JONES DAY | One Firm Worldwide®

WHITE PAPER

July 2020

A Guide to Navigating Cybersecurity, Privacy, and Employment Law Issues with COVID-19 Contact Tracing in the Private Sector

As the United States and other countries gradually ease stay-at-home orders and mandatory lockdowns, data-driven technologies have become increasingly discussed as a potential strategy for tracing and mitigating the further spread of the COVID-19 virus. While these emerging technologies can serve a variety of pandemic response purposes, one use is to automate contact tracing through mobile applications, wearable devices, and other tracking technologies to complement other efforts to safely reopen the economy.

The use of digital contact tracing solutions within business enterprises raises a variety of privacy, cybersecurity, and employment law issues organizations cannot afford to overlook. This *White Paper* provides a practical, high-level overview of the digital technologies proposed for contact tracing in the private sector, identifies potential cybersecurity, privacy, and employment law concerns that may arise in connection with deploying these technologies, and summarizes some of the legislative proposals to address these concerns.

TABLE OF CONTENTS

DIGITAL CONTACT-TRACING TECHNOLOGIES

Technology Overview: How Does It Work?

At a high level, digital contact-tracing technologies automate the process of manually identifying and informing individuals who have come into contact with others testing positive for the COVID-19 virus. The goal of contact tracing is to suppress transmission of the virus by getting ahead of its spread. To this end, digital contact-tracing technologies can promote rapid identification of the individuals who must self-isolate and seek priority testing after coming into contact with a positively diagnosed person during the incubation period.

While much attention has been devoted to contact-tracing technologies developed by major technology companies for use by public health authorities, companies are developing their own solutions and repurposing existing technologies for use in the private sector. These solutions generally rely on mobile applications installed on smart phones, wearable technologies, or other tracking mechanisms, such as Bluetooth beacons.

Digital contact-tracing solutions vary and are rapidly evolving. Current contact-tracing technologies generally rely on the collection of either proximity data or more precise geolocation data, or a combination of both. Contact-tracing solutions available for use in the private sector also may link proximity or geolocation data with other categories of personally identifiable information such as names and contact information, identification numbers (e.g., employee ID), data related to a COVID-19 diagnosis or symptoms, and information about third parties with whom the individual has come into contact. Understanding the nature of the data collected by a particular device is critical to assessing the legal issues that will arise when deploying a given technology.

Proximity Data. Proximity data generally refers to information that identifies the distance between two individuals and the duration of their interaction, as opposed to the individual's precise location in space and time. Bluetooth signals are a popular technology for measuring proximity. Using this technology:

- Person A downloads a mobile application or uses a wearable device, each of which can broadcast a unique identifier via Bluetooth on a rolling basis. Other compatible applications or devices in close proximity detect this identifier.
- When devices approach one another, the technology estimates the distance using the Bluetooth signal strength. If the technology measures a distance of approximately six feet or less for a sufficient period of time (as determined by either the administrator of the technology or its manufacturer), the devices record the interaction.
- If Person A learns she is infected with COVID-19 and uploads her diagnosis or otherwise communicates it to her employer, other individuals who came into contact with her for a sufficient period of time (according to the technology's risk calculation algorithm) can be notified so they can take appropriate self-isolation and testing measures. If the employer uses Bluetooth beacons on premises that interface with a mobile application or wearable device, proximity data also can be used to identify areas that require disinfection.

Geolocation Data. Geolocation data generally refers to information capable of determining the physical location of an individual at a specific point in time using location data generated, for example, by a global positioning system ("GPS"), WiFi, or cellular site location information ("CSLI") stored by telecommunication operators. Technologies that rely on "geolocation data" can:

- Create "heat maps" to visually track the spread of COVID-19 in a particular area and to communicate zones of elevated infection in the population;
- Log an individual's location data in order to notify other individuals who test positive of encounters they may have had while contagious or aid contact-tracing efforts by reminding the individual of his or her location history and potential encounters with others; or
- Measure proximity between individuals and notify those who come into contact with infected individuals of a potential exposure.

Depending on the design, technologies being deployed in the private sector may grant the company centralized access to detailed logs of employee interactions within the organization and even health information about personnel using the technologies.

Digital contact tracing is new and developing and may prove an imperfect solution to automating contact-tracing efforts. For example, to the extent it relies on users to self-report diagnoses, that may yield either over-reporting (e.g., individuals indicate they have COVID-19 based on symptoms even without testing) or under-reporting (e.g., individuals fail to update their status on a digital contact application).

