, *Digital Contact Tracing in the European Union – Best Practices for United States Legislators and Regulators?*, AM. BAR ASS'N (Oct. 11, 2020), https://www.americanbar.org/groups/health_law/publications/health_lawyer_home/2020-october/dig-con/ (last visited Mar. 28, 2022).

[9] *See PEPP-PT Context and Mission* (last visited Mar. 28, 2022), https://404a7c52-a26b-421d-a6c6-96c63f2a159a.filesusr.com/ugd/159fc3_878909ad0691448695346b128c6c9302.pdf [https://perma.cc/2WVT-9WEW]; Dan Cooper, Kristof Van Quathem & Anna Oberschelp de Meneses, *COVID-19 Apps and Websites – The "Pan-European Privacy Preserving Proximity Tracing Initiative" and Guidance by Supervisory Authorities*, COVINGTON: INSIDE PRIV. (Apr. 2, 2020), https://www.insideprivacy.com/covid-19/covid-19-apps-and-websites-the-pan-european-privacy-preserving-proximity-tracing-initiative-and-guidance-by-supervisory-authorities/ [https://perma.cc/TVC8-T2WV]; Jaap-Henk Hoepman, *A Critique of the Google Apple Exposure Notification (GAEN) Framework*, CORNELL UNIV.: ARXIV (Jan. 12, 2021, 10:08 AM), https://arxiv.org/pdf/2012.05097 [https://perma.cc/9RKM-BGFN].

[10] *See Joint Statement on Contact Tracing*, KASTEL *(*Apr. 19, 2020), https://www.kastel.kit.edu/downloads/Joint%20Statement.pdf [https://perma.cc/T8XE-EZLU].

[11] *See id.*; Samuel Stolton, *EPP Cite Controversial PEPP-PT as Example for Single European COVID-19 App*, EURACTIV (Apr. 21, 2020), https://www.euractiv.com/section/digital/news/epp-cite-controversial-pepp-pt-as-example-for-single-european-covid-19-app/ [https://perma

Researchers who remained with PEPP-PT published their protocol in April 2020.[12] Other researchers, including some originally affiliated with PEPP-PT, developed protocols with a decentralized architecture.[13] Meanwhile, Google and Apple intervened by releasing application programming interfaces (APIs) that favored decentralized approaches.[14] After some debate, Germany decided to launch its "Corona Warn-App" using a decentralized architecture.[15]

This paper proceeds in three parts. Part II describes the development of Germany's Corona Warn-App, which interestingly involved a national-scale public-private partnership along with open-source contributions from individual researchers and from technology giants Apple and Google. Part III discusses some legal and policy issues raised by Germany's Corona Warn-App relating to privacy and intellectual property. A core issue about user consent to processing using the Corona Warn-App under GDPR was publicly debated but never fully resolved. A set of potential intellectual property and accountability issues relating to public-private partnerships and open-source projects have never been discussed. Part IV concludes by offering some suggestions relating to privacy, intellectual property, and accountability in future projects of this kind.

II. DEVELOPMENT OF THE GERMAN CONTACT TRACING APP

A. Germany's Decision to Adopt the Decentralized DP-3T Protocol

Germany, along with other EU countries, began to consider a national contact tracing app, with EU-wide coordination, during the first wave of the pandemic in spring 2020.[16] German authorities first considered using GPS for location information.[17] GPS is the "Global Positioning System," which is implemented through a network of space satellites.[18] This proposal was rejected because of fears that lawmakers would compel telecommunications

---

.cc/BV4R-7S4P].

[12] *See PEPP-PT*, GITHUB (June 10, 2020), https://github.com/pepp-pt/pepp-pt-documentation [https://perma.cc/47FP-Q9DY] [hereinafter PEPP-PT Repository].

[13] *See DP-3T*, GITHUB (Sept. 30, 2020), https://github.com/DP-3T/documents [https://perma.cc/2RTS-6H69] [hereinafter DP-3T Repository].

[14] *See* Casey Newton, *Why Countries Keep Bowing to Apple and Google's Contact Tracing App Requirements*, THE VERGE (May 8, 2020, 6:00 AM), https://www.theverge.com/interface/2020/5/8/21250744/apple-google-contact-tracing-england-germany-exposure-notification-india-privacy (last visited Mar. 28, 2022); Casey Newton, *How Big Tech is Dictating the Terms of the Coronavirus Response to National Governments*, THE VERGE (Apr. 28, 2020, 6:00 AM), https://www.theverge.com/interface/2020/4/28/21238633/apple-germany-contact-tracing-exposure-notification-nhs-shin-bet-australia (last visited Mar. 28, 2022).

[15] CHRISTIAN THÖNNES, CIVIL LIBERTIES UNION FOR EUROPE, COVID-19 CONTACT TRACING APPS IN THE EU: LESSONS FROM GERMANY 11 (Orsolya Reich ed., 2021), https://dq4n3btxmr8c9.cloudfront.net/files/XKDH18/COVID_19_Contact_Tracing_Apps_in_the_EU_Lessons_from_Germany.pdf [https://perma.cc/TN7E-K9EY] [hereinafter CLUE Report].

[16] *See id.* at 10.

[17] *Id.*

[18] *How GPS Works*, GPS.GOV (Aug. 24, 2020), https://www.gps.gov/multimedia/poster/ [https://perma.cc/2DK2-YMVM].

providers to supply consumer information that would allow government authorities to track citizens' movements in real time.[19]

The conversation quickly moved on to the Bluetooth Low Energy (BLE) capacities of most modern smartphones.[20] BLE utilizes a radio that transmits data over multiple channels using low power in an unlicensed radio frequency band.[21] Most current smartphones and tablets support BLE.[22]

In 2020, Google, which sponsors the Android mobile operating system, developed an "Exposure Notification" protocol that it registered with the Bluetooth Special Interest Group.[23] The Bluetooth Special Interest Group is a private organization led by engineers working in the mobile device industry that develops Bluetooth standards.[24] The Exposure Notification protocol encodes information when a BLE device is in proximity to another BLE device, including a range approximation based on the power level of the signal received.[25] This information is encrypted as set forth in a related Cryptography Specification.[26] Google and Apple further developed an API called the Google-Apple Exposure Notification (GAEN) to implement the Exposure Notification protocol in Android and iOS devices, which together comprise the vast majority of smart phones and tablets worldwide.[27]

German authorities initially proposed the more centralized PEPP-PT framework using GAEN.[28] Objections from privacy advocates, along with the GAEN APIs' restriction of BLE functionality for centralized apps, pushed

