ALERTS

Contact Tracing Applications: Privacy and Other Legal Considerations for Employers Under Existing Laws and Recent Senate Proposals (COVID-19)

June 4, 2020

As states have started to reopen their economies amidst the COVID-19 pandemic, employers are evaluating strategies that will allow their employees to return to work while protecting against a resurgence. Among those strategies is the use of technologies that track the movement of individuals for purposes of limiting the spread of COVID-19, in particular contact tracing applications.

The deployment of contact tracing applications by employers raises serious concerns about privacy rights, data security and other workplace legal protections. In response to these concerns, senators have introduced three bills aimed at protecting the privacy of individuals who use contact tracing applications or are subject to other COVID-19-related measures. On May 7, 2020, Republican Senators Roger Wicker, John Thune, Jerry Moran and Marsha Blackburn introduced the COVID-19 Consumer Data Protection Act of 2020 ("Wicker Bill"). On May 14, 2020, Democratic Senators Richard Blumenthal and Mark Warner introduced the Public Health Emergency Privacy Act ("Blumenthal Bill"). Finally, this week, on June 1, 2020, Democratic Senators Maria Cantwell and Amy Klobuchar and Republican Senator Bill Cassidy introduced the Exposure Notification Privacy Act ("Cantwell Bill" and collectively, the "Bills"). While all three Bills aim to protect the privacy of individuals during the nation's response to the COVID-19 pandemic, the scope, focus and rights provided by each have significant differences.

This *Alert* provides a brief background on contact tracing applications, a high-level overview of the requirements of the Bills, and a discussion of certain legal issues employers should bear in mind in evaluating the proper role of contact tracing applications in their reopening strategies.

Contact Tracing Applications

Contact tracing applications are smartphone-based applications that track users' interactions with other users to identify and notify potential exposed contacts.[1] While the design of these applications varies and is quickly evolving, most applications employ a smartphone's GPS or Bluetooth technology to track users' interactions. By tracking the whereabouts of users' devices and their proximity to each other, the contact tracing application is able to notify users of potential exposure to any other users who have self-reported as testing positive for COVID-19. Users who have been exposed might then be advised to contact their local health department to obtain guidance and resources, including the most current recommendations for assessing symptoms and preventing community spread.

While applications have been launched in Europe, Asia and Australia, it remains unclear exactly how contact tracing applications will work, and the extent to which they will be adopted, in the United States.[2] Programs may have differing accessibility for governments and employers and different structures for data centralization. One potential technology for use in the United States, which has received significant media coverage, is the technology under development through a partnership between Apple and Google.[3] An application using a version of this technology, launched in Switzerland on May 26, 2020,[4] follows an opt-in approach (where users voluntarily download and use the application) and uses Bluetooth technology to track users' interactions in order to identify exposure to COVID-19. The data is stored on individuals' devices and shared directly with public health authorities only; Apple and Google have said they would not have access to the information collected. Employers also would not have access to this information.

The Senate Bills

Who and What Data Do the Bills Cover?

The Bills aim to protect the privacy of Americans during the COVID-19 public health emergency, focusing on information collected by contact tracing applications. The Bills would regulate certain entities that collect or use personal health information, geolocation data, proximity data and other information generally used by contact tracing applications to track the spread of COVID-19. The most recent bill, the bipartisan Cantwell Bill, specifically targets services associated with the use of contact tracing applications and similar technologies used for the purpose of digitally notifying, in an automated manner, individuals who may have become exposed to an infectious disease.

What Do the Bills Require?

While the Wicker Bill, Blumenthal Bill and Cantwell Bill each have some distinct requirements, the Bills all generally require that regulated entities:

- Minimize the protected information collected to what is needed and take steps to protect the security of protected information;
- Obtain affirmative express consent from individuals to collect or use their protected information;
- Allow individuals to opt out of the collection of their protected information and/or revoke consent;
- Publish a privacy policy, disclosed to consumers prior to or at the point of data collection, that includes how their information will be handled and how long it will be retained; and
- Delete all personally identifiable information upon the user's request and when it is no longer being used for the public health emergency.

Notably, the Cantwell Bill, unlike the other Bills, would mandate that operators of contact tracing applications and similar technologies collaborate with a public health authority in the operation of such service. Another notable difference in the Cantwell Bill is its restriction against the use of aggregate data for any purpose other than for public health purposes. The Blumenthal Bill and Cantwell Bill would not place any restrictions on the use of aggregate data. Further, the Cantwell Bill, unlike the other Bills, would prohibit discrimination regarding access to public accommodations on the basis of an individual's choice to use or not use a contact tracing application.[5]

Employer Considerations

If any of these Bills were to pass, they may or may not create direct obligations for employers. For example:

- The Wicker Bill notably excludes from coverage employee screening data, defined as data collected, processed or transferred for the purposes of determining whether the individual is permitted to enter the employers' physical site of operation. The Wicker Bill would apply only to employers who collect, process or transfer protected information for a purpose that goes beyond employee screening.