How Companies Are Using Contact-Tracing Technology

Companies are rapidly ramping up use of contact-tracing solutions for a variety of business purposes. Some uses of this technology in the private sector include:

Employers. Mobile applications and wearable devices can aid employers' internal contact-tracing efforts and help verify that employees abide by social distancing guidelines in the workplace. Some employers are requiring employees to wear and activate such devices. If an employee reports symptoms or a positive diagnosis, companies using this technology can identify and inform other employees who may have been exposed and, depending on the data collected, identify physical locations in the workplace that may require disinfection and cleaning. In addition, employers can potentially use data from contact-tracing applications to quickly identify locations or contexts in which appropriate social distancing is not being observed.

Universities and Schools. Much like employers, universities and schools are contemplating using contact-tracing applications to inform students and staff if they have been exposed to an individual who has tested positive and to monitor adherence to social distancing guidelines. We have written about specific considerations for education institutions in light of the COVID-19 pandemic in our *White Paper*, "A Guide to Navigating the COVID-19 Crisis for Institutions of Higher Education."

Cooperation with Public Health Authorities. Private-sector companies have also considered requiring employees, students, or customers to use a contact-tracing technology managed or mediated by a federal, state, or local public health authority as a means of contributing to community control of COVID-19. Indeed, some companies developing contact-tracing solutions for internal use are considering ways to leverage the technology to collaborate with external public health sources. In the European Union, France and Italy have already released their own contact-tracing applications, while Germany and the United Kingdom are about to do so.

CYBERSECURITY, DATA PRIVACY, AND EMPLOYMENT LAW RISKS

Before deploying a contact-tracing solution, companies should carefully evaluate the security features of the technology; understand the types of data that will be collected; and consider where, how, and by whom that data will be stored, accessed, used, and disclosed and how long the data will be retained. Using that information, companies can assess the cybersecurity and legal risks, develop appropriate policies and procedures, and properly train stakeholders.

Cybersecurity

Digital contact tracing presents potential security risks. Applications, devices, and centralized databases may collect sensitive information (e.g., an individual's COVID-19 health status and geolocation data) and may be vulnerable to malicious attacks from bad actors looking to exfiltrate such information. U.S. law enforcement and national security officials are issuing increasingly stark warnings about a surge of attempted cyber intrusions and other malicious cyber activity seeking to exploit weaknesses due to, for example, reduced IT staffing or use of insecure networks.

A data security incident could give rise to a variety of harms. Companies suffering a significant data security incident may incur large incident response and remediation expenses and face an array of legal challenges, including regulatory investigations and litigation. Their reputations and relationships with employees and business partners also may be negatively impacted.

Cyberattacks also could interfere with the operational effectiveness of digital contact-tracing technologies. For example, denial of service or ransomware attacks may prevent logging of contacts and/or reporting of infections or may otherwise corrupt the integrity of the data. Organizations should consider security measures that are appropriate in light of the risk involved in the data processing activity. Such measures could include:

- Developing technical and policy controls that limit who has access to sensitive data generated by digital contact tracing;

- Implementing technical measures to improve security (e.g., encryption and patch maintenance);

- Systematically monitoring the environment to detect anomalous activity (e.g., proactive review of logs);

- Conducting appropriate due diligence and oversight of third-party vendors that an organization uses to develop, operate, or manage digital contact-tracing technology;

- Executing written agreements with the third-party providers of the contact-tracing technologies that require maintenance of appropriate security measures (e.g., encryption controls), and contemplate data breach incident response requirements and indemnification in the event of an incident; and

- Reviewing incident response plan protocols, including updating contact information for incident response team members, establishing secure communications channels, and confirming incident reporting protocols for those employees who may still be working remotely.

Data Privacy

Use of digital contact-tracing solutions also requires careful consideration of data privacy issues. To this end, the Federal Trade Commission ("FTC") has offered guidance for companies seeking to leverage consumer data to facilitate contact tracing and other pandemic response efforts. The FTC underscored the importance of deleting data when the crisis subsides and limiting the purposes for which data is used to those addressing pandemic-related issues. The guidance also cautions companies to consider privacy and security issues throughout the lifecycle of developing their products and services. While the FTC's guidance echoes longstanding privacy tenets and positions the Commission has taken in previous enforcement actions, companies should bear in mind this advice and consider various data privacy issues, including the following.

Consent or Other Legal Basis for Collection and Processing. Organizations contemplating the use of contact-tracing technology should identify the legal basis for collecting and processing data under laws such as the General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA"). For example, under the GDPR, potential legal bases could include consent of the data subject or the legitimate interest of the data controller, if specific requirements are met. Under both the GDPR and the CCPA, organizations must provide notice prior to collecting personal information that informs individuals of the key features of the processing of their data, such as categories of data that will be collected and the purposes of the collection.