---

[19] *See generally* CLUE Report, *supra* note 15.
[20] *Id.* at 10.
[21] *Bluetooth Technology Overview*, BLUETOOTH (last visited Mar. 28, 2022), https://www.bluetooth.com/learn-about-bluetooth/tech-overview/ [https://perma.cc/H8C5-WVDZ].
[22] *See* Monika Adarsh, *Bluetooth Low Energy (BLE) Beacon Technology Made Simple: A Complete Guide to Bluetooth Beacons*, BEACONSTAC (Mar. 7, 2022), https://blog.beaconstac.com/2018/08/ble-made-simple-a-complete-guide-to-ble-bluetooth-beacons/ [https://perma.cc/YA4Y-65BE].
[23] *Exposure Notification Bluetooth® Specification*, GOOGLE 3–4 (Apr. 2020), https://covid19-static.cdn-apple.com/applications/covid19/current/static/contacttracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf?1 [https://perma.cc/4VZN-FTSJ].
[24] *See About Us: Board of Directors*, BLUETOOTH (last visited Mar. 28, 2022), https://www.bluetooth.com/about-us/board-of-directors/ [https://perma.cc/S8MA-N4M2].
[25] *Exposure Notification Bluetooth® Specification*, *supra* note 23, at 4.
[26] *See Exposure Notification Cryptography Specification*, GOOGLE 3 (Apr. 2020), https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-CryptographySpecificationv1.2.pdf?1 [https://perma.cc/LM9X-Z2EQ].
[27] *Exposure Notifications API*, GOOGLE (last visited Mar. 28, 2022), https://developers.google.com/android/exposure-notifications/exposure-notifications-api#architecture [https://perma.cc/CGG6-QMVG]. On Android and iOS global market share, *see* Jack Wallen, *Why is Android More Popular Globally, While iOS Rules the US?*, TECHREPUBLIC (May 12, 2021), https://www.techrepublic.com/article/why-is-android-more-popular-globally-while-ios-rules-the-us/ [https://perma.cc/7FMV-JMLJ]. There are some open-source alternatives to Android and iOS, but they are quirky and niche. *See* Max Eddy & Ben Moore, *Break Away from Android and iOS: 7 Free Open-Source Mobile OSes to Try*, PC MAG. (Jan. 28, 2021), https://www.pcmag.com/picks/break-away-from-android-ios-7-free-open-source-mobile-oses-to-try [https://perma.cc/FUZ9-2M43].
[28] CLUE Report, *supra* note 15, at 10.

lawmakers towards the decentralized approach.[29] Meanwhile, a working group of public health and information technology professionals, including some previously affiliated with PEPP-PT, developed a BLE-based protocol called Decentralized Privacy-Preserving Proximity Tracing (DP-3T).[30] German authorities decided on DP-3T, using the GAEN API to process identifiers, as a national framework.[31] This decision was consistent with choices made by several other European states, although others opted for a centralized approach.[32]

The German government commissioned SAP SE and Deutsche Telekom to create the Corona Warn-App (CWA) based on DP-3T and GAEN. SAP is a private company chartered in Germany that is a global market leader in business enterprise software, with over €9 billion in global annual revenue from cloud services.[33] Deutsche Telekom is also a private company with over €108 billion in global revenue, in which the German government and a German government bank hold a thirty percent stake.[34] The German public health authority, the Robert Koch Institute (RKI), also played a pivotal role.[35] Testing labs were asked to communicate positive COVID-19 test results to a CWI server controlled by RKI.[36]

---

[29] *Id.* at 11; Margherita Russo, Claudia Cardinale Ciccotti, Fabrizio De Alexandris, Antonela Gjinaj, Giovanni Romaniello, Antonio Scatorchia & Giorgio Terranova, *A Cross-Country Comparison of Contact-Tracing Apps During COVID-19*, VOX EU (Aug. 2, 2021), https://voxeu.org/article/cross-country-comparison-contact-tracing-apps [https://perma.cc/7772-U2XC]; Judith Simon & Gernot Rieder, *Trusting the Corona-Warn-App? Contemplations on Trust and Trustworthiness at the Intersection of Technology, Politics and Public Debate*, 36 EUR. J. OF COMMC'N 334, 340 (2021); Hoepman, *supra* note 9, at 14 (noting that GAEN raises problems because "Google and Apple dictate how contact tracing works.").

[30] *See* DP-3T Repository, *supra* note 13.

[31] CLUE Report, *supra* note 15, at 11–12.

[32] *See, e.g.*, Hinta Meijerink, Camilla Mauroy, Mia Karoline Johansen, Sindre Møgster Braaten, Christine Ursin Steen Lunde, Trude Margrete Arnesen, Siri Laura Feruglio, Karin Nygård & Elisabeth Henie Madslien, *The First GAEN-Based COVID-19 Contact Tracing App in Norway Identifies 80% of Close Contacts in "Real Life" Scenarios*, FRONTIERS IN DIGIT. HEALTH 2 (Nov. 2021), https://www.frontiersin.org/articles/10.3389/fdgth.2021.731098/full [https://perma.cc/7VWE-UNF2].

[33] *See Q4 and Full-Year 2021 Financial Reports*, SAP INVESTOR RELATIONS (Jan. 27, 2022), https://www.sap.com/investors/en/investment-story/recent-results.html [https://perma.cc/NKN2-PV6D].

[34] *See Company: Leading Digital Telco*, T-MOBILE (last visited Mar. 28, 2022), https://www.telekom.com/en/company/companyprofile/company-profile-625808 [https://perma.cc/C9CZUM6A]; *Fidesz Now has Another Way to Rig Elections: The Sale of T-Systems to 4IG*, HUNGARIAN SPECTRUM (July 13, 2019), https://hungarianspectrum.org/tag/deutsche-telekom/ [https://perma.cc/7VN3-TZLX].

[35] *See The Institute*, ROBERT KOCH INST. (last visited Mar. 28, 2022), https://www.rki.de/EN/Content/Institute/institute_node.html;jsessionid=3DB687301EAB92B9CC5A9695A02F1093.internet061 [https://perma.cc/D66L-NBGE]; *"The Performance of the Local Health Authorities During this Pandemic is Extremely Impressive": Crisis Response is the Motto of the 2021 Local Health Authority Day*, ROBERT KOCH INST. (Mar. 16, 2021), https://www.rki.de/EN/Content/Institute/Press_Office/PressReleases/2021/01_2021_en.html;jsessionid=BE36D6EAC917B2EF653BA2BD6702F5C1.internet111 instead [https://perma.cc/7L4G-363K].

[36] CLUE Report, *supra* note 15, at 12.

The method through which DP-3T keeps location information anonymous involves the use of simple cryptographic techniques. In its most basic implementation, an app using DP-3T pseudo-randomly generates ephemeral identification codes (EphIDs) using a daily seed (SK_t) and broadcasts them over BLE.[37] The EphIDs contain no personally identifiable information (PII) and cannot be converted into plaintext.[38] If a user tests positive for COVID-19, the app loads a "representation" of that user's daily seeds (SK_t) to a central backend database for the time period surrounding the test.[39] The app also (1) listens over BLE for EphIDs generated by other users' phones; (2) queries the central backend database to retrieve the positive seed list; and (3) applies the EphID algorithm to generate EphIDs corresponding to the positive seeds.[40] If there is a match of EphIDs within defined parameters—for example, proximity to six or more matches within a defined time period—the user receives a warning to self-quarantine.[41]

Although DP-3T does require a centralized backend database, it is not supposed to facilitate government surveillance because the database contains only lists of seeds, which are not associated in the database with any user or device.[42] This limits the utility of DP-3T for contact tracing.[43] Unlike traditional contact tracing, DP-3T does not give public health authorities access to any epidemiologically useful data.[44] Its sole utility is to notify individual users that they should self-quarantine. On the other hand, DP-3T does not entail all the privacy risks of traditional contact tracing and is not very expensive to implement, so its benefits could substantially outweigh its costs.

