crowell moring

CLIENT ALERT

Mobile Applications For COVID Tracking & Tracing – Balancing the Need for Personal Information and Privacy Rights in the Time of Coronavirus

Apr.15.2020

Introduction

As the COVID-19 pandemic continues and there is mounting pressure to ease business and social restrictions, governments, non-profits, and private corporations are all increasingly focused on solutions that would not only track and trace the movements of individuals to determine exposure to the virus and compliance with stay-at-home orders, but also potentially signal the person's COVID-19 status. This, of course, raises a slew of privacy issues.

Establishing where an infected individual has been and with whom they may have interacted is critical for both public and private entities attempting to manage the impact of this virus, to slow its spread, and to assess when restrictions can be lifted. One method of contact tracking and tracing is gathering cellular location information through the use of purpose-built mobile applications that individuals can download on their mobile devices. These mobile applications now being developed for the stated purpose of COVID-19 tracking and tracing, referred to herein as "COVID Apps," may use Bluetooth technology to measure proximity to other Bluetooth-enabled mobile devices, or they may use GPS data and other technologies such as Wi-Fi to track precise location of individual mobile devices. They may also include features such as QR-Codes for purposes of verifying a person's COVID-19 status or controlling access to certain locations.

Mobile operating system platforms are also in the process of releasing tools for developers of COVID Apps, be they government entities or private companies, and even integrating some of these tools as part of their operating systems.

Several governments have announced the development or launch of COVID Apps in some or all of their territory, including Russia, Singapore, India, and multiple EU Member States. Some are making the download of COVID Apps mandatory, while others are relying on individuals to voluntary download them and self-report COVID status, making such data available to designated government authorities. Approaches to what data gets collected through COVID Apps and who has access to it vary significantly depending on local laws. To the extent that companies in the United States are planning on introducing COVID Apps, the following laws, at a minimum, may be implicated:

- State personal information laws;
- Federal and State consumer protection laws;
- Federal health information laws;
- Federal and State information security laws;
- Government contracting laws; and
- Employment laws.

As described in more detail below, companies and other entities developing and deploying COVID Apps for use in the United States should carefully consider:

- The types of data they collect and the technologies they use;
- The types of third parties accessing data, or providing data, collected in and through the COVID App;
- The types of contracting parties involved in connection with the COVID App;
- The jurisdictions and platforms in which the COVID App is deployed;
- Information security; and
- Disclosures made to COVID App users.

The California Consumer Privacy Act

There are many state laws that could be triggered by a COVID App gathering location data or health information on an individualized and identifiable basis. For any COVID App to serve its intended purpose, it would need to identify at least the individual's self-reporting infection status.

For private companies considering developing or using a COVID App, the California Consumer Privacy Act (CCPA) is likely the most prominent state law that must be considered. The CCPA requires that any entity qualifying as a "business"[1] provide "consumers" – which it defines as lawful residents of California – with a number of rights, and obligates businesses to make specific disclosures about the collection and use of personal information.

The CCPA defines "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The statute also gives a non-exclusive list of examples, specifically including "geolocation data." Any COVID App collecting geo-location data or health information specific to a California resident would almost certainly be collecting "personal information" within the meaning of the law – assuming that data could be "reasonably linked, directly or indirectly, to particular consumer or household." Under this broad definition, such location information or health information could still be considered personal information even if disassociated from an individual's name, if it could still be linked to some other identifying information, such as a phone number or unique device identifier – for example, a device advertising identifier. Some COVID Apps may ask users to define a "home" location for the purposes of monitoring exposure and quarantine.

Under the CCPA, businesses must provide consumers with a notice "at or before the point of collection" of personal information that describes both the categories of personal information to be collected and the purposes for collecting that information. Businesses must additionally allow consumers to request access to and request deletion of personal information, as well as opt-out of the sale of any personal information, and make more specific disclosures about the collection and processing of personal information in a detailed privacy policy.

Some COVID Apps claim that any data collected is de-identified and/or aggregated, and that no personal information is processed during their use. While the CCPA makes clear that personal information does not include consumer information that is de-identified or aggregate consumer information, there are specific requirements that a business must meet in order for information to qualify as de-identified.

For information to be considered "de-identified" under the CCPA, it cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses de-identified information:

1. Has implemented technical safeguards that prohibit re-identification of the consumer to whom the information may pertain.
2. Has implemented business processes that specifically prohibit re-identification of the information.
3. Has implemented business processes to prevent inadvertent release of de-identified information.
4. Makes no attempt to re-identify the information.

At a minimum, any business considering the development of a COVID App for broad use in the United States should be prepared to carefully document what personal information is collected, how it is used, who it is shared with, and to provide individuals with an effective means to request access to, and deletion of, any personal information associated with it. If instead a business plans to represent that information collected will be "de-identified," the business should pay careful attention to documenting the specific safeguards required under the CCPA.

Consumer Protection Laws

At the Federal level, companies should consider their use of personal information collected by means of a COVID App through the lens of the Federal Trade Commission (FTC) Act. In particular, Section 5(a) of the FTC Act states that "unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful." 15 U.S.C. Sec. 45(a)(1). The FTC Act could be implicated, for example, where a company fails to disclose the collection of COVID-19 tracking information or fails to disclose third parties with whom such personal information is shared. Similarly, many states, such as the State of New York, prohibit "deceptive acts or practices in the conduct of any business, trade or commerce." NY Gen Bus L § 349.