Data Minimization. Contact-tracing technologies may allow organizations to access and collect more data than necessary for achieving workplace safety, and, therefore, organizations should assess exactly what data is needed. For example, organizations should consider whether to collect proximity data instead of geolocation data and whether to obtain data that identifies the users or only random identifiers processed in a way that prevents re-identification of the individuals.

Sensitive Data. Contact-tracing technologies may allow companies to collect information that raises privacy concerns as a matter of law and/or perception, such as health and geolocation data. Device location data, for example, may be subject to heightened privacy protections in certain circumstances by, for example, the FTC and state privacy laws. The GDPR imposes specific requirements for processing special categories of data, such as health data, including that the processing be for health care purposes, necessary for the public interest in the area of public health, or based on the explicit consent of the data subject. These types of sensitive data are higher risk and require special consideration.

Secondary Use of Data and Purpose Limitations. Companies using contact-tracing technology should consider whether to strictly limit collection, use, and disclosure of any data to contact tracing or whether to permit secondary uses of such data. Any such secondary uses could implicate additional legal considerations. For example, the GDPR generally requires a clear definition of the purpose(s) of the data processing and prohibits uses outside those defined purposes. Similarly, the final proposed regulations to the CCPA prohibit the use of a consumer's personal information for purposes "materially different than those disclosed in the notice at collection" unless the business directly notifies the consumer of the new use and obtains "explicit consent from the consumer to use it for this new purpose."

Biometric Privacy Laws. As new contact-tracing solutions emerge, developers may introduce new functionalities that implicate data privacy laws, such as the integration of facial recognition software to identify, for example, the user of a contact-tracing application. The collection of biometric data could

trigger obligations under state biometric privacy laws, such as those in Illinois, Texas, and Washington.

Data Retention and Disposal. Companies also will need to determine how long to retain the data processed by contact-tracing technologies. The GDPR, for example, generally provides that data should be retained only for the period necessary to achieve the processing purpose defined by the data controller. For contact tracing in the context of COVID-19, companies may consider whether 14 days is an appropriate retention period since that is the currently understood incubation period for the virus, or whether a longer period may be justified. Relatedly, companies should take steps to dispose of data in compliance with specific laws that govern destruction of certain types of sensitive data.

Sharing Data with the Government. Any cooperation with the government that gives public health authorities or other agencies access to data collected through contact-tracing technologies may give rise to additional privacy issues.

Interoperability. If companies envisage making their contact-tracing apps interoperable with other contact-tracing apps, this may require factoring additional elements into the data protection compliance analysis. Under the GDPR, adding interoperability in the context of contact-tracing apps will typically require making sure the data subjects keep sufficient control over their data and have sufficient transparency on the additional recipients of the data, as well as who the additional data controllers will be, if any. In addition, interoperability may trigger questions about the respective accuracy of the data sets of interoperable apps—interoperability should not be detrimental to the accuracy of the data processed by either of the apps.

HIPAA. Organizations contemplating the use of contact-tracing technology need to determine if the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") will be implicated. HIPAA applies to only "covered entities" (e.g., health plans, health care clearinghouses, and certain health care providers) and their "business associates," which process protected health information on behalf of covered entities. If the organization is not a covered entity or a business associate under HIPAA, the HIPAA analysis ends there. If the organization is subject to HIPAA's requirements: (i) HIPAA could subject companies and the data derived from their contact-tracing apps to stringent privacy and security requirements that may restrict the collection and sharing of individuals' health-related information without the individuals' prior written authorization; and (ii) the organization would need to treat contact-tracing data that meets HIPAA's definition of "protected health information" in the same manner that the organization handles its other protected health information. In some cases, covered entities may have functions or components that are not subject to HIPAA (e.g., when operating in their capacity as employers or in the case of "hybrid entities" that have covered and non-covered components for purposes of HIPAA). Those organizations may want to operate the contact-tracing process through the non-covered entity function or component.

Labor and Employment Law Risks

Use of contact-tracing technologies also implicates various labor and employment laws. The precise legal considerations will vary depending on the type of information collected, the way in which the information is used, and the jurisdiction in which the business operates. The labor and employment laws implicated include the following.

Disabilities Law. The Americans with Disabilities Act ("ADA") prohibits employers from requiring employees to submit to medical examinations or tests unless they are job-related and consistent with business necessity. In most cases, employees testing positive for COVID-19 would pose a direct threat to their coworkers. Therefore, to the extent the technology functions as a medical test, it would likely be considered job-related and consistent with business necessity, at least insofar as the data is used to help track and mitigate the spread of COVID-19 in the workplace. If, however, the data is also used for other purposes—such as tracking worker productivity or gathering information for a disciplinary investigation—an employer would have a more difficult time defending itself against possible ADA claims.