It is not quite accurate, however, to say that the communication between user devices and the centralized backend database involves no PII at all. Since that communication occurs over the internet, a user's internet protocol (IP) address will be disclosed.[45] Under GDPR, an IP address is a form of PII because it can be used to identify an individual, or at least to identify that a device associated with an individual communicated over a network at a specific time.

---

[37] EphIDs are generated "pseudo-randomly" because the "seeding" of the codes is accomplished through a standard function such as file hashing. *See* Troncoso, *supra* note 2, at 15.
[38] *See id*. at 13.
[39] *Id.* at 14.
[40] *See id*. at 16–17.
[41] *Protecting Lives & Liberty: How Contact Tracing Can Foil COVID-19 and Big Brother*, NCASE (last visited Mar. 28, 2022), https://ncase.me/contact-tracing/ [https://perma.cc/M7HN-LJB3].
[42] Troncoso, *supra* note 2, at 14.
[43] *See, e.g.*, Ryan Browne, *Why Coronavirus Contact-Tracing Apps Aren't Yet the 'Game-Changer' Authorities Hoped They'd Be*, CNBC (July 3, 2020), https://www.cnbc.com/2020/07/03/why-coronavirus-contact-tracing-apps-havent-been-a-game-changer.html [https://perma.cc/3AQP-B489].
[44] *See* Troncoso, *supra* note 2, at 10–11.
[45] *See* CLUE Report, *supra* note 15, at 13.

B. Luca App

By the spring of 2021, a third wave of infections was sweeping through Europe. To facilitate contact tracing, most of the German Bundesländer (states) adopted laws that required hosts of social gatherings, such as restaurants, to maintain attendance records.[46] Many of these states adopted an app developed by neXenio GmbH and marketed by culture4life GmbH, both small private companies located in Berlin.[47]

This app enables individuals to check in to a location with their phones using a QR code at a scanner operated by a venue. The user's information is stored on their phone and is transmitted along with location information to a central server maintained by culture4life (the "Luca Server"). Local health authorities can access the Luca Server to gather contact tracing data.[48] Information on the Luca Server is encrypted using public key encryption.[49]

The Luca App website contains a 2021 copyright notice which presumably claims copyright on behalf of culture4life.[50] The "Contributors" section of the Luca App Security Overview states that "This document is owned by culture4life GmbH, which is also responsible for the development of *luca*."[51] The source code is not open source and has been made available for testing only under highly restrictive license terms.[52] There have been media reports of German law enforcement authorities using legal process to obtain information from local health authorities compiled using the Luca App.[53] In January 2022, a Culture4life spokesperson said the company received law enforcement requests "almost every day" for information from the Luca Server, but that the company always resisted.[54] At the same time, most local health authorities have not regularly used the Luca App.[55]

---

[46] Jascha Galaski, *Why Was Germany's Covid Contact Tracing App Barely Used by Health Authorities?*, C.L. UNION FOR EUR. (Feb. 22, 2022), https://www.liberties.eu/en/stories/luca-app/44032 [https://perma.cc/F5B6-DXH4].

[47] *Id.*

[48] *See Actors and Components—Security Overview*, LUCA APP (last visited Mar. 28, 2022), https://luca-app.de/securityoverview/properties/actors.html [https://perma.cc/G8G4-LULB].

[49] *Secrets and Identifiers—Security Overview*, LUCA APP (last visited Mar. 28, 2022), https://luca-app.de/securityoverview/properties/secrets.html [https://perma.cc/DA3W-A3ZE]; Theresa Stadler, Wouter Lueks, Katharina Kohls & Carmela Troncoso, *Preliminary Analysis of Potential Harms in the Luca Tracing System*, CORNELL UNIV.: ARXIV 13 (Mar. 2021), https://arxiv.org/pdf/2103.11958.pdf [https://perma.cc/8V7Z-7MQL].

[50] *Luca Security Overview*, LUCA APP (last visited Mar. 28, 2022), https://luca-app.de/security overview/intro/landing.html [https://perma.cc/554Z-6PDQ].

[51] *Introduction—Security Overview*, LUCA APP (last visited Mar. 28, 2022), https://luca-app.de/securityoverview/intro/intro.html [https://perma.cc/9GTF-9FX9].

[52] *See, e.g.*, Rachel Pannett, *German Police Used a Tracing App to Scout Crime Witnesses. Some Fear That's Fuel for Covid Conspiracists*, WASH. POST (Jan. 13, 2022), https://www.washingto npost.com/world/2022/01/13/german-covid-contact-tracing-app-luca/ [https://perma.cc/6XGJ-EQ YM].

[53] *See id.*

[54] *Id.*

[55] *See id.*

III. LEGAL ISSUES RAISED BY DP-3T AND GAEN

A. Consent Under GDPR

The most significant legal issue regarding the CWA was the question of lawful basis under GDPR. The GDPR requires a lawful basis for any processing of PII.[56] Two possible bases could have applied to the Corona Warn-App: consent for "specific purposes" or that the processing was "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."[57] Some states that used the DP-3T protocol and were governed by GDPR invoked both of these bases.[58] Germany, however, chose to rely primarily on consent.[59] This may reflect Germany's choice to outsource the app development to SAP and Deutsche Telekom. Private companies can invoke the "public interest" basis, and perhaps a private company working on behalf of a public authority could also exercise the "official authority" basis, but these bases are more complicated than consent. Consent is the typical means by which a private company establishes legal basis.

Under the GDPR, for consent to be valid, it must be "freely given, specific, informed, and unambiguous."[60] This generally requires opt-in consent for every purpose for which the data is being processed.