The impact of these consumer protection laws is that any consumer disclosure relating to the COVID App, such as a privacy policy, must accurately describe how the COVID App collects personal information, for what purposes personal information is used, and with whom personal information is shared.

With respect to sharing of personal information, particular care must be taken to ensure that the developer of the COVID App does not include in it any software elements that share, inadvertently or intentionally, personal information with third parties where such sharing is not disclosed in the COVID App's privacy policy.

The Health Insurance Portability and Accountability Act

Developers of COVID Apps could be subject to restrictions under the federal health privacy law, the Health Insurance Portability and Accountability Act of 1996, and its implementing regulations (collectively, HIPAA). HIPAA generally applies to covered entities (health plans, health care clearinghouses, and most health care providers) and their business associates, which include COVID App developers and other vendors that create, receive, maintain, or transmit protected health information (PHI) for, or on behalf of, a covered entity (or another business associate).

Whether a developer of a COVID App falls under HIPAA's definition of a business associate is a fact-specific inquiry. COVID App developers will need to carefully consider all relevant facts and circumstances to determine whether they have created or are

offering the COVID App on behalf of a covered entity or are otherwise providing services to a covered entity that involve access to PHI.

This determination will come down to a careful consideration of all facts and circumstances, including but not limited to (1) whether the COVID App developer has executed agreements with any covered entities, (2) whether the COVID App developer receives any funding from covered entities, (3) whether consumers independently select the COVID App, and (4) how much control consumers have over directing their data to third parties.

If a COVID App developer is indeed subject to HIPAA, it will need to comply with various privacy and security requirements and sign business associate agreements with any covered entity for which it creates, receives, maintains, or transmits PHI. This includes implementing reasonable and appropriate safeguards to protect PHI, conducting periodic security risk assessments, and developing and maintaining HIPAA policies and procedures. In addition, PHI collected through the COVID App will be subject to HIPAA restrictions and generally may not be disclosed except as permitted or required under HIPAA and the applicable business associate agreement.

Information Security Laws

If COVID Apps interface with government systems, or in the event a company compiles information that can be utilized for tracking COVID-19 on the government's behalf, then NIST SP 800-53, Rev. 5 (currently in draft form) would likely be implicated as an information security standard. This NIST standard integrates both privacy and cybersecurity controls, and companies that will or may need to comply with it should also be considering use of the NIST Privacy Framework and the NIST Cybersecurity Framework.

At the State level, California and Ohio are prominent examples of states that have encouraged the protection of consumers' sensitive information. For example, Cal. Civ. Code § 1798.81.5(a)(1) requires companies to "maintain reasonable security procedures and practices appropriate to the nature of the information it processes." Companies should note that the meaning of "reasonable security" in this statute was informed by the California Attorney General's 2016 Data Breach Report, which listed the Center for Internet Security's Critical Security Controls as an information security baseline that all organizations that collect or maintain personal information should follow. The Report went on to state that "failure to implement" these Controls indicates that a company lacks "reasonable security."

The Ohio Legislature is incentivizing companies to safeguard personal information through a Safe Harbor provision of the Ohio Data Protection Act. The Safe Harbor protects entities against data breach civil suits where they "reasonably conform" to a recommended information security framework, including but not limited to:

- National Institute of Standards and Technology's (NIST) Cybersecurity Framework;
- NIST SP 800-171;
- NIST SP 800-53;
- Federal Risk and Authorization Management Program's (FedRAMP) Security Assessment Framework; and
- Center for Internet Security's Critical Security Controls for Effective Cyber Defense; and
- International Organization for Standardization (ISO) 27001 – Information Security Management Systems Standards.

App Distribution Platform Restrictions

Aside from legal restrictions, any COVID App will need the permission of the major mobile application distribution platforms in order for any widespread adoption of a COVID App to take place. These app distribution platforms have standard requirements for permitting any mobile application that collects personal information to be available on their platforms. Furthermore, mobile application platforms place restrictions on the types of entities that are allowed to publish COVID Apps on their platforms.

Conclusion

In general, businesses considering the development of a COVID App should consider ensuring that, as the COVID App is built, policies are drafted covering the specific personal information collected, the uses of that personal information, and how that personal information is shared. Additionally, any COVID App should implement a feature that captures a record of when a user is asked to consent to the use of location information, and includes a way for the user to access and review these practices. Given app distribution platform restrictions, any businesses outside of the health, medical, and educational sectors should exercise appropriate due diligence about investing in the development of a COVID App for distribution on app distribution platforms.

---

[1] Per Cal. Civ. Code § 1798.140(c) "Business" means:
(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:
(A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.
(B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.
(2) Any entity that controls or is controlled by a business as defined in paragraph (1) and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, service mark, or trademark.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Kristin J. Madigan, CIPP/US
Partner – San Francisco

Phone: +1 415.365.7233
Email: kmadigan@crowell.com

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com

Jarno Vanto, CIPP/E, CIPP/US
Partner – New York
Phone: +1 212.803.4025
Email: jvanto@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Brandon C. Ge
Counsel – Washington, D.C.
Phone: +1 202.624.2531
Email: bge@crowell.com

Matthew B. Welling
Counsel – Washington, D.C.
Phone: +1 202.624.2588
Email: mwelling@crowell.com

Michael G. Gruden, CIPP/G
Associate – Washington, D.C.
Phone: +1 202.624.2545
Email: mgruden@crowell.com