Arnold & Porter

June 10, 2020

COVID-19 Contact-Tracing Apps: What Privacy Law Will Apply?

Coronavirus: Multipractice Advisory

By Jami Mills Vibbert, Nancy L. Perkins, Gregory M. Louer, Javier Ortega, Erin Soyoung Park

To help our clients navigate the coronavirus (COVID-19) crisis, Arnold & Porter has established a Coronavirus Task Force covering a wide range of issues and challenges. Subscribe to our "Coronavirus (COVID-19)" mailing list to receive our latest client Advisories and register for upcoming webinars.

Introduction

Contact-tracing technology may have significant power to help combat the spread of COVID-19. If deployed through cell phone applications, the technology typically works by creating a digital record of each contact that each application user has with any other user. When one user becomes infected with the virus, the records provide a means for notifying all other app users with whom the infected user was in contact. As a general rule, the greater the number of individuals using the app and the greater the precision of the information collected, the greater the technology's power to help halt the virus' spread.

But with this benefit comes a corresponding intrusion on individual privacy. Is that appropriate? Is it legal?

Several non-US countries have deployed COVID-tracing technologies through government mandates, including South Korea, where a combination of tools such as GPS phone-tracking, credit card records, and surveillance video have reportedly facilitated rapid notices to individuals of their contacts with infected persons.[1] Other countries, including Japan, India, Israel, and Singapore, have adopted various other technologies to trace the movements of individuals who test positive for the virus and to identify others for quarantine.

Should the United States do the same? Should state governments mandate contact-tracing technologies? Should the government allow employers to do so? What information should be collected, used and shared, and what should be off-limits?

These questions may soon be addressed by Congress, where three different bills are pending, largely aimed at preventing contact-tracing technology from transgressing personal privacy boundaries. There are also contact-tracing bills pending in state legislatures, several of which we briefly highlight below. Whether many or any of these bills will become law during the current pandemic is unclear, but the issues they aim to address are of ongoing importance. COVID-19 will not be the last life-threatening pandemic, and technology will increasingly offer sophisticated options for tracing individuals. Legislators and administrators will need to make choices about how much personal information collection from particular populations is needed to serve public-health goals, and what that may mean for our protections of civil liberty and privacy.

The Federal Bills

In May 2020, two bills were introduced in Congress to address privacy rights with respect to contact tracing apps: the COVID-19 Consumer Data Protection Act of 2020 (S. 3663), sponsored by Roger Wicker (R-MS) and several other Republican Senators (the Republican Bill) and the other by a bicameral coalition of Democratic Senators and Representatives, including Senators Richard Blumenthal (D-CT) and Mark Warner (D-VA) and Representative Anna Eshoo (D-CA), the Public Health Emergency Privacy Act (S. 3749) (the Democratic Bill). On June 1, Senators Maria Cantwell (D-WA) and Bill

Cassidy (R-LA), supported by Senator Amy Klobuchar (D-MN), introduced a third bill: the Exposure Notification Privacy Act (S.3861) (the Bipartisan Bill). All three bills aim to establish the parameters for collection, use, and disclosure of information through contact-tracing technology. They are similar in many respects, including by granting enforcement authority to the Federal Trade Commission (FTC) in conjunction with state attorneys general, but they also have marked differences. For example, the Republican Bill would preempt state law on the same subject while the Democratic Bill would not, and the Democratic Bill includes a private right of action while the Republican Bill does not.

Who would be regulated?

All three bills have wide application. The Republican Bill covers, with limited exceptions, all entities subject to FTC jurisdiction as well as non-profits and common carriers subject to the Communications Act of 1934, to the extent they collect, process, or transfer "covered data" or determine the means and purposes for such collection, processing, or transfer. The Democratic Bill also embraces government actors, defining a "covered organization" (again with limited exceptions) as any public or private entity that collects, uses, or discloses "emergency health data" electronically or by wire or radio communication, or that develops or operates a website, web application, mobile application, mobile operating system feature, or smart device application "for the purpose of tracking, screening, monitoring, contact tracing, or mitigating, or otherwise responding to the COVID-19 public health emergency." The Bipartisan Bill would regulate "operators" of automated exposure notification systems, defined as any person or entity (with limited exceptions), other than a public health authority, that operates an automated exposure notification system. An "automated exposure notification service" includes a website, online service, online application, mobile application, or mobile operating system designed to be used or marketed for the purpose of digitally notifying, in an automated manner, an individual who may have become exposed to an infectious disease, the device of such individual, or a person or entity that reviews such disclosures.

Both the Republican Bill and the Democratic Bill, but not the Bipartisan Bill, exempt from regulation service providers of the covered entities, as well as entities regulated under the data privacy rules implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA) with respect to their use and disclosure of information that is "protected health information" (PHI) under HIPAA. (The Republican Bill might be read to exempt PHI even as handled by persons not regulated by HIPAA, but that is likely not its intent.) The Democratic Bill also exempts healthcare providers that are not HIPAA covered entities, persons engaged in *de minimis* collection or processing of data, persons acting in their individual capacity, and public health authorities. The Bipartisan Bill regulates service providers[2] only insofar as they must notify an operator or public health authority if they believe such operator or public health authority is not in compliance with the Bill's standards.