Some civil society groups argued that Germany had not clearly specified that IP addresses would be transmitted and stored with the central repository of EphIDs associated with positive test results.[61] But the bigger issue behind the debate about consent with the Corona Warn-App was whether any consent would truly be freely given and therefore voluntary. The German government argued that consent is voluntary because no law required anyone to use the Corona Warn-App.[62] Some privacy advocates argued that societal pressure resulting from an official government app would compel some people to use the app. The European Data Privacy Board, for example, stated in 2020 that:

> [T]he mere fact that the use of contact-tracing applications takes place on a voluntary basis does not mean that the processing of

---

[56] *See* General Data Protection Regulation 2016/679, art. 6, 2016 O.J. (L 119) [hereinafter GDPR].
[57] *Id.*
[58] *See* CLUE Report, *supra* note 15, at 10–13.
[59] *See Privacy Notice*, CORONA WARN APP (last visited Mar. 28, 2022), https://www.coronawarn.app/assets/documents/cwa-privacy-notice-en.pdf [https://perma.cc/Q49Z-DJJ5].
[60] GDPR, *supra* note 56, art. 7, recital 32.
[61] *See* CLUE Report, *supra* note 15, at 13.
[62] *E.g.*, Bericht zur Datenschutz-Folgenabschätzung für die Corona-Warn-App der Bundesrepublik Deutschland Öffentliche Version [Data Protection Impact Assessment Report for the Corona Warning App the Federal Republic of Germany Public Version] 54 (Sept. 12, 2021), https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf [https://perma.cc/F2JC-EKU4] [hereinafter Official DPIA]. The German authorities have not published an official English version of this DPIA. English quotations from the official DPIA are based on a Google Translate version, on file with the Author.

> personal data will necessarily be based on consent. When public authorities provide a service based on a mandate assigned by and in line with requirements laid down by law, it appears that the most relevant legal basis for the processing is the necessity for the performance of a task in the public interest, i.e. Art. 6(1)(e) GDPR.[63]

An independent data protection impact assessment (DPIA) relating to various types of contact tracing apps, including apps using DP-3T, was conducted by the Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (Forum of Computer Scientists for Peace and Social Responsibility, FIfF), a German NGO.[64] The FIfF DPIA expressed the concern that, even though use of the Corona Warn-App was not legally mandatory, "the question of loosening lockdowns by government representatives has been explicitly or at least effectively linked to the use of the app and the widest possible use by the population . . . ."[65] The FIfF DPIA noted that "there is no realistic alternative to using the app" for individuals who desire the kind of information the app can provide.[66] Voluntariness is compromised, the FIfF DPIA argued, when "there is a clear difference in power between the controller and the data subject."[67] In particular, the FIfF suggested, "[t]his is classically the case in the relationship between citizens and public authorities," so that "[i]f consent is given to a public authority, it is generally assumed that it is not given voluntarily. . . ."[68]

This language in the FIfF DPIA derives from Recital 43 of the GDPR.[69] At one point, the FIfF DPIA suggests that Recital 43 "categorically" states that consent is not voluntary if a public authority is involved.[70] This is not the case: Recital 43 uses the words "should not" and "unlikely," which is equivocal.[71] The European Data Protection Board stated that, although consent to a public

---

[63] *Guidelines 4/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak*, EUR. DATA PROT. BD. 7 (Apr. 21, 2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en [https://perma.cc/HL3U-WV7A].

[64] Kirsten Bock, Christian Ricardo Kühne, Rainer Mühlhof, Měto R. Ost, Jörg Pohle & Rainer Rehak, *Data Protection Impact Assessment for the Corona App*, FORUM INFOMATIKERINNEN FÜR FRIEDEN UND GESELLESCHAFTLICHE VERANTWORTUNG 5 (Apr. 29, 2020), https://arxiv.org/pdf/2101.07292 [https://perma.cc/CYG7-VAU3].

[65] *Id.* at 51–52 (citing Dietmar Neuerer, *Regierung startet Vorbereitungen für Corona-App-Kampagne*, HANDELSBLATT (June 4, 2020), https://www.handelsblatt.com/technik/medizin/digitale-virus-eindaemmung-regierung-startet-vorbereitungen-fuer-corona-appkampagne/25717362.html [https://perma.cc/4ZH9-B95U]).

[66] Bock, *supra* note 64, at 52.

[67] *Id.* at 51.

[68] *Id.*

[69] GDPR, *supra* note 56, recital 43 (stating that "in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.").

[70] Bock, *supra* note 64, at 52.

[71] GDPR, *supra* note 56, recital 43.

authority is "unlikely" to be voluntary, "the use of consent as a lawful basis for data processing by public authorities is not totally excluded under the legal framework of the GDPR."[72]

German authorities produced their own DPIA (official DPIA) for the Corona Warn-App.[73] The official DPIA maintained that the Corona Warn-App is not required by law and is not the only means for individuals to demonstrate that they are vaccinated, have not tested positive, or affirmatively have tested negative.[74] The official DPIA therefore concluded that "there is currently no reason to assume that the voluntariness of the CWA users' consent is not sufficiently guaranteed."[75]

The Privacy Notice that accompanies the Corona Warn-App states that:

> Using the app is voluntary. It is entirely up to you whether you install the app, which of the app's features you use, and whether you share data with others. As a matter of principle, all of the app's main features that require the transfer of your personal data to RKI [Robert Koch Institute] or to other users will obtain your express consent in advance.[76]

The Privacy Notice further states that processing of user data for the purpose of exposure logging and individual warnings is based on consent.[77] The Privacy Notice also states that RKI relies on the public interest clause of GDPR article 6 for certain statistical information reporting based on the data processed.[78] The Privacy Notice does disclose that IP addresses and packet metadata are part of the information processed in addition to exposure data.[79] The official DPIA further describes how the app requires a user's affirmative consent before the app's risk determination features are activated.[80]

However, as the Corona Warn-App's official DPIA acknowledged, Apple and Google only allowed one "official" Corona application per country to be registered using the Exposure Notification Framework (ENF) within the GAEN API.[81] The Corona Warn-App was the only official application in Germany authorized to use the ENF in Germany.[82] Therefore, German users

---

[72] Guidelines 05/2020 on Consent Under Regulation 2016/679, Eur. Data Prot. Bd., at 8 (May 4, 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf [https://perma.cc/QA4N-6WDG].

[73] Official DPIA, *supra* note 62, at 2.

[74] *Id.* at 167.

[75] *Id.* at 169 (showing the following German quote that was translated into English using Google Translate: "Gegenwärtig gibt es im Hinblick auf die obigen Erwägungen keinen Grund zu der Annahme, dass die Freiwilligkeit der Einwilligungen der CWA-Nutzer nicht ausreichend gewährleistet ist.").

[76] *Privacy Notice*, *supra* note 59, at ¶ 2.

[77] *Id.* at ¶ 3.

[78] *Id.*

[79] *Id.* at ¶ 5a–b.

[80] Official DPIA, *supra* note 62, at 29.

[81] *Id.* at 65.

[82] *Id.*

have no other option if they wish to use this kind of approved warning app. Nevertheless, on balance, the official DPIA argued, this implementation was necessary for public health and did not unduly compromise consent.[83]

B. Other Security and Privacy Issues

In addition to whether consent was freely given, there are privacy issues arising from the Corona Warn-App's security and architecture. As discussed in Part II.A. above, the DP-3T protocol is decentralized in that it does not implement a centralized database through which users learn of local exposure risks. This local warning function happens among local devices using BLE. As further discussed in Part II.A. above, however, DP-3T does require a central server to store and distribute sets of EphIDs associated with positive COVID-19 tests.

