COVID-19: WHEN EU TRACKING APPS MEET THE PANDEMIC, TRUST AND PRIVACY BY DESIGN ARE THE HOSTS

Date: 20 May 2020

EU Data Protection, Privacy, and Security Alert

By: Claude-Étienne Armingaud, Natali Adison

As the COVID-19 pandemic continues to spread around the world and cause unprecedented health and economic challenges, technological measures, once thought extreme, are now being deployed for the purposes of contact tracing, infection tracking, and quarantine compliance. While the search for the right tracking app and software development kits continues, the European Union (EU) is still far from finding a consensus on harmonized model and functionalities. Nevertheless, it is already clear that while app design may be the end result, a complex process of regulatory compliance, risk management and ethics checks, and balances lie ahead.

TO CENTRALIZE OR DECENTRALIZE, THAT IS THE QUESTION

The next normal will consist of the ability to predict what may be expected in the near future and how continued health and economic disruptions can be mitigated. In their search of that kind of predictability, EU Member States are communicating their lockdown exit plans, which to a certain extent include practices of contact tracing, disease monitoring, and regularly testing massive numbers of people. In that regard, tracking devices may particularly be relevant both during the exit and thereafter, provided their potential to help preventing COVID-19 infection chains and reducing the risk of further transmissions.

In view of the development of mobile tracking devices, EU institutions have published guidelines, a common EU toolbox and a data protection guidance regarding tracking apps, all favoring a pan-European decentralized approach, which led to some criticism from confused developers. Subsequently, the European Data Protection Board published a clearer set of guidelines consisting of Guidelines on the use of location data and contact tracing tools and Guidelines on the processing of data concerning health for the purpose of scientific research. However, as communicated through the EU Exit strategy Roadmap, the only existing consensus regarding mobile tracking apps is that their use will be subject to a voluntary basis, a specific timeframe, and that the national health authorities should be involved in the design of the system. Consequently, EU Member States seem to be lost in translation and are considering and deploying different approaches.

Some EU Member States, such as Austria and Estonia, have recently announced they plan to implement a protocol called DP-3T, a decentralized pan-European technical solution, which operates via Bluetooth functionality, embedded in mobile devices. In the meantime, other EU Member States, such as France, the United Kingdom, and Italy, are deploying a different architecture of a centralized national contact-tracing app based on the contract-tracing framework, while Germany and other EU Member States are seeking to adopt the Pan-

European Privacy-Preserving Proximity Tracing , a proximity matching decentralized solution, and Belgium decided to stick to traditional manual contact tracing.

The main difference between the considered solutions lies in the storage location of sensitive data, including health and location data, which leads to different privacy and data protection consequences:

- The decentralized solution entails storage of data exclusively on the user's device rather than in a centralized database and is based on devices generating and sharing ephemeral Bluetooth identifiers, allowing connection between phones located in close proximity of one another. Users could opt-in to share their phone number or symptom details in the app after a confirmed COVID-19 diagnosis, which would be used by health authorities in order to further contact and advise them on the best course of action.
- The centralized solution entails proximity data storage in a central server controlled by a national authority (e.g., health care service), which may create concerns of government's mass surveillance on citizens in the absence of strong fundamental rights and security safeguards.

While the various objectives and architecture considered by EU Member States diverge significantly, they will all commonly rely on the use of sensitive personal data and data analytics. However, while apps are being developed, it is clear that there is more than meets the eye and a process of constantly evolving checks-and-balances, as discussed hereunder, must be in place in order to enable a tracking app to function both legally and efficiently.

THE ROAD TO SUCCESS IS UNDER CONSTRUCTION, INCLUDING PRIVACY AND DATA PROTECTION BY DESIGN

Remarkably, countries such as China and Israel have demonstrated that tracking apps prove to be effective (when immediately put in place) to enforce the confinement measures, to prevent the spread, or to treat COVID-19. Nevertheless, EU Member States will need to strike the right balance when it comes to the legality and ethical soundness of tracking apps. Given that tracking apps require the collection and storage of a myriad of personal data, including sensitive (health) data, device identifiers and, potentially, location data, both the GDPR (General Data Protection Regulation) and ePrivacy Directive, as well as their implementing legislations, will mandate specific compliance steps.

While mobile tracking apps will subject their use to a voluntary basis, their efficiency will rely on users' trust and perceived added-value. Consequently, compliance with fundamental rights, privacy and data protection by design and by default are crucial. While it is clear that from a technological perspective, a decentralized solution of contact tracing via Bluetooth hardware would facilitate compliance with the data minimization tenet of GDPR, the lack of centralized storage may also limit the possibilities for governments to steer the public through the crisis. On the other hand, gathering too much data would also open the door to a myriad of risks of privacy, security breaches and public backlash, gathering too little may render the app ineffective of relying on a voluntary basis.

