Acting as Our Fiduciary:

The Duties of Tech Companies in Times of Pandemic

On April 10, 2020, in order to facilitate health agencies across the globe in their efforts to reduce the spread of COVID-19, Apple and Google announced a joint project to use contact -tracing Bluetooth technology. The system is called "Exposure Notifications Express," which will let public health authorities submit parameters for contact tracing to Apple and Google. However, currently, there are only 25 states in the U.S. considering using the Bluetooth contact tracing solution. At the same time, foreign governments, including Australia, France, India, Italy, Japan, have failed to convince at least 60% of their respective population to adopt contact tracing apps, a threshold that Oxford University found necessary for the technology to prove meaningful. While governments are reluctant to cooperate with Silicon Valley giants, the general public is hesitant to trust the capacity of both governments and companies to curb the pandemic through an app.

In order to obtain the trust of the people, we believe that "Information Fiduciary Duties" should be imposed on the tech companies; however, it's not always clear what that means. Therefore, this article aims to examine the core idea of the information fiduciary theory, analyze whether the current guidelines released by Apple and Google meet these duties, and propose additional duties that the current approach lacks.

Traditional fiduciary relationships are established when trust is at the core of the relationship. This typically exists between doctors and patients or lawyers and clients. As the clients rely on the professional responsibility to safeguard their sensitive information, these professionals are called "information fiduciaries".

Similarly, as massive amounts of data are stored on Facebook and Google, these companies must also take on fiduciary responsibilities. The theory was first introduced by Yale Law Professor Jack Balkin in an article known as the "Information Fiduciary Theory". Balkin applies the duties of care and loyalty to information service providers. Specifically, the *duty of care* requires data controllers to take all necessary measures to ensure the most robust protection of sensitive information, while the *duty of loyalty* compels data controllers to preserve the clients' interests from actual or potential conflicts of interest.

To some extent, Google and Apple's contact tracing policy meets both the duty of care and the duty of loyalty. The *duty of care* is met as random Bluetooth identifiers rotate every 10-20 minutes to prevent tracking. The system is employed only for contact tracing by public health authorities' apps, and the companies will disable the exposure notification system on a regional basis when it is no longer needed. The companies fulfill their *duty of loyalty* by not collecting geolocation data. Simultaneously, the collected data is not going to be monetized by the company, and the technology can be turned off at any time. However, despite all these measures, the system has not been fully approved by governments and notification apps have not been downloaded by enough people. Thus, additional measures should be developed. Inspiration can be drawn from legal scholarship and the IoT (Internet of Things) baseline requirements proposed by ETS (The European Telecommunications Standards Institute).

The additional measures necessary to promote confidence in the contact-tracing system can be elaborated through the concept of duty of care and duty of loyalty. In order for these measures to be binding, they should be included in the terms and conditions of the companies' policy. For the duty of care, Apple and Google must commit to regularly monitoring the system's integrity and keeping the software updated to ensure the strongest level of protection. Additionally, establishing a public policy disclosure regarding vulnerabilities and data breaches is essential to keep the public informed. As for duty of loyalty, third parties shall not access the collected data, including law enforcement, except if statutorily provided. Moreover, the collected data should not be used for monetization. The data should not be employed to enhance the company's service, such as the newly released COVID data in Google Maps. Finally, sunset provisions should be included in the terms and conditions to prevent further misuse of the data and ensure this mechanism's temporary nature.

In this unprecedented pandemic, people expose their most intimate vulnerabilities to companies absent legally defined responsibilities. As the Apple-Google guidelines fill the gap by protecting users' information and placing both companies as the user's information fiduciary, more measures should be implemented in the terms and conditions between the government and the company. Overall, Balkin's framework helps us understand how the terms and conditions between users and companies, companies and governments should be designed. The fiduciary model, thus, serves as an appropriate and compelling standard for tech companies.

Kamel Ajji, Affiliate Fellow at Yale Law School Information Society Project and Doctoral candidate at Paris 2 Panthéon Assas University -- kamel.ajji@u-paris2.fr

Chieh Jan (Simon) Sun, Doctoral student at Indiana University (Bloomington) Maurer School of Law and Duke University School of Law Graduate '20. -- sunchi@iu.edu