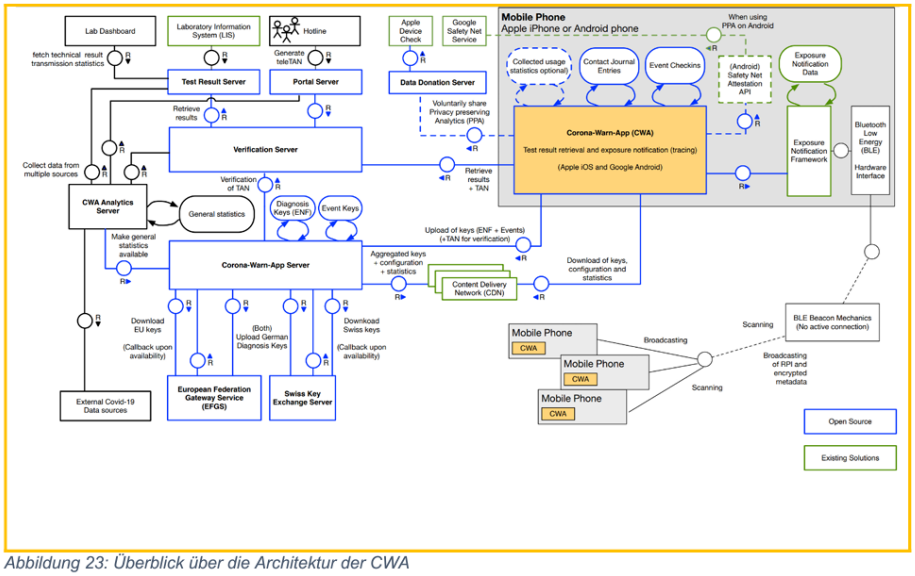

Abbildung 23: Überblick über die Architektur der CWA

Figure 1: The Corona Warn-App Architecture[84]

As shown in Figure 1, the Corona Warn-App architecture, as disclosed in the official DPIA, used seven different servers—some operated by RKI and some by other parties.[85] The servers operated by RKI include a verification server that links with testing labs through two intermediate servers and an application server that links both with the app on user devices and with European Federation and Swiss exchange services.[86] The European Exchange

[83] *See id.*
[84] Official DPIA, *supra* note 62, at 64 (showing a copy of the architecture diagram from the official DPIA).
[85] *Id.* at 64.
[86] *Id.*

Federation and Swiss exchange services facilitate information sharing with other European states that have adopted a contact tracing app.[87]

These additional layers of servers, including the outside connection to the European and Swiss exchange servers, present additional data security risks beyond the simpler model in the DP-3T Protocol.[88] The official DPIA concluded that these risks were acceptable in light of the purposes of the data processing given that the information being processed across these servers—EphIDs—cannot be connected with any specific individual.[89] The official DPIA further concluded that the consents given through the Corona Warn-App satisfied the GDPR requirements relating to these risks.[90]

C. The Ongoing Role of SAP and TSI (Deutsche Telekom)

In addition to their roles in the Corona Warn-App's development, both SAP and T-Systems International (TSI is a subsidiary of Deutsche Telekom) provide ongoing maintenance support.[91] SAP subcontracts some of its responsibilities to affiliates in Romania, Bulgaria, and Ireland.[92] TSI subcontracts some of its responsibilities to Deutsche Telekom affiliates in Germany, Hungary, and to at least one third party call center provider.[93]

The agreements between RKI, SAP, and TSI, along with any subcontracting agreements, do not appear to be a matter of public record. Although the roles of SAP and TSI are discussed at length in the official DPIA, there does not appear to be any publicly available documentation concerning intellectual property contributed by SAP, Deutsche Telekom/TSI, or concerning other terms of the relationship such as duration, warranties, indemnities, or fees. The official DPIA concluded that these relationships did not create any unacceptable privacy risks.[94] Nevertheless, although SAP and Deutsche Telekom appear to have acted altruistically, this lack of disclosure is a significant lacuna for a public health application, particularly when the underlying protocols were touted as open source.

D. The DP-3T Terms of Service

The most significant legal issue regarding the CWA was the question of lawful basis under GDPR. An additional concern, not previously discussed in the literature about these apps, relates to intellectual property. The DP-3T protocol is offered under a Creative Commons Attribution license.[95] This license allows anyone to copy, distribute, and create derivative works using the

---

[87] *See id.* at 21–22.
[88] This is noted in the official DPIA at 19.
[89] *Id.* at 64.
[90] *Id.* at 162.
[91] *Id.* at 145–46.
[92] *Id.* at 146.
[93] *Id.*
[94] *See id.* ¶ 5.9.4.
[95] *See* DP-3T Repository, *supra* note 13; *Site Policy/LICENSE.md*, GITHUB (Mar. 31, 2020), https://github.com/github/site-policy/blob/main/LICENSE.md [https://perma.cc/9N8L-YAK9].

protocol, provided that (1) attribution to the author is supplied, and (2) derivative works carry an equivalent license. The Creative Commons Attribution license (CC By 2.0) also prohibits the use of "technological measures" restricting access to the licensed content or to derivative works.[96]

Code supplied with the DP-3T protocol is offered under the Mozilla Public License (MPL) 2.0, which likewise requires attribution and attaches to derivative works to the extent the derivative work contains MPL code or modifications thereof.[97] The MPL 2.0 license further requires that MPL code remain royalty-free, and that the user not claim any further copyrights or patent rights in the code or modifications thereof. Further, the MPL 2.0 license states the code is available "as is," expressly disclaiming any warranties or any liabilities for defects in the code.[98]

Both the CC By 2.0 and MPL 2.0 are open-source "viral" licenses. This form of license is widely regarded as beneficial for projects such as DP-3T that are meant to promote the general welfare rather than function primarily as commercial products. Open-source projects can produce better code because the source code is open for inspection and improvement by the community.[99] Open-source protocols and code can also establish a technological platform "layer" that allows interconnection among disparate nodes, while remaining scalable and resisting commercial monopolization through intellectual property. Perhaps the best example of such an open technological platform layer is the internet, which from its beginnings in the 1960s to the present has operated under open-source protocols.

The main potential problem for public health policy under the CC By 2.0 and MPL 2.0 licenses is accountability. What happens if the protocol or code is defective and causes harm? For example, what if a contact tracing app fails to warn users properly under certain circumstances, facilitating an outbreak? Users who relied on the app to their detriment may not have any legal recourse.

There are several responses to this concern. First, open-source code and protocols, by definition, are open. Public health authorities and civil society can inspect the protocols and code before adoption. Second, a key benefit of open source is that a good open-source project is regularly debugged and updated by a diverse community of programmers and users.[100] Finally, if a public health authority is involved, government accountability mechanisms may exist outside the tort system, including at the ballot box or through dedicated compensation funds and the like. On balance, it is probably better for

---

[96] "Technological measures" refers to encryption or other technologies that restrict access to copyrighted works. *See, e.g.*, 17 U.S.C.A. § 1201(a)(3)(B) (Westlaw through Pub. L. No. 117-20).