- The Blumenthal Bill would apply more generally to organizations collecting, using or disclosing covered information and would not exempt employee screening data. Therefore, its requirements may apply directly to employers.

- More so than the other Bills, the Cantwell Bill targets the providers and notification services associated with the use of contact tracing applications and similar technologies. As such, the Cantwell Bill would also not apply to employers directly.

Whether or not any of these Bills moves forward, employers that are deciding whether to require (or encourage) employees to use contact tracing applications as a way to protect the workplace will need to consider the existing laws that may apply. While not an exhaustive discussion of all issues that may apply to contact tracing applications in the workplace, below is a discussion of some workplace protection, privacy and data security laws to consider.

Workplace Protections

Employers have a duty under the Occupational Safety and Health Act ("OSHA") to provide their employees with "a place of employment which [is] free from recognized hazards that are causing or likely to cause death or serious physical harm."[6] The U.S. Equal Employment Opportunity Commission ("EEOC") has issued guidance concerning workplace protections related to the COVID-19 pandemic, including related to the monitoring of COVID-19 symptoms and making medical inquiries that may impact employers' use of contact tracing applications. As employers consider requiring or encouraging use of contact tracing applications, the limitations and employee protections imposed by various workplace laws

will need to be considered. Striking a balance between protecting employees from exposure to COVID-19 and complying with other workplace rights and protections may prove to be delicate.

For example, under the Americans with Disabilities Act ("ADA"), employers may restrict employee access to the workplace, in a manner no more intrusive than necessary, where there is a "direct threat" to the health and safety of others. COVID-19 has been categorized by the EEOC as a "direct threat,"[7] which means that employers may exclude individuals with COVID-19 from the workplace if the threat posed by the employee cannot be eliminated or reduced by reasonable accommodation. Contact tracing applications have not been suggested as a reasonable accommodation, but arguably could be used as an inquiry to identify the existence of a direct threat to the workplace. Inquiries must be "job-related" and a "business necessity" to be permitted.[8] Permitted inquiries include employee body temperatures and other COVID-19 tests. Contact tracing applications may not, however, qualify as a business necessity, particularly because of the invasiveness of the location tracking in some of these applications and in cases where employees can and do work remotely. If they do qualify, any inquiries conducted must be administered in a non-discriminatory manner. Further, under the ADA, any records of health or medical data collected by employers through inquiries, including contact tracing applications, must be kept separately from the employees' personnel file.

Restrictions on employee workplace access may also implicate off-duty conduct laws, like those in New York and California, which prohibit employers from discriminating or taking adverse action against their employees for legal activities outside of work.

Employers may also be limited in their ability to require employees to use contact tracing applications based on the device ownership. While employers likely can mandate an employee use a contact tracing application on an employer-owned device, they may not be able to mandate use on employee-owned devices, including those used for Bring Your Own Device ("BYOD") programs. Employers should review their internal BYOD policies and ensure any contact tracing applications comply with these policies.

Privacy Laws

Existing privacy laws may also impact employers' adoption of contact tracing applications. For example, if an employer were to require employees to use a contact tracing application, and the data collected by the applications would be shared with the employer, the employer would need to comply with applicable state and federal laws that apply to the types of employee data collected. Many states, including Maine and California, have recently expanded their laws to expressly protect geolocation data as a form of personal information. Further, like the Bills, the California Consumer Privacy Act, which went into effect on Jan. 1, 2020, imposes robust disclosure, opt-out and deletion obligations on entities collecting personal information of this nature. A way to avoid such obligations could be to choose an application design where the employer does not have any access to the data collected, or only has access to anonymized data, and the public health authority and/or vendor engages in all communications with users.

While HIPAA does not apply to most employers,[9] all employers should be aware of communications to and from any contact tracing application they utilize, especially between applications and health plans or health care providers, to ensure that the technology complies with HIPAA. Employers should review contact tracing vendors' privacy policies to ensure they are HIPAA compliant.[10]

Data Security Laws

Employers who maintain or have access to data collected by contact tracing applications may also be subject to the increasing data security regulation at the state level. For example, under New York's Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act"), as of March 21, 2020, many companies[11] who possess personal information about New York residents are required to develop, implement and maintain "reasonable safeguards" to protect the "security, confidentiality and integrity" of the collected data. Employers will also need to be sure to comply with state data breach notification laws if there is a security incident involving personal information collected from contact tracing applications.

