

CONTACT TRACING APPLICATIONS UNDER THE EUROPEAN REGIME

Raif Baran Tombul

PhD Student at Universitat Autònoma de Barcelona

Barcelona, Spain

rbtombul@gmail.com

UAB

Universitat Autònoma
de Barcelona



R. B A R A N T O M B U L

- R. Baran Tombul received his master's degree in European Master in Law and Economics from Hamburg University and Aix-Marseille University in 2016. He is currently a doctoral student majoring in Law and Technology, at the Faculty of Law of Universitat Autònoma de Barcelona. His research interest lies in data protection law and contact tracing applications.

AIMS TO CONTRIBUTE

- 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).

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]. 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.

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 [4];



CONCERNS AND RISKS ABOUT CONTACT TRACING APPLICATIONS

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].

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].

TECHNICAL AND ORGANISATIONAL MEASURES

The EDPB Guideline sets out;

- The adoption of both centralized and decentralized systems, provided that adequate security measures are implemented [21].
- 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].
- Additionally, the EDPB guideline elaborated other valuable suggestions for adequate security measures implemented by data controllers.

TECHNICAL AND ORGANISATIONAL MEASURES

In addition to the EDPB guideline;

- 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.
- 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].

CONCLUSION

Efficient safeguards and privacy-by-design are vital for contact tracing applications' success. App architecture isn't the main factor in privacy protection, as the goal is virus control, not extensive data processing or tracking. Most EEA data controllers comply with GDPR and related guidelines.

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\(0\)](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

REFERENCES

- [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\(08\)](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

REFERENCES

- [25] U. Gasser, M. Ienca, J. Scheibner, J. Sleight 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/tehhik/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)



THANK YOU