[97] E-mail from Carmela Troncoso, EPFL, to author David W. Opderbeck, Seton Hall University Law School (Mar. 9, 2022, 15:55 EST) (on file with the author).

[98] *Mozilla Public License Version 2.0*, MOZILLA, ¶¶ 6–7 (Mar. 31, 2022), https://mozilla.org/en-US/MPL/2.0/ [https://perma.cc/SM2N-X8P7].

[99] *See generally* David W. Opderbeck, *The Penguin's Genome, or Coase and Open Source Biotechnology*, 18 HARV. J.L. & TECH. 167 (2004).

[100] *Id.* at 180–81.

a governing authority to utilize the expertise of an open-source community than to rely only on private industry or only on work by government employees.

The DP-3T project, however, highlights an additional concern with open-source projects that was not addressed anywhere in the DP-3T documentation. The primary intellectual property right in protocols and code—copyright—inheres in the author without any formalities such as notice or registration.[101] Contributors to an open-source project typically agree to the project's license terms, such as CC By 2.0 or MPL 2.0. This means that an open-source project is a contractual locus of multiple bits of intellectual property from hundreds or thousands of individual contributors. The CC By 2.0 license agreed to by a user of the full project is really a collection of many sub-licenses. Interestingly, the validity and enforceability of this method of aggregating viral licenses has never been conclusively tested by a court.

Under the Berne Convention, copyright protection belongs to the "author" of a work.[102] In the United States, the work for hire doctrine states that an employer is the "author" of a work created by an employee within the scope of employment.[103] Some European countries recognize a similar work for hire doctrine, while others, including Germany, do not.[104]

Contributors to the DP-3T project hailed from eleven different universities and non-profit institutes located in Switzerland, Belgium, the Netherlands, England, Germany, Italy, France, Spain, and Portugal.[105] The trademarks of these institutions are prominently displayed in the DP-3T Whitepaper.[106] It is not clear whether copyrightable contributions by these individuals initially would have belonged to them as individuals or to their institutions.

The DP-3T documentation states that "[t]he DP3T project is not funded by Google or Apple. All of the funding project's expenses have come from Prof. James Larus's discretionary funds at EPFL, in anticipation of a grant from the Botnar Foundation."[107] EPFL, the École Polytechnique Fédérale de Lausanne, is a public research university in Switzerland. It is unclear what obligations attach to "discretionary funds" provided to EPFL faculty. The Botnar Foundation is a Swiss private philanthropic foundation established by Marcela Botnar.[108] It is unclear whether Professor Larus or EPFL ever received

---

[101] *See* World Intellectual Property Organization, Berne Convention for the Protection of Literary and Artistic Works, Art. 2(1), (2) (as amended Sept. 28, 1979).
[102] *Id.* at art. 1.
[103] 17 U.S.C.A. § 101 (Westlaw through Pub. L. No. 117-120).
[104] *See* Robert A. Jacobs, *Work-for-Hire and the Moral Rights Dilemma in the European Community: A U.S. Perspective*, 16 B.C. INT'L & COMP. L. REV. 29, 50–63 (1993).
[105] *See* Troncoso, *supra* note 2, at 1.
[106] *Id.*
[107] DP-3T Repository, *supra* note 13.
[108] *See About*, FONDATION BOTNAR (last visited Mar. 28, 2022), https://www.fondationbotnar.org/about/ [https://perma.cc/98BL-X54H]; *The Botnar Legacy*, FONDATION BOTNAR (last visited Mar. 28, 2022), https://www.fondationbotnar.org/about/the-botnar-legacy/ [https://perma.cc/B37Z-G65C].

a Botnar Foundation grant, or whether any such grant reimbursed EPFL for the use of its funds.

This description of DP-3T's funding is not to suggest Professor Larus or any of the other project contributors misapplied any funds. Their intention, appropriately, appears to be disclosure of these financial interests. This information does, however, raise legal questions about whether all potential rights in the project have been fully documented and licensed. It seems unlikely, nearly to the point of inconceivable, that an intellectual property dispute would ever arise between any of these institutions and a public health authority using the DP-3T protocol in a contact tracing app. However, as a best practice, we should not leave these sorts of legal loose ends hanging. A public health authority that wants to rely on open-source protocols or code should ask for due diligence showing that any necessary rights or permissions of individual contributors and their employers have been cleared. Contributors to such a project should include these due diligence materials with the publicly available project documentation.

E. The GAEN Terms of Service

For the DP-3T protocol to be useful it must be implemented on consumer smart phones. Nearly all consumer smart phones utilize either the Apple iOS (for iPhones and other Apple devices) or the Android operating system (developed by Google).[109] Developers must utilize application programing interfaces (APIs), which are bits of code and protocols that allow applications to interact with the operating system. The GAEN API is a "[j]oint effort between Apple and Google" to create a common, open-source set of APIs for the implementation of DP-3T on Apple and Android phones.[110]

The GAEN API webpage states that the project documentation is offered under a Creative Commons Attribution 4.0 license and that code samples are offered under an Apache 2.0 license.[111] The website also notes that "Google Developer Site Policies" apply.[112] The Creative Commons Attribution 4.0 license contains essentially the same terms as the CC By 2.0 license under which the DP-3T protocols are made available.[113] The Apache 2.0 license is a free and open-source software license, which contains essentially the same terms as the MPL 2.0.[114] The Google Developer Site Terms of Service state

---

[109] *See Mobile Operating System Market Share Worldwide*, STATCOUNTER (last visited Mar. 28, 2022), https://gs.statcounter.com/os-market-share/mobile/worldwide [https://perma.cc/8S9M-XYQ4].

[110] *See Exposure Notifications API*, *supra* note 27.

[111] *Id.*

[112] *Id.*

[113] *Compare Attribution 4.0 International (CC BY 4.0)*, CREATIVE COMMONS (last visited Mar. 28, 2022), https://creativecommons.org/licenses/by/4.0/ [https://perma.cc/45CP-MTF7] *with Attribution 2.0 Generic (CC BY 2.0)*, CREATIVE COMMONS (last visited Mar. 28, 2022), https://creativecommons.org/licenses/by/2.0/ [https://perma.cc/3U2L-BVCL].

[114] *Compare Apache License, Version 2.0*, APACHE SOFTWARE FOUNDATION (last visited Mar. 28, 2022), https://www.apache.org/licenses/LICENSE-2.0 [https://perma.cc/7BQZ-BYTS] *with Mozilla Public License Version 2.0*, *supra* note 98.

that the development site materials are offered under the CC By 4.0 license.[115] The Google Developer Site Policies further state that "Google may change these terms from time to time" and that users "understand and agree that if you use the Service after the date on which these terms have changed, Google will treat your use as acceptance of the updated terms."[116] There is no other documentation indicating Apple's role in the project and nothing in the documentation offers licenses from Apple.