Employers will also need to be mindful of how employee health information collected through the technology is stored and shared. The ADA requires employee medical information to be maintained in separate files and kept confidential. This provision and other laws limit the amount of information that can be shared with employees regarding coworkers who have tested positive for COVID-19.

Health and Safety Laws. The Occupational Safety and Health Act imposes a duty on employers to provide a workplace free of serious known hazards. Similarly, some U.S. states impose duties on employers to take reasonable measures to minimize work-related injuries, including the spread of infectious diseases. The deployment and use of contact-tracing technology may be relevant to whether these duties were met.

The Occupational Safety and Health Administration ("OSHA") requires COVID-19 cases to be reported when they are work-related and meet other criteria. The reporting determination in COVID-19 cases typically turns on whether the illness is work-related. Contact-tracing technology should make it easier to determine the likelihood that an employee contracted COVID-19 in the workplace, and this information must be taken into account in deciding whether to report the illness to OSHA.

OSHA also has standards governing access to and retention of certain medical records and workplace exposure records. Such records must be maintained for the duration of employment plus 30 years, and they must be provided to certain individuals upon request. Careful consideration must be given to whether data collected through contact-tracing technology is subject to these requirements, and to the interplay between these requirements and other laws that may mandate a shorter retention period.

Labor Law. Unionized employers must consider whether existing collective bargaining agreements and federal labor law allow contact-tracing technologies to be deployed, with or without first bargaining with the union. The answer to these questions could depend on the way in which the data is used. If, for example, the data is used strictly for health and safety purposes, the employer may be able to implement the technology unilaterally, but if the data is also used for other unrelated purposes, the employer may either be prohibited from implementing it or able to do so only after first bargaining with the union.

Unionized and non-unionized employers must also take care to avoid using the technology in a way that might infringe on an employee's rights to join a union or engage in other concerted activities. For example, employers subject to a labor organizing campaign would not be allowed to use data collected through contact-tracing technology to determine whether and where employees were meeting with union officials. Even creating the impression that such meetings or other union activities are being watched is unlawful.

Other Considerations. Employers should also be mindful of the potential that information gathered through contact-tracing technologies could be used against them in subsequent litigation. Several employers have already been sued by employees who claim they contracted COVID-19 on the job or were not provided a safe place to work. Employers have a number of possible defenses to these claims. If the lawsuit is not dismissed upfront, however, information gleaned through contact-tracing technology could be used to argue negligence or to substantiate health and safety complaints. This could be the case, for example, if numerous employees were in contact with someone who contracted COVID-19 but the employer failed to warn those employees or follow proper cleaning protocols. Before implementing the technology, therefore, employers should adopt a policy or plan for responding to health and safety risks sure to be uncovered.

POTENTIAL LEGISLATIVE RESPONSES

In the United States, lawmakers are considering privacy and cybersecurity issues in response to the rush to develop and adopt contact-tracing technologies.

Congress has introduced three legislative proposals aimed at providing consumers with greater transparency, choice, protection, and control over the collection and use of their data for managing the spread of COVID-19. Notably, each framework requires affirmative, express consent from users of contact-tracing technologies and identifies the FTC and state attorneys general as relevant enforcement authorities. However, each differs in critical respects, including the scope of protected data, categories of entities covered, availability of a private right of action, and use of a state preemption clause.

- On May 7, 2020, a group of Republican Senators introduced the "COVID-19 Consumer Data Protection Act." The Act would require a wide range of businesses to obtain affirmative, express consent from individuals to collect, process, or transfer health, proximity, or geolocation data for contact tracing related to COVID-19, impose transparency and data minimization requirements, and require

covered entities to implement administrative, technical, and physical data security policies and practices. The bill does not allow for a private right of action and has a pre-emption clause under which states are prohibited from adopting, enforcing, or maintaining any law "related to the collection, processing, or transfer of covered data."

- On May 14, 2020, a group of Democratic lawmakers introduced the "Public Health Emergency Privacy Act." The Act would prohibit the use of certain health-related information for discriminatory or commercial purposes (i.e., advertising or e-commerce), impose various civil rights-related requirements, and allow states to adopt their own stronger privacy protections. It would also provide a private right of action, requiring proof of a concrete and particularized injury in fact, with tiered remedies based on the nature of the violation in addition to a public enforcement framework. In addition to the data elements covered by the "COVID-19 Consumer Data Protection Act," the Democrats' proposal also covers, for example, certain types of medical testing data and contact information.