What information would be protected?

All three bills seek to limit data collection, use, and disclosure to what is necessary and proportionate for COVID-19 prevention purposes. The Republican and Democratic Bills define the relevant data in this context, with limited exemptions, as data that: (i) identifies, is linked to, or is reasonably linkable to an individual or device; (ii) is capable of determining the past or present actual physical location of an individual at a specific point in time; or (iii) identifies the past or present proximity of one individual to another. This data specifically includes personal health information that identifies or is reasonably linkable to individuals, including genetic information, biometric data, and treatment or diagnosis information. The Bipartisan Bill even more broadly defines "covered data" as any non-aggregated information collected, processed, or transferred in connection with an automated exposure notification service that is linked or reasonably linkable to any individual or a device that can be linked or is reasonably linkable to an individual.

The Democratic Bill limits covered data to data that concerns the public COVID-19 health emergency, but otherwise does not provide other exemptions. The Republican Bill expressly carves out nonidentifiable data, employee data, and other data already governed by federal law; specifically including: (i) aggregated data that is "not linked or reasonably linkable" to any individual; (ii) information that is collected, processed, or transferred solely for purposes related to an individual's professional activities; (iii) de-identified data; (iv) publicly available information; (v) education records subject to the Family Educational Rights and Privacy Act; and (vi) health information subject to the HIPAA privacy regulations. The Republican Bill also exempts "employee screening data" defined as data collected, processed, or transferred solely for purposes of determining whether employees, including vendors, visitors, interns, volunteers, and contractors, are permitted to enter the physical site of a covered entity.

What requirements would be imposed to protect privacy?

Transparency; Notices

Each of the bills would require covered entities to provide a privacy notice to users of the data-collection technology and to

make that notice available at the point of data collection in a clear and conspicuous manner. The notice would have to describe the manner and purpose of the covered entity's data collection and with whom, if anyone, the data collected will or might be shared. The Democratic Bill would additionally require covered entities to describe how an individual may exercise their rights under the Bill, and the Bipartisan Bill would require, in the event covered data were subject to a security breach, that "service providers" notify "operators" of the breach and that "operators" provide detailed breach notifications to the relevant individuals and the FTC.

Consent

Perhaps the most significant aspect of the federal bills is that all of them would require affirmative, express consent for the use, collection, or transfer of data through a contact-tracing technology. Opt-in consent requirements have the important benefit of confirming an active decision on the part of the consenter, but they almost uniformly result in less participation than when consent is *assumed* absent a choice to opt-out. In the contact-tracing context, the difference could be critical, as the core purpose and value of contact-tracing technology is to be as comprehensive as possible in identifying contacts between an infected individual and others. Obtaining opt-ins from 20% of a given population may simply not be sufficient to empower the technology to halt the spread of infection.

Use and Disclosure Limitations

All three bills also impose restrictions to prevent unwarranted use and disclosure of collected data. The Republican Bill would require covered entities to commit publicly not to collect, process, or transfer covered data other than to track the spread of COVID-19, measure compliance with COVID-19 related regulations and requirements, and to conduct contact-tracing. The Democratic Bill imposes a more generalized restriction by permitting the collection, use, and/or disclosure of covered data that is necessary, proportionate, and limited for a good-faith public health purpose and expressly prohibiting the collection, use, and/or disclosure of data for commercial purposes or in a manner resulting in unfair discrimination. Under the Bipartisan Bill, operators could not transfer covered data except: (1) to notify enrolled individuals of a potential exposure; (2) to inform a public health authority for public health purposes related to infectious disease; (3) to the operator's service provider; or (4) in connection with legal claims. And the Bipartisan Bill prohibits any form of discrimination against a person by any place of public accommodation based on either covered data collected or processed through an automated exposure notification service or an individual's decision to use or not use such a service.

With respect to any "actual, potential, or presumptive positive diagnosis of an infectious disease," operators could transfer only an "authorized diagnosis," which is "an actual, potential, or presumptive positive diagnosis of an infectious disease confirmed by a public health authority or a licensed health care provider," and then only as determined by the affected individual.

Reporting

Both the Republican and Democratic Bills require covered entities to provide periodic reports to the public on the number of individuals whose data have been collected, the categories of data collected, the purposes for which it has been used and disclosed, and the categories of entities to whom it has been transferred. The Democratic Bill would require such reporting only by covered entities that have collected data on at least 100,000 individuals, and only every 90 days. The Republican Bill would require reporting no later than 30 days after enactment and every 60 days thereafter, with no threshold minimum number of individuals whose data has been collected.