There is little reason to doubt that Google and Apple meant well in providing the GAEN API under free open-source licenses. Nevertheless, it is worrisome that Google retains the right to update the terms of service (TOS) at any time without notice. It is equally worrisome that all the documentation is provided by Google without any clear reference to licenses, terms, or agreements by Apple. Perhaps, in the unlikely event a dispute arose, a court would find that Apple is at least estopped from contesting the open-source license terms. But a tool used in a major public health initiative should not rest on discounting an "unlikely" event with a "perhaps," particularly when the key players are two of the GAMAM companies, with revenues greater than the GDP of many small countries.[117]

F. DP-3T Implementation Variants and Privacy Enhancements

The DP-3T Protocol includes a basic low-cost variant as described in Part II.A. above, along with two other variants and proposed enhancements to system security and user privacy. The DP-3T team suggested that authorities implementing DP-3T using the GAEN APIs adopt these enhancements. It appears that Germany adopted the basic low-cost model and never adopted any of the proposed variants or enhancements.[118]

The first variant would not disseminate a list of seeds to the centralized database, which the DP-3T team calls "unlinkable." Instead, the EphIDs of users who tested positive would be converted to hash values and stored in a "Cuckoo filter," which would be distributed to other users through the database.[119] A Cuckoo filter is a way of comparing two sets of information for matches without disclosing the specific information in the reference set.[120] The reference set is encrypted and the filter only discloses whether there are any matches without providing the information in plaintext.[121] Further, under this

---

[115] *Site Policies*, GOOGLE DEVELOPERS (last visited Mar. 28, 2022), https://developers.google.com/terms/site-policies [https://perma.cc/ZX4W-ZQK2].
[116] *Google Developers Site Terms of Service*, GOOGLE DEVELOPERS (last visited Mar. 28, 2022), https://developers.google.com/terms/site-terms [https://perma.cc/FMG5-CZ75].
[117] The "GAMAM" companies are Google, Apple, Meta, Amazon, and Microsoft.
[118] E-mail from Carmela Troncoso, EPFL, to author David W. Opderbeck, Seton Hall University Law School (Mar. 8, 2022, 03:17 EST) (on file with the author).
[119] Troncoso, *supra* note 2, at 18.
[120] Bin Fan, David G. Andersen, Michael Kaminsky & Michael D. Mitzenmacher, *Cuckoo Filter: Practically Better than Bloom*, CARNEGIE MELLON UNIV. (last visited Mar. 28, 2022), https://www.cs.cmu.edu/~dga/papers/cuckoo-conext2014.pdf [https://perma.cc/C7PB-3G7G].
[121] *Id.*

enhancement, before adding these positive EphIDs to the Cuckoo Filter, the user could have an opportunity to redact some identifiers, such as EphIDs generated during particular days of the week or particular periods of a day. This variant enhances privacy and security because the centralized database stores only encrypted Cuckoo filter files rather than individual seeds from which specific EphIDs can be reconstructed. The trade-off is that the Cuckoo filter files are larger than the sum of individual seeds, which requires more bandwidth and storage space. This trade-off could be significant when scaled to a national level.[122]

The second variant, which the DP-3T describes as a "hybrid" between the low-cost and unlinkable designs, would generate random seeds for specific time windows and would permit users to redact time windows from seed disclosure.[123] This variant would require more storage and bandwidth than the low-cost design because storing seeds in time-specific windows requires additional bytes of information delineating the time periods.[124] It would not require as much bandwidth and storage as the unlinkable version because it would not employ a Cuckoo filter.[125]

The DP-3T Whitepaper notes several ways in which a motivated, tech-savvy attacker could potentially obtain information about infection patterns and re-identify EphIDs with particular individuals.[126] As the Whitepaper notes, these risks are inherent to any proximity-based notification system.[127] For the basic low-cost variant, the Whitepaper recommends that the app run within a privileged OS-level module, which is the approach taken in the GAEN API, or inside a local trusted execution environment (TEE).[128] A TEE uses more system resources and is more difficult to implement than only a privileged OS-level module. The use of a TEE was not part of the GAEN API.[129]

The Whitepaper also noted that an attacker could gather large numbers of EphIDs by using specialized BLE collection equipment, either in a static location or while "wardriving."[130] To mitigate this concern, the Whitepaper

---

[122] Troncoso, *supra* note 2, at 18–20.
[123] *Id.* at 20.
[124] *Id.*
[125] *Id.*
[126] *Id.* at 30–31.
[127] *Id.* at 30.
[128] *Id.* at 32–33. A "privileged OS-level module" refers to the levels of privilege in the different layers of a computing system. *See, e.g.*, *Privilege and Exception Levels*, ARM DEV. (last visited Mar. 28, 2022), https://developer.arm.com/documentation/102412/0102/Privilege-and-Exception-levels [https://perma.cc/HT5W-CQAM]. Moving down the stack requires higher levels of privilege. Locating the contact tracing app in an OS-level module rather than at the less privileged application-level means that a higher degree of authentication is required to execute the application. A TEE is separated from other applications so that an intrusion or infection that affects general applications will not affect an application within the TEE. *See, e.g.,* Don Felton, *What is a Trusted Execution Environment (TEE)?*, TRUSTONIC (last visited Mar. 28, 2022), https://www.trustonic.com/technical-articles/what-is-a-trusted-execution-environment-tee/ [https://perma.cc/4JTA-F57F].
[129] Troncoso, *supra* note 2, at 32–33.
[130] *Id.* at 38–39. "Wardriving" involves equipping a vehicle with electronic eavesdropping

suggests using a "k-out-of-n secret sharing scheme."[131] In this technique, the message is broken into parts that are shared in a specified number of packets over time. The message can only be reconstructed if all the packets are received and reconstructed according to the sharing algorithm. A wardriving attacker is not likely to receive all the packets and, therefore, would not be able to reconstruct the message.[132] Of course, this technique would not help if it were easy to infer the missing pieces, like a contestant on Wheel of Fortune guessing a phrase when some letters have not yet been revealed on the board. An EphID seed presumably is complex enough that the whole could not be inferred from numerous smaller parts. The problem with this technique is that it requires more usage of the BLE antennas and more computation time, which can deplete phone battery life.[133] The DP-3T team suggested that its proposed enhancement would offer an acceptable tradeoff between increased security and battery life, but it was not adopted in the GAEN API.[134]

IV. CONCLUSION AND RECOMMENDATIONS

In a report on the German Corona Warn-App, the Civil Liberties Union for Europe (CLUE) offered several helpful observations and recommendations. The CLUE report noted that privacy principles should not be suspended during a public emergency such as a pandemic, public authorities should ensure transparency and accountability for interventions such as contact monitoring or tracing, decentralized open-source solutions should be preferred, and voluntariness should be ensured including relating to penalties and incentives for use of the technological intervention.[135]

These are all good recommendations, to which we should add some additional best practices and qualifiers. First, the CLUE report mentions voluntariness only briefly. This was the most contested issue regarding privacy and the Corona Warn-App. Aside from the specific interpretation of GDPR Recital 43, there is an intractable ideological debate about whether any government-sanctioned public health application that collects PII can ever be "voluntary." The concerns of privacy advocates about voluntariness, particularly in the context of a public health emergency, are important. From time immemorial, "emergencies" have been the pretext for stripping away civil liberties. The German historical experience of the Reichstag Fire Decree in 1933 is of course a searing example.[136]

However, it is unrealistic to argue that a public emergency should never suspend or limit any privacy protections of any kind. Perhaps we can make an

---

equipment and driving around target areas to collect signals. *Id.*

[131] *Id.*

[132] *See id.*

[133] *Id.*

[134] *See id.*

[135] CLUE Report, *supra* note 15, at 6–8.