Other Considerations

An employer's use of contact tracing applications may trigger other important considerations. For example, an employer should ensure that the new technologies and the collection of personal data comply with its

internal data security and privacy policies. Similarly, if an employer is engaging third-party vendors to provide contact tracing applications, the selection and engagement of those vendors should comply with the employer's vendor policies, particularly if the new technology vendors will also have access to or store any protected information. That would include rigorous vetting of the vendor's privacy and data security policies.

Conclusion

It is unclear at this point whether any of the Bills will gain momentum and move forward in Congress. Given the significant privacy concerns, contact tracing applications and similar technologies may in fact prove to be fertile ground for the first federal privacy legislation in more than a decade. Regardless, the appropriate role of contact tracing applications is an issue many employers will need to confront as businesses reopen. In deploying any sort of application, employers will need to understand the technology's design and be cognizant of the privacy, data security and workplace protection laws that such designs implicate. The potential benefits of the applications in terms of safety and preventing workplace spread will need to be carefully weighed against the risks these laws present. Employers will also want to reassess the available designs and the steps taken to comply with such laws on a periodic basis given the high potential for changes in the technological and legal landscapes.

Authored by Edward H. Sadtler, John C. Garces and Melissa J. Sandak.

If you have any questions concerning this *Alert*, please contact your attorney at Schulte Roth & Zabel or one of the authors.

---

[1] Contact tracing applications are intended to supplement manual contact tracing efforts already conducted by public health authorities.

[2] A few states, including North Dakota, South Dakota and Utah, have already launched voluntary contact tracing applications, but adoption rates have been very low. *See* Elliot Setzer, "Contact Tracing Apps in the United States," *Lawfare*, May 6, 2020, available here. Applications in the United States may also be very different from those currently in use in Europe, Asia and Australia. *See* Miles Johnson et al., "Europe Split Over Approach to Virus Contact Tracing Apps," *Financial Times*, May 1, 2020, available here; Yasheng Huang et al., "How Digital Contact Tracing Slowed Covid-19 in East Asia," *Harvard Business Review* , April 15, 2020,

available here; Josh Taylor, "Covidsafe App: How Australia's Coronavirus Contact Tracing App Works, What it Does, Downloads and Problems," *The Guardian*, May 14 2020, available here.

[3] "Privacy Preserving Contact Tracing," *Apple*, available here.

[4] Leo Kelion, "Coronavirus: First Google/Apple-Based Contact-Tracing App Launched," *BBC News*, May 26, 2020, available here.

[5] In doing so, the Cantwell Bill potentially restricts the use of contact tracing applications by a broad range of business and other organizations, such as hotels, restaurants and schools. Specifically, the Bill makes it unlawful for "any person or entity to segregate, discriminate against, or otherwise make unavailable to an individual or class of individuals the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation (as such term is defined in section 301 of the Americans With Disabilities Act of 1990 (42 U.S.C. 12181)), based on covered data collected or processed through an automated exposure notification service or an individual's choice to use or not use an automated exposure notification service."

[6] Section 5(a)(1) of the Occupational Safety and Health Act of 1970.

[7] *See* "Pandemic Preparedness in the Workplace and the Americans with Disabilities Act," *U.S. Equal Employment Opportunity Commission* (last updated March 21, 2020), available here.

[8] *See* 42 U.S.C. § 12112 & 29 C.F.R. § 1630.14.

[9] HIPAA's Privacy Rule applies to disclosures made by employees, volunteers and other members of a covered entity's and/or business associate's workforce. A covered entity is a health plan, health care clearinghouse or health care provider who conducts certain health care transactions electronically (e.g., transmitting health care claims to a health plan). "Business associates" are generally individuals or entities that perform functions on behalf of, or provide services to, a covered entity. Business associates also include subcontractors that create, receive, maintain or transmit protected health information ("PHI") on behalf of another business associate.

[10] HIPAA is carved out of, but not preempted by, the Wicker Bill and Blumenthal Bill. Therefore, entities that are regulated by HIPAA likely would not be regulated by the Wicker Bill and Blumenthal Bill.

[11] The SHIELD Act's data security requirements may not apply to all employers. For example, fund managers are likely outside such requirements. *See* "Data Security: Update for Private Fund Managers — NY SHIELD Act," *SRZ Alert*, March 18, 2020, available here.

This is a fast-moving topic and the information contained in this Alert is current as of the date it was published.

Practices

CYBERSECURITY AND DATA PRIVACY

EMPLOYMENT AND EMPLOYEE BENEFITS

Attachments

Download Alert