In order to be effective, tracking apps should: (1) provide users accurate information on the pandemic, provide questionnaires for self-assessment and guidance; (2) provide a safe communication forum between patients and doctors; and (3) alert users who have been in proximity to other infected users in order to limit further spread of the disease.

THE POSITIVE IMPACT OF TRUST BY DESIGN

While EU institutions have acted rapidly and provided extensive guidelines regarding the added value of tracking apps in the COVID-19 fight, they have surprisingly left some opportunities on the table. The recent weeks have shown that following the EU guidelines has led EU Member States to adopt a fragmented and uncoordinated approach in their deployment of tracking apps, which is likely to hamper the effectiveness of the latter to combat the pandemic. Clearly, the idea of a single harmonized European app seems more unlikely everyday, or even that of compatible and interoperable centralized and decentralized apps across EU Member States.

Another issue which may affect the effectiveness of tracking stands in their expected voluntary use. Based on a study by WHO and Oxford University, contact tracing apps would need to be used by at least 60 percent of a given population in order to be effective. In other words, European trust will either make or break the success of tracking apps.

Moreover, there seems to be a lack of clarity on the functioning of tracking apps, and the efficiency in densely populated areas, when Bluetooth contact tracing may generate false positives or negatives. Other operational factors may also limit the relevancy of the processing, such as the possibility for users to switch the app (or its Bluetooth signal) on and off, the steady provision of relevant information to the users or will it be provided, or just the carrying of their mobile phone on a continuous basis.

In a nutshell, contact tracing apps will only be worth as much as the trust their users are willing to grant them.

ACTION ITEMS

The most effective way for tracking app developers/businesses/governments to leverage users' trust would consist in embedding the “Privacy by Design” and “Privacy by Defaults” principle of GDPR and combine them into “Trust by Design” (TbD) into their solutions by designing transparent, value-generating experiences, which will empower users to make informed choices about how their data will or will not be used.

The following TbD best practices will enable all stakeholders to generate acceptability at every stage of the operational process:

- Understanding the exact impact contact tracing apps may have on their users and the possible consequences;
- Defining and determining the absolute necessary personal data, sensitive or not, to be processed and the justifiable purposes thereof (data minimization and purpose limitation);
- Determining the exact technologies to be used and the legal basis relied upon, which will vary according to the type of data collected (e.g., personal, sensitive, pseudonymized, anonymized, aggregated, structured or unstructured);
- Implementing less intrusive measures, e.g., proximity data instead of location data and aggregate and de-identify/anonymize data where possible;
- Assessing the proportionality of the data processing, to ensure that no less intrusive solution could achieve a similar goal;
- Considering with whom the data is shared and for what purpose;

- Implementing sufficient security measures (e.g., state of the art encryption measures);
- Documenting all the steps taken, demonstrating necessity and proportionality, carrying out a Data Protection Impact Assessment, and keeping that document under review;
- Providing users clear and transparent information about the origin of the data that will be collected, shared (with whom) and for what reasons. Such transparency and thoroughness in the information will be key when relying on a voluntary use based on trust;
- Ensuring that data is only retained for as long as necessary to serve its purpose and is irrevocably destroyed thereafter;
- Verifying the proper functioning accuracy of the solution and ensuring it may not be linked with other databases;
- Ensuring interoperability and information exchange with the supporting authorities and servers within and beyond national borders, and that all necessary data transfer safeguards and security measures are in place;
- Enabling users to withdraw their consent, where applicable, opt -out or uninstall the tracking app at any time;
- Managing vulnerabilities actively through the app's lifecycle and enabling users to take control and effectively intervene from within the system in order to recall, contest or delete incorrect disease notifications or ensuing restrictions;
- Where the tracking app entails warning those who have been in close contact with COVID-19 affected persons, assessing whether this should be done anonymously or through trusted health organizations in order to provide transparency; and
- Consulting and collaborating with the relevant Data Protection Authorities all through the development and deployment of the tracking app.

As public health authorities, developers, and tech companies are working on apps to help fight COVID-19, the real issues remain individual compliance, enthusiasm, and, more importantly, the wide-scale testing regime, without which the proximity alerts will remain ineffective.

While every challenge is unique, now is an unprecedented opportunity to show privacy and data protection compliance. If you are interested in privacy and data protection or are a developer or a business considering the development and deployment of a tracking app in response to the COVID-19 pandemic, our resilient K&L Gates' data protection team remains available to assist you during these difficult times. Stay safe.

KEY CONTACTS

CLAUDE-ÉTIENNE ARMINGAUD
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.