[136] *See Reichstag Fire Decree*, U.S. HOLOCAUST MEM'L MUSEUM (last visited Mar. 28, 2022), https://www.ushmm.org/learn/timeline-of-events/1933-1938/reichstag-fire-decree [https://perma.cc/MRN7-C2LW].

analogy here to limits on privacy that are necessary and appropriate to investigate crimes. Every Western democracy provides for search warrants or other official process for governmental searches and seizures.[137] We can, of course, debate how this balance between privacy and security works out in specific situations, but it is always a balance.

Privacy regulators should therefore develop specific guidelines regarding the voluntariness of consent under GDPR in times of public emergency. Emergency powers statutes typically allow for the graded suspension of some civil liberties upon the official declaration of a state of emergency for limited times, with a requirement of further affirmative approvals by a legislative or judicial authority and other judicial oversight.[138] GDPR Recital 43 could be developed to establish that a public health authority could authorize and encourage the use of an application for limited times under emergency circumstances, with specific requirements for data deletion after the emergency subsides, and specific provisions for judicial review of specific circumstances that might undermine an individual's human rights. A rule or interpretation along these lines could also include parameters such as a preference for decentralized app architecture. At the very least, discussion of this question beyond an absolute yes or no seems necessary.

Second, open-source solutions should indeed be preferred over proprietary code. In the German example, this is illustrated by the different scrutiny both PEPP-PT and DP-3T protocols received, compared to the problems created by the Luca App. The open-source repository, however, should always include a thorough history of rights conferred. As the analysis in this paper shows, open-source projects also involve multiple layers of intellectual property and contract rights. "Open-source" does not mean "free of intellectual property." Rather, open-source is a means of bundling clusters of intellectual property and contractual rights into viral license terms. If an open-source project looks to provide scalable public health solutions, the documentation should include clear assignments or licenses to all links in the chain of rights. This includes, critically, assignments or licenses from the institutions and funding sources with which contributors are affiliated.

Third, the role of technology companies at the OS layer of the project should be more carefully scrutinized and documented. The practical reality for the foreseeable future is that Google and Apple will remain necessary partners in any application using mobile technology. If an application uses desktop technology, Microsoft (Windows) will become a necessary partner as well. There is no getting around the need for APIs to implement a project like the Corona Warn-App on proprietary or semi-proprietary operating systems. Google and Apple acted commendably in releasing open-source APIs for contact tracing apps. The full chain of rights, however, should be established in the documentation. As this paper shows, there are potentially significant gaps

---

[137] *See, e.g.*, U.S. CONST. amend. IV; EUR. CONSULT. Ass., *European Convention for the Protection of Human Rights and Fundamental Freedoms*, art. 8 (Nov. 4, 1950).
[138] *See, e.g.*, 50 U.S.C.A. § 1621 *et seq.* (Westlaw through Pub. L. No. 117-120).

in the GAEN documentation, particularly concerning Apple's role.[139] The rights should also be provided apart from terms of service that allow any private entity to change the terms unilaterally, as is currently the case with Google's developer TOS.

Further, regarding the role of technology companies, the distribution of official public health apps through the Google or Apple app stores should be reconsidered. The final nail in the coffin for PEPP-PT might have been Google's decision to authorize only one GAEN app per country and to tie the GAEN APIs so closely to decentralized approaches that other methods became infeasible. A privacy scholar might agree that decentralized approaches such as DP-3T are preferable from a privacy perspective, but this kind of risk-benefit analysis concerning public health should not fall to a private for-profit company. Governments should work closely with Google and Apple to ensure that these choices are made democratically and not by the companies, even if some regulatory pressure is required to cement this fundamentally important principle.

Fourth, there should be a more active public framework for implementing privacy and security enhancements developed by technologists. The enhancements suggested by the DP-3T team were never implemented into the GAEN APIs. Perhaps, in the end, this choice reflected the best balance of functionality and efficiency, but it appears to have been mostly a default option. Public health authorities should include a robust review process to ensure that privacy and security enhancements are carefully considered as they are developed.

Fifth, the public-private model reflected in the Corona Warn-App also requires more careful thought. Companies like SAP and Deutsche Telekom also acted commendably by providing expertise and resources for development and maintenance that only the private sector can deploy at such scale and speed. But, again, there was no readily publicly accessible documentation of their intellectual property rights and other potential interests. All of this should be made clear in the central open-source repository. This practice imposes a discipline on the parties to specify their intentions and provides accountability to the public.

Finally, related to the fifth observation, there should be more discussion of legal accountability in cases where applications contain flaws that cause serious harms. Most open-source licenses such as the MPL provide code on an "as-is" basis with a disclaimer of any representations or warranties. To the extent these provisions are enforceable, they leave the public exposed to a product without adequate insurance against personal or even systemic harms. We do not accept this kind of liability shifting in other areas of public health where private actors are significant players. Doctors, hospitals, pharmacies, and medical device and pharmaceutical suppliers all face some risk of liability,

---

[139] Some researchers have suggested that the GAEN framework itself introduces privacy vulnerabilities precisely because some information remains within the control of Google and Apple. *See* Hoepman, *supra* note 9, at 1–2.

which is then spread through insurance, at least in countries with a robust tort system. Vaccine manufactures, for example—including for the COVID-19 vaccines—must pass regulatory approvals and risk liability for certain harms. In countries with a less robust tort system than the United States, these entities at least are accountable to licensing and credentialing bodies, while public insurance may play a bigger role in compensating for harms.

This question of initial oversight and accountability for defects is potentially the most significant conflict between open-source norms and public health policy next to the question of voluntary consent. It will likely become an even more substantial question as artificial intelligence and other computing technologies offer scalable interventions for public health crises, both as traditional software applications and as code embedded in devices and therapies.[140] This is not to suggest that open-source is a bad model for code relating to public health or that public-private partnerships with firms such as SAP, Deutsche Telekom, Google, or Apple should be avoided. From a privacy perspective as well as a technology development perspective, this kind of model is greatly promising. It does, however, mean that public health authorities should think carefully about how to approve, monitor, and insure such projects in the future.

[140] On the issue of artificial intelligence in medical devices, *see generally* David W. Opderbeck, *Artificial Intelligence in Pharmaceuticals, Biologics, and Medical Devices: Present and Future Regulatory Models*, 88 FORDHAM L. REV. 553 (2019).