AN EPUBLICATION OF THE LOS ANGELES COUNTY BAR ASSOCIATION

LACBA

PRIVACY AND CYBERSECURITY SECTION

Section Home Page
click here ›

JUNE 2020

Back to June 2020 issue

Information Privacy and the Pandemic Response: Risks and Solutions for Contact Tracing Apps

DAVID NAVETTA, KRISTOPHER KLEINER and ANDREW EPSTEIN, Cooley LLP

Governments[1], non-governmental organizations[2] and private parties[3] around the world are rushing to leverage technology to enable broad-based contact tracing[4] to help better understand the spread of COVID-19; however, will doing so come at the expense of information privacy? Contract tracing implicates a host of privacy and security concerns based on the sensitivity of the data at issue (location data[5] and health information) and the parties with whom such data may be shared (*e.g.*, governments, insurers and employers). Balancing privacy against public health concerns is even more challenging because organizations feel the need to work at break-neck speeds in an effort to combat the COVID-19 pandemic[6]. Nonetheless, in order to increase confidence in, and the wide adoption of these technologies, it is critical for organizations to incorporate privacy-by-design[7] principles and robust vulnerability testing and assessments[8] into the development process.

---

[1] Katie Collins, *Europe's contact-tracing apps are a test of its privacy-focused culture*, available at https://www.cnet.com/news/europes-contact-tracing-apps-are-a-test-of-its-privacy-focused-culture/ (last visited May 5, 2020).
[2] About CoEpi, available at https://www.coepi.org/about/ (last visited May 5, 2020).
[3] Apple, *Apple and Google partner on COVID-19 contact tracing technology*, available at https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/ (last visited May 5, 2020).
[4] World Health Organization, *Contact Tracing Q&A*, available at https://www.who.int/news-room/q-a-detail/contact-tracing (last visited May 5, 2020).
[5] United Kingdom Information Commissioner's Office, *Location data*, available at https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/location-data/ (last visited May 5, 2020).
[6] World Health Organization, *Rolling updates on coronavirus disease (COVID-19)*, available at https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen (last visited May 5, 2020).
[7] Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, available at https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf (last visited May 5, 2020).
[8] *OWASP Mobile Security Testing Guide*, available at https://owasp.org/www-project-mobile-security-testing-guide/ (last visited May 5, 2020).

Privacy-by-design involves embedding, *by default*, privacy protective processes and technology into contact tracing IT solutions. For example, organizations should consider building decentralized collection and storage of relevant data (an approach supported by over 500 academics[9] globally) into a contract tracing apps. Under this approach, the app stores data only on the end user's device rather than on a central server. Privacy is enhanced because no single entity stores or has access to the tracing data and thus it is less vulnerable to a breach or to misuse by relevant stakeholders. By contrast, the South Korean government[10] is reportedly implementing contract tracing by tracking individuals' phones, augmenting this data with credit card records and face-to-face interviews, and then building maps, which are publicly accessible, to show individuals whether they may have crossed paths with individuals diagnosed with coronavirus. Without additional controls, this widespread collection and centralized aggregation of this sensitive data arguably presents additional risk such as a data breach[11].

Other examples of how privacy-by-design principles can be incorporated into contact tracing applications include: (i) focusing on anonymized location data; (ii) limiting the processing of personal data only to that which is necessary and proportionate to responding to COVID-19; and (iii) retaining the data only so long as necessary to assist in limiting the spread of COVID-19. Specific government organizations, such as the United Kingdom's Information Commissioner[12] and the European Data Protection Board[13] support these types of measures.

Beyond privacy concerns, it is also important to address common security risks during development, and thoroughly test applications prior to release. The OWASP mobile "Top 10"[14] publication is a useful resource for developers to identify common vulnerabilities and incorporate secure coding practices. In addition, the OWASP Mobile Security Testing Guide provides a comprehensive manual for testing and reverse engineering for iOS and Android mobile applications. Once apps are launched, organizations should consider implementing a vulnerability management program[15] to help identify, risk-rate and remediate vulnerabilities.

Understandably, the world wants to leverage technology to aid in the COVID-19 response as quickly as possible. While "speed" is an important goal, if users feel their privacy is not being respected, it could adversely affect adoption rates and undermine the fight against COVID-19. As such, developers and their legal

---

[9] Joint Statement on Contact Tracing: Date 19th April 2020, available at https://www.esat.kuleuven.be/cosic/sites/contact-tracing-joint-statement/ (last visited May 5, 2020).

[10] Isobel Asher Hamilton, *Compulsory selfies and contact-tracing: Authorities everywhere are using smartphones to track the coronavirus and it's part of a massive increase in global surveillance*, available at https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3#south-korea-gives-out-detailed-information-about-patients-whereabouts-2 (last visited May 5, 2020).

[11] Charlie Osborne, *Proposed government coronavirus tracking app falls at the first hurdle due to data breach*, available at https://www.zdnet.com/article/proposed-government-coronavirus-app-falls-at-the-first-hurdle-due-to-data-breach/ (last visited May 5, 2020).

[12] *See* United Kingdom Information Commissioner's Opinion, *Apple and Google joint initiative on COVID-19 contact tracing technology*, available at https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf (last visited May 5, 2020).

[13] *See* 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*, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf (last visited May 5, 2020).

[14] *OWASP Mobile Top 10*, available at https://owasp.org/www-project-mobile-top-10/ (last visited May 5, 2020).

[15] *Vulnerability management*, available at https://en.wikipedia.org/wiki/Vulnerability_management (last visited May 5, 2020).

counterparts should embrace privacy-by-design principles and vulnerability testing and assessments to help strike the right balance.

Back to June 2020 issue