The Computer & Internet Lawyer

Volume 37 ▲ Number 7 ▲ JULY/AUGUST 2020

Ronald L. Johnston, Arnold & Porter, LLP, Editor-in-Chief

From Contact Tracing to Virtual Temperature Taking: Privacy Considerations for Employers

By Steven G. Stransky

As the COVID-19 pandemic declines and businesses start their "reopening" process, many employers are seeking to implement novel health and safety technologies to protect their employees, contractors and other personnel from the disease. Two such measures, contact tracing and virtual temperature taking, have recently garnered significant attention because of both their potential to mitigate a resurgence of COVID-19 and the privacy concerns related to their use and implementation.

The United States does not have a single, comprehensive data privacy law regulating these technologies and activities, and federal and state laws governing the use of protected health information and similar medical data only apply in a narrow context (for instance, healthcare providers and company health plans) and often do not extend to these areas. In response, a group of U.S. senators recently drafted and introduced the "COVID-19 Consumer Data Protection Act"[1] to bring a new level of uniformity and clarity to this area. Unfortunately, until such a bill is enacted into law, employers will continue to be subject to a patchwork of federal and state data privacy and cybersecurity requirements, including in the employment context.

This article addresses key data privacy principles and laws that employers should consider prior to executing any contact tracing, virtual temperature taking, or any other new COVID-19 related health and safety program involving the collection, retention, and use of personal information or other data.

The Tech Tools: Contact Tracing and Temperature Taking

The phrase "contact tracing" often refers to the process of identifying individuals with whom a person diagnosed with, or suspected of having, COVID-19 may have contacted in a certain defined timeframe and manner (for example, within six feet for 20 minutes). In short, the purpose of contact tracing is to identify those individuals who are at risk of developing COVID-19 because of their proximity to COVID-19

Steven G. Stransky is a partner in Thompson Hine's Privacy & Cybersecurity practice, primarily focusing on advising clients on complex national and international privacy and information security issues. Prior to joining Thompson Hine, Mr. Stransky spent a total of 10 years serving in the federal government, including with the U.S. Department of Homeland Security and the National Security Council. He may be contacted at *steve.stransky@thompsonhine.com*.

patients and interrupt the onward transmission of the disease.

In recent months, technology companies, universities, and research institutes have been developing digital tools and technologies to assist healthcare organizations, governments, and employers implement more effective and efficient contact tracing. For example, several governments[2] and private sector companies[3] have developed applications ("apps") that can be installed on cell phones that use short-range Bluetooth signals to maintain an encrypted record of other applications (installed on third-party devices) with which they have been in close proximity for a defined time period. If a user of the app is diagnosed with COVID-19, the third parties who are on record of being within this proximity are notified (via the app) of the potential COVID-19 exposure. Some governments and organizations are developing similar, but more intrusive, app-based technologies that use a combination of GPS, WiFi, cellular, Bluetooth, and internet protocol addresses to triangulate the user's precise location,[4] which then can assist in identifying and broadcasting physical locations (such as schools, grocery stores, and places of worship) where individuals with COVID-19 have spent time and where there may be potential outbreaks.

Still, other companies[5] are developing digital "employee badges" that enable employers to monitor their employees' movements, locations, and proximity to other personnel at a particular work site or location in order to better analyze people and areas of health and safety concern.

Separately, since the outbreak of COVID-19 many employers have begun screening their employees for fevers in order to address warnings from the CDC that a fever, as well as a cough and shortness of breath, may be symptoms of COVID-19. Yet, manually taking the temperature of every employee in any given day can be time consuming and places health officials and other employees at risk of exposure.

Thus, in response, employers have sought to streamline this process by implementing temperature screening kiosks and cameras[6] to quickly screen large number of employees while avoiding human contact. Generally, the kiosks employ infrared technology to measure the body temperature of individuals within its narrow radius and the thermal cameras use similar technology to measure the temperature of individuals at a greater distance and in larger numbers.

Data Privacy Considerations for Employers

The United States has multiple federal and state laws regulating data privacy, and non-compliance can expose employers to significant regulatory penalties and civil litigation. Yet, domestic data protection laws often vary by the type of personal data collected, the business sector in which the data is used, and the method in which the data is obtained by an organization.

Accordingly, prior to implementing any of the health and safety technologies described herein, it is important for employers to understand how these tools operate and the types of data they collect in order to implement and maintain the appropriate policies and procedures. At a high level, employers should scrutinize whether any of the following data privacy principles are applicable in their jurisdiction, and if not, whether they should incorporate them, as a matter of policy, into their business operations.