- On June 1, 2020, lawmakers introduced a bipartisan bill, the "Exposure Notification Privacy Act," which would place obligations on an narrower set of entities than the two bills described above. The entities are defined as "automated exposure notification service[s]" (e.g., operators of any website, online service, online application, mobile application, or mobile operating system that is "designed, in part or in full, specifically to be used for, or marketed for, the purpose of digitally notifying, in an automated manner, an individual who may have become exposed to an infectious disease"). The bill contains various privacy protections, including an affirmative, express consent requirement, a right to deletion, data transfer restrictions except for specifically enumerated purposes, a prohibition on processing covered data for "any commercial purpose," data security requirements, and obligations to notify affected individuals and the FTC in the event of a security breach. The FTC and state attorneys general would enforce the law, and individuals would still be able to bring actions under various federal or state common law or state statutes.

States also are introducing legislative proposals to protect user privacy as contact-tracing technologies are developed and deployed as part of state reopening strategies. For example:

- On May 11, 2020, New York lawmakers introduced a bill that would require that an individual voluntarily opt in to any contact-tracing program. The opt-in disclosure would require provision of a "conspicuous, plain language explanation of the application, the application's functions and any information that the application will collect prior to the user being able to give consent." Any information stored or transmitted by an application would be required to be encrypted. Individuals would be able to withdraw consent at any time, and the bill would establish a cause of action enabling individuals to sue entities responsible for a violation of their privacy rights in connection with contact tracing and to seek damages or declaratory or injunctive relief.

- Also on May 11, 2020, Minnesota lawmakers introduced a bill that would prohibit an employer from mandating the installation of a contact-tracing application on its employees' mobile phone and from requiring employees to share their location information as part of contact-tracing efforts.

- On May 28, 2020, New Jersey lawmakers introduced a bill that would restrict the use of data collected for purposes of contact tracing related to the COVID-19 pandemic, including "digital data from Bluetooth devices or global positioning systems." The bill would require a public health entity that shares contact-tracing data with a third party to name the third party entity on its internet website or on the internet website of the Department of Health, and it would require that the third party use the data only for purposes of completing contact tracing related to the pandemic. The third party would be required to delete the data by the same date the public health entity was required to delete the data (e.g., 30 days). A third party that misuses or discloses COVID-19 contact-tracing data or retains it beyond the permissible date would be liable for a civil penalty up to $10,000.

Although it is unclear whether these U.S. proposals or others will become law, they highlight some of the privacy and security concerns that use of contact-tracing technologies may raise and that companies should consider as they decide whether to deploy contact-tracing technologies. U.S. legislators, at least, appear keen to: (i) limit companies' ability to make the use of contact-tracing applications mandatory; (ii) require notice and clear opt-in consent of the individual prior to download or use of the technology; (iii) limit companies'

ability to use the data collected from contact-tracing applications beyond the COVID-19 pandemic; (iv) impose data minimization and retention requirements; and (v) develop administrative, technical, and physical data security policies and practices to safeguard the data collected in connection with such technologies. International organizations should also be mindful of guidance issued by applicable supervisory authorities on the collection and use of personal data with these technologies to avoid noncompliance with the GDPR.

As digital contact-tracing solutions evolve, companies should continue to monitor developments. Jones Day can assist companies as they consider leveraging contact-tracing applications.

LAWYER CONTACTS

Wendy C. Butler
New York
+1.212.326.7822
wbutler@jonesday.com

Thomas R. Chiavetta Jr.
Washington
+1.202.879.3975
tchiavetta@jonesday.com

Natalia O. Delaune
Dallas
+1.214.969.5258
ndelaune@jonesday.com

Jennifer C. Everett
Washington
+1.202.879.5494
jeverett@jonesday.com

Olivier Haas
Paris
+33.1.56.59.38.84
ohaas@jonesday.com

Jörg Hladjk
Brussels
+32.2.645.15.30
jhladjk@jonesday.com

Samir C. Jain
Washington
+1.202.879.3848
sjain@jonesday.com

Jeffrey L. Kapp
Cleveland
+1.216.586.7230
jlkapp@jonesday.com

David E. Kopans
Columbus
+1.614.281.3895
dkopans@jonesday.com

Jonathan M. Linas
Chicago
+1.312.269.4245
jlinas@jonesday.com

Lisa M. Ropple
Boston
+1.617.449.6955
lropple@jonesday.com

Undine von Diemar
Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Special thanks to Clinton P. Oxford, an associate in the Washington Office, for his contributions in preparing this White Paper.