Contact Tracing Applications Under the European Regime

Raif Baran Tombul,
PhD Student at Universitat Autonoma de Barcelona
Barcelona, Spain
rbtombul@gmail.com

Abstract- Covid-19 pandemic obliged scholars to scrutinize new privacy concerns due to the use of digital contact tracing applications. Considering that we are living in the digital age, the type of privacy safeguards that data controllers need to take should be thoroughly investigated. Although the main goal of these applications is to tackle the spread of the pandemic in society, the privacy rights of users must also be preserved. Otherwise, serious privacy risks might appear when the pandemic is eventually over. This paper aims to contribute to this discussion by addressing the potential questions related to the privacy risks of contact tracing applications from technical and organizational measures perspectives and thus to provide a contribution to the use of privacy-preserving contact tracing applications within the European Economic Area (EEA).

Keywords- Privacy; General Data Protection Regulation; Law; Pandemic; Contact Tracing.

I. INTRODUCTION

There are many samples in the history of medicine, ranging from AIDS to Ebola, where tracing methods were conducted to determine symptomatic people and, where required, employ isolation strategies [1]. Traditional contact tracing, where a public health official interviews an infected person to determine the places and people they met, is still in place [2]. Contact tracing, identifying individuals that have been in contact with an infected person, is a key component in tackling the spread of infectious illnesses [3]. The tasks conducted by contact tracing applications could be accumulated into 3 groups: detection of contact events (proximity tests), transmission, and exposure notification [4]. Accordingly, contact tracing applications have played an important role in controlling the spread of Covid in society. However, there are some privacy concerns among users about the use of these applications, which will be reviewed in this paper. Accordingly, the European Data Protection Board (EDPB) published a guideline about contact tracing applications [5]. Additionally, the European Commission published a communication about contact tracing applications [6] to establish certain points to consider for data controllers during their use of these applications in addition to the General Data Protection Regulation (GDPR)[7]. This idea paper briefly addresses the privacy concerns stemming from the use of contact tracing applications within the EEA and mentions the importance of privacy safeguards that could play an important role in mitigating these concerns. Accordingly, in Section 2, concerns and risks about contact tracing applications will be addressed. Subsequently, in Section 3 privacy implications of the applications' architectural choice applications will be briefly analyzed. Finally, in Section 4, technical and organizational measures will be elaborated, and potential solutions will be evaluated.

II. CONCERNS AND RISKS ABOUT CONTACT TRACING APPLICATIONS

The increased use of the Internet, together with rapid advances in technology, has changed the way in which information about users is gathered, stored, and exchanged was detailed [8]. Having said that, in order to fight with pandemic efficiently, individuals should trust the privacy features of the applications, thereby downloading these applications to their mobile phones. However, mobile applications possess, as seen, both certain advantages and ambiguous aspects [9]. Applications for contact tracing can be broadly divided into two categories [10]. In the centralized system, public institutions gather data on a single server, where data matching takes place [11]. The unique codes generated by a contact event are stored on each person's device in the decentralized approach instead of being sent to a centralized server [12]. While the centralized approach assumes that individual user data which could be leaked through the application is the most notable risk, the decentralized approach assumes that the compromising of all the user data in one location is the largest risk [13]. Therefore, it is plausible to say that each method is subject to a certain amount of risks. Generally, there are two types of privacy risks to an individual when we consider exposure notification applications, these are namely identity privacy, in which situation user individuals would not desire their identity to be shared without their affirmation) and location privacy, which response to the case where the individual would not desire other people may be able to link the various locations they visited to discover location history, without their consent) [14]. Hence, citizens who live in the community and download contact tracing applications to their mobile phones due to the Covid pandemic are concerned about being tracked by data controllers that process this personal data processed via the Global Positioning System (GPS). Tracking patients with Covid-19 and activities of contact persons could cause a breach of their privacy [15]. Furthermore, processing location data has further consequences because it would enable businesses to collect the data to learn about the movements of individuals and draw conclusions about preferences and habits [16]. Although contact tracing systems do not explicitly collect or record the true identities of individual users, movement profiles based on pseudonymous tracing data make it possible to identify a large fraction of users with a high probability [17].