Confidentiality and Data Security

At the core of all data privacy norms and laws is that personal information is to remain confidential and should only be processed and disclosed in accordance with the applicable individual's instructions and guidance. In order for employers to maintain such confidentiality, they must implement and maintain technical, physical, and administrative controls to preserve the authorized restrictions governing access to, and disclosure of, the personal information in their custody and control. In the United States, there are several federal and state laws governing these confidentiality and security principles.

For example, the Americans with Disabilities Act ("ADA") generally prohibits an employer from making "disability-related inquiries" and requiring "medical examinations" of employees, and measuring an employee's body temperature is generally considered a medical examination for ADA purposes. Yet, because of the severity of COVID-19, the federal government has authorized employers to undertake such activities in order to protect their workforce and premises. The medical and health-related data derived from these temperature screenings are subject to the ADA's confidentiality requirements, and must be stored separately from the employee's personnel file (such as in an employee's medical file) and is also subject to stringent access and disclosure controls. This medical information may include an employee's self-disclosure that he or she has, or may have, COVID-19, or the data derived from the technologies implemented to discover symptoms of the same.

There are several data protection laws at the state level that require organizations to implement strict data security measures to protect the personal information derived from their health and safety technologies and programs.

For example, pursuant to Oregon Rev. Stat. § 646A.622(1), covered businesses are required to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of personal information, including safeguards that protect the personal information when the covered entity or vendor disposes of the personal information."

Importantly, the law defines "personal information" to include an individual's name in combination with, among other data elements, any information about his or her medical history, physical condition, or about a health care professional's medical diagnosis or treatment of the consumer.

At Section 646A.622(2)(d), the law further provides that a business can satisfy such "reasonable safeguards" if it implements the technical, physical, and administrative controls defined therein, which include, but are not limited to, the following:

- Designating an employee to coordinate its security program;
- Routinely seeking to identify data privacy and security risks;
- Training its workforce on its data security program;
- Assessing and addressing risks and vulnerabilities in network and software design applicable to its computing infrastructure; and
- Monitoring, detecting, preventing and responding to cyberattacks and intrusions to, or failures in, its networks and systems.

Accordingly, employers should assess their confidentiality and data security policies and programs prior to collecting any new employee data as part of their COVID-19 response program to ensure they satisfy applicable legal requirements. Although several other state laws require organizations to implement "reasonable" security measures to safeguard personal information in their custody or control, only a few (for example, Alabama, Massachusetts, New York) provide the same level of granularity as set forth in the Oregon law, and organizations may consider looking to these statutes for guidance as they implement their own information security measures.

Notice and Consent

A fundamental data privacy principle is that individuals should be given notice of, and consent to, when and how their personal data is collected, processed, and used. These privacy principles are codified in several domestic laws, many of which are applicable in the employee-employer relationship and may be implicated in the event a business seeks to implement COVID-19 technologies.

A fundamental data privacy principle is that individuals should be given notice of, and consent to, when and how their personal data is collected, processed, and used.

For example, pursuant to Conn. Gen. Stat. Ann. § 31-48d(b)(1), any employer who engages "electronic monitoring" is required to "give prior written notice to all employees who may be affected, informing them of the types of monitoring which may occur" by "conspicuous[ly]" posting a written "notice concerning the types of electronic monitoring which the employer may engage in." The law defines "electronic monitoring" very broadly and aligns with several of the contact tracing apps and digital employee badges on the market today.

In addition, the California Consumer Privacy Act of 2018 ("CCPA") requires covered businesses that collect "personal information" to "inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used."[7]

It is important to the note that the CCPA defines the term "consumer" to essentially mean any California residents, which would include employees, contractors, and other personnel; it further defines the term "personal information" to mean any information or data "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" and may include geolocation data, electronic and thermal information, and health data that "contain[s] identifying information."[8]

Although the CCPA exempts employee or "HR" data from much of its scope, this notice requirement is still applicable to California-based employees. Accordingly, businesses should consider whether they have to make formal disclosures to their employees before implementing any health and safety program that involves the collection and use of personal information.

Pursuant to Illinois law, businesses that collect certain types of biometric data from individuals, including employees, are required to:

- Publicly disclose a retention schedule and guidelines for permanently destroying the data;
- Inform the individual in writing about the collection, storage and retention of, and the specific purpose for collecting, the data; and
- Obtain the individual's written release prior to collecting the data.[9]

In the context of employment, a "written release" includes a release executed by an employee as a condition of employment, such as a standard employment agreement. Given that advanced thermal cameras and kiosks have the capability to collect an individual's biometric data in addition to his or her temperature, employers should thoroughly examine (prior to their use) whether the consent requirements in the Illinois law, or in any other data protection framework, are applicable to their business operations.

Third-Party Support and Management

Another important aspect