The Bipartisan Bill does not have a similar requirement, but would require that operators publish guidance for the public on the functionality of their automated exposure notification service, including any limitations related to the accuracy and reliability of the exposure risk and measures of effectiveness, including adoption rates. In addition, the Bipartisan Bill would authorize the Privacy and Civil Liberties Oversight Board (PCLOB) to review the government's collection, processing, and sharing of covered data in connection with a public health emergency and require the PCLOB to issue a report assessing the impact on privacy and civil liberties of government activities taken to respond to the COVID-19 public health emergency within one year of the Bill's enactment.

Data Minimization, Security and Deletion

All three bills require data minimization, reasonable mechanisms to provide data security, and data destruction. The Democratic Bill mandates that covered data be destroyed within 60 days of termination of the national public health emergency and within 30 days after an individual revokes consent. The Republican Bill obligates covered entities to destroy or de-identify covered data once the data is no longer used for a covered purpose or necessary for legal compliance.

The Bipartisan Bill would require operators to delete covered data of participating individuals within 30 days of receipt, on a rolling basis, or at such times as is consistent with local public health authority standards, as well as upon an individual's request. For security, the Bipartisan Bill would require operators to undertake security risk assessments, security breach prevention measures, and to implement corrective safeguards.

Enforcement

As noted, all three bills give the FTC and the State Attorneys General enforcement powers. The Democratic Bill also provides for a private cause of action with a sliding scale of statutory damages for negligent violations ($100-$1,000), and reckless, willful, or intentional violations ($500–$5,000).

Pre-emption

The Republican Bill expressly preempts state and local laws to the extent they are related to the collection, processing, or transferring of covered data for purposes of tracking the spread, signs, or symptoms of COVID-19, measuring compliance with COVID-19-related regulations, or conducting contact tracing for COVID-19 cases.

Neither the Democratic Bill nor the Bipartisan Bill would preempt state law.

State Efforts

Certain states have already been aggressive in seeking to use contact-tracing technology to help protect their residents from the virus. Both Utah and North Dakota have launched mobile applications that collect location data and provide symptom trackers. Alabama, South Carolina, and North Dakota have publicly announced their intentions to develop and adopt contact tracing apps for mobile devices. Given the significant possibility that Congress may fail to enact legislation to regulate such technologies, or may enact a non-preemptive bill, state legislators and administrators will likely play a prominent role in determining how privacy interests will be factored into the use of COVID-tracing technologies.

Within the past month, several state legislators have introduced bills addressing the issue.

In California, for example, bill AB 660 would prohibit any contractor providing contact-tracing services or technology to a state agency from sharing personal information obtained from contact-tracing applications or services, except as required to comply with a warrant/subpoena or to facilitate a public health provider's efforts to mitigate the spread of a communicable disease.

Another example is Minnesota bill H.F. 4665, which is targeted particularly at employers and would prohibit them from requiring employee use of digital contact tracing technology without consent. The bill would also prohibit employers from pre-installing digital contact tracing apps in an employer-issued personal device and from forcing employees to provide location information to determine contact with a contagious person, or using that information. And it would prohibit employers from imposing terms or conditions of employment based on an employee's refusal to install a contact-tracing app or to provide location information.

Similarly, New York bill S08327 would require an individual's affirmative consent before a contact-tracing app could be downloaded onto the individual's personal device. Before consenting, the individual would have to be provided with information about the app and the type of information the app collects. After consenting, the individual would have the right to revoke consent at any time.

Both of the latter bills provide for a private cause of action. Under the Minnesota bill, a plaintiff could recover up to three times the actual damages suffered due to a violation, punitive damages, reasonable costs and attorney's fees, and injunctive or other equitable relief. Under the New York bill, which specifically authorizes class actions, a court could award damages and/or declaratory and injunctive relief, as well as any other remedies available by law.

Future Steps

The use of contact-tracing technologies will almost certainly continue to fuel debate about the relative value of the technology and its intrusion on privacy. In the meantime, technology leaders will move forward with alternatives, such as the COVID-19 exposure notification technology and set of software tools that Apple and Google jointly developed and recently released.[3] Employers and businesses considering requiring the use of contact-tracing apps by their employees and customers will do well to follow closely legal developments surrounding any such mandates, as well as to focus on triggers for the application of existing laws, including not only certain privacy laws but also laws such as the Americans

With Disabilities Act and its state analogues.[4]

[1] *See* Washington Post, A 'travel log' of the times in South Korea: Mapping the movements of coronavirus carriers, March 13, 2020.

[2] A "service provider" under the Bipartisan Bill is "any person or entity, other than a platform operator, that processes or transfers covered data in the course of performing a service or function {for} a platform operator, an operator of an automated exposure notification service, or a public health authority but only to the extent that such processing or transfer is related to the performance of such service or function."

[3] *See* USA Today, Apple and Google release coronavirus contact tracing technology for public health mobile apps, May 20, 2020.

[4] For a discussion of the privacy-related responsibilities of employers in the COVID-19 context, see Employee Privacy with Respect to COVID-19.