In summary, although there are plenty of advantages generated by contact tracing applications, there are also a few vulnerabilities in terms of privacy aspects thereof. In the

 ISBN: 978-1-68558-056-8

following sections, this paper addresses these concerns by mentioning the safeguards that could be used.

III. ARCHITECTURE OF THE APPLICATIONS AND PRIVACY IMPLICATIONS THEREOF

Processing activities with centralized or decentralized protocols do have several implications for data controllers and data subjects. There is a need to understand the logic of decentralized and centralized processing. To track infected people and alert those who have come into touch with them, the centralized approach entrusts a central server with user information [18]. In contrast, the decentralized strategy relies on users' phones to keep user data and alert them, in case they are exposed to an infectious person[19]. Either choice of architecture brings advantages as well as disadvantages in terms of privacy, as already discussed in the relevant literature. However, more privacy-preserving technologies are required to mitigate the aforementioned risks rather than centralized or decentralized protocol discussion. For instance, many experts favored Bluetooth technology to prevent any sort of location-tracking-related risk. Similarly, the EPDB is in favor of the idea that the priority should be to process it without collecting localization data via Bluetooth [20]. These secure means of tracking are in line with the privacy-preserving perspective.

IV. TECHNICAL AND ORGANISATIONAL MEASURES

The EDPB recommended the adoption of both centralized and decentralized systems, provided that adequate security measures are implemented [21]. This perspective brought by the EDPB is quite useful for grasping the significance of adequate security measures implemented by data controllers. Also, as mentioned by the Commission, in general, the degree of security should match the amount and sensitivity of personal data processed [22]. Therefore, in order to control privacy and data protection risks and manage ethical concerns, this necessitates taking into consideration and combining the most efficient legal, organizational, and technical safeguards, including cutting-edge statistical and computational measures [23]. Accordingly, as per the EDPB Guidance, modern cryptographic techniques must be used to protect the data that is stored on servers and in applications, communications between the remote server and the apps [24]. EDPB also mentions the requirement of mutual authentication between servers and applications required [25]. These measures are feasible, as they have already been used for different types of digital applications by data controllers for years. However, considering the evolving nature of privacy threats, in addition to technical and organizational measures set out under article 32-1 of the GDPR and proposed by the EDPB, some tailor-made options could solidify the quality of these measures. For instance, blockchain technology, which is an open and shared database, over which no single party has control, and transactions, which include messages exchanged when two devices come into close contact, are safely recorded in blocks [26], could be useful for digital contact tracing, as proposed by Klaine and colleagues. As they mentioned, due to the fact that blockchain does not rely on a central server, this can enable global access to information while simultaneously being more resistant to harmful attacks [27]. Hence, considering that blockchain is now being used in keeping health records of patients in preserving their overall medical history without any involvement of service providers [28], it is also possible to generate a privacy-preserving, and feasible solution by implementing blockchain measures for the European contact tracing applications.

More of a generic solution to mitigate other unexpected privacy-related threats not listed in section II, hiring subject matter experts specifically devoted to implementing technical and organizational measures and designating contractual safeguards with third-party suppliers or vendors within the scope of cyber security activities could enhance the security capabilities of data controllers. In particular, considering safeguards for third-party vendors involved in any process of contact tracing applications are of massive importance to provide oversight on activities of data processors in line with article 28 of the GDPR. To this end, due to it is prevalent use and cost-efficient nature in many other fields, standard contractual clauses between controller and processor introduced by the EU Commission [29] could be an efficient safeguard for stipulating the required tailor-made safeguards that processors must implement. By this, it would be possible to generate a feasible solution for the implementation of required technical and organizational measures by third-party data processors as well, in order to mitigate any potential risk related to the involvement of third parties.

Last but not least, detailed and recurring data protection impact assessments could be an efficient way to determine privacy-related risks, regardless of the architectural design of the applications. Privacy risks associated with data regarding identifiable individuals can be mitigated in great part by using de-identification techniques in conjunction with reidentification procedures [30]. In order to have more privacy-friendly applications for any future case scenarios, all these safeguards should keep being implemented from a privacy-by-design perspective. The principle of Privacy by Design supports the idea that privacy should be deemed as a first-class citizen in the technology design and ought to be intensely inserted, as described by Besik and Freytag [31].

As a positive sign of compliance with these requirements, almost each of the data controllers in the EEA pays attention to these aforementioned risks and technical and organizational safeguards, based on their privacy policies. For instance, as a few samples of many successful ones, the Estonian application [32] properly indicates the third-party companies involved in the process, while at the same time and the Lithuanian application [33], displays the details of permissions and features the application requires. Likewise, the Italian application shared on the documentation website many important aspects related to the security of the application, such as privacy-preserving analytics, security document, and design information with the users [34].

Therefore, it is plausible to state that designing contact tracing applications with security and privacy considerations based on the potential vulnerabilities described in section II is important to diminishing any potential risks posed to data subjects.

 ISBN: 978-1-68558-056-8

V. CONCLUSIONS

Implementation of efficient technical and organizational safeguards, as well as a privacy-by-design approach, are of key importance to the success of contact tracing applications. Therefore, if efficient safeguards are put in place by data controllers of contact tracing applications, the type of architecture of applications will not have a massive impact on the level of privacy protection by merely itself, as the main goal of these applications is to block the spread of the virus throughout society, rather than tracking people movement or processing an excessive amount of their personal data. Accordingly, as a positive sign of this perspective, almost each of the data controllers within the EEA acts responsibly to comply with the GDPR requirements and other relevant guidance. For the path forward, in case such tracking applications are required again, it is diligent to implement such necessary safeguards elaborated in section IV of this paper, in addition to the existing safeguards that are already put in place by data controllers, to maintain privacy-preserving technology.

ACKNOWLEDGEMENT

Raif Baran Tombul thanks Prof. Antoni Roig Batalla for his constant support during the research.

REFERENCES

[1] T. Scantamburlo, A. Cortés, P. Dewitte, et al. “Covid-19 and tracing methodologies: A lesson for the future society”, Health Technol., Vol. 11, pp. 1051–1061, p.1052, 2021

[2] Dig Watch Website https://dig.watch/trends/contact-tracing-apps retrieved: January 2023)

[3] A. Anglemyer, et al. “Digital contact tracing technologies in epidemics: a rapid review” Cochrane Database Syst Rev., Aug 18;8(8): CD013699, p.4, 2020, doi: 10.1002/14651858.CD013699. PMID: 33502000; PMCID: PMC8241885.

[4] J. C. Nobre, L. R. Soares, B. O. R. Huaytalla, E. D. S. Júnior, and L. Z. Granville ‘On the Privacy of National Contact Tracing COVID-19 Applications: The Coronav\'irus-SUS Case’ arXiv preprint arXiv:2108.00921. p.1. 2021

[5] The European Data Protection Board, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020

[6] Communication from the Commission Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection 2020/C 124 I/01 available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417(0) (retrieved: January 2023)

[7] 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)

[8] C. Paine, U.D. Reips., S. Stieger, A. Joinson, and T. Buchanan, “Internet users’ perceptions of ‘privacy concerns’ and ‘privacy actions” International Journal of Human-Computer Studies 65, no. 6, pp. 526-536, 2007

[9] Amnesty Web Site: https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/ (retrieved: January 2023)

[10] Friedrich Naumann Foundation Website, https://www.freiheit.org/turkey/safety-and-privacy-time-covid-19-contract-tracing-applications (retrieved: January 2023)

[11] Friedrich Naumann Foundation Website, https://www.freiheit.org/turkey/safety-and-privacy-time-covid-19-contract-tracing-applications (retrieved: January 2023)

[12] M. Shahroz, F. Ahmad, M.S. Younis., N. Ahmad, M.N.K. M. Boulos, R. Vinuesa, and J. Qadir “COVID-19 digital contact tracing applications and techniques: A review post initial deployments”. Transportation Engineering, 5, p.100072, 2021

[13] Duke TechPolicy Sanford Article 21 February 2021 comparing centralized and decentralized contact-tracing approaches https://sites.sanford.duke.edu/techpolicy/2021/02/21/centralizedvsdecentralized/ (retrieved: January 2023)

[14] E. Mbunge “Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls.” Diabetes Metab Syndr., Nov-Dec;14(6), pp. 1631-1636, 2020, doi: 10.1016/j.dsx.2020.08.029. Epub 2020 Aug 26. PMID: 32892060; PMCID: PMC7833487

[15] R.A. Kleinman and C. Merkel “Digital contact tracing for COVID-19.” CMAJ. 2020 Jun 15;192(24), pp.E653-E656, p.E654, doi: 10.1503/cmaj.200922. Epub 2020 May 27. PMID: 32461324; PMCID: PMC7828844.

[16] R. Raskar, et al." Comparing manual contact tracing and digital contact advice." arXiv preprint arXiv:2008.07325, p.6, 2020

[17] L. Baumgärtner, A. Dmitrienko, B. Freisleben, A. Gruler, J. Höchst, J. Kühlberg and Mira Mezini et al. "Mind the gap: Security & privacy risks of contact tracing apps." In 2020 IEEE 19th international conference on trust, security, and privacy in computing and communications (TrustCom), pp. 458-467, p.461, 2020

[18] Duke TechPolicy Sanford Article 21 February 2021 comparing centralized and decentralized contact-tracing approaches https://sites.sanford.duke.edu/techpolicy/2021/02/21/centralizedvsdecentralized/ (retrieved: January 2023)

[19] Duke TechPolicy Sanford Article 21 February 2021 comparing centralized and decentralized contact-tracing approaches https://sites.sanford.duke.edu/techpolicy/2021/02/21/centralizedvsdecentralized/ (retrieved: January 2023)

[20] P. Chakraborty, M. Subhamoy, N. Mridul, and T. Suprita “Contact Tracing in Post-Covid World: A Cryptologic Approach.” Singapore: Springer, p.31, 2020

[21] European Data Protection Board, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020, p.9

[22] Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01 available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417(08) (retrieved: January 2023)

[23] European Data Protection Board, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020, p.9

[24] European Data Protection Board, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020, p.9

[25] U. Gasser, M. Ienca, J. Scheibner, J. Sleigh and E. Vayena “Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid.” Lancet Digit Health, 2020 Aug;2(8), pp. e425-e434, p.431, doi: 10.1016/S2589-7500(20)30137-0. Epub 2020 Jun 29. PMID: 32835200; PMCID: PMC7324107.

[26] V.P. Klaine, L. Zhang, B. Zhou, Y. Sun, H. Xu, and M. Imran, Privacy-preserving contact tracing and public risk assessment using blockchain for COVID-19 pandemic. IEEE Internet of Things Magazine, 3(3), pp. 58-63, p.58, 2020

[27] V.P. Klaine, L. Zhang, B. Zhou, Y. Sun, H. Xu, and M. Imran, Privacy-preserving contact tracing and public risk assessment using blockchain for COVID-19 pandemic. IEEE Internet of Things Magazine, 3(3), pp. 58-63, p.58, 2020

[28] B. Aslam, A. R. Javed, C. Chakraborty, J. Nebhen., S. Raqib. and M. Rizwan, Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic. Personal and ubiquitous computing, pp.1-17, 2021

[29] EU Commission Website, Standard Contractual Clauses https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_en (retrieved: January 2023)

[30] A. Cavoukian and J. Jonas “Privacy by design in the age of big data” Information and Privacy Commissioner of Ontario, Canada, p.8, 2012

[31] S. I. Besik and J. C. Freytag. "Managing Consent in Workflows under GDPR." In ZEUS, pp. 18-25, p.18, 2020

[32] HOIA Phone Application Privacy Policy https://koodivaramu.eesti.ee/tehik/hoia/app-web/-/blob/master/content/privacy.en.md (retrieved: September 2022)

[33] Korona Stop, Privacy Policy https://koronastop.lrv.lt/uploads/documents/files/corona-stop-app/Privatumo-politika-korona-stop-en.pdf (retrieved: September 2022)

[34] Immuni Application Documentation https://github.com/immuni-app/immuni-documentation#privacy (retrieved: September 2022)

 ISBN: 978-1-68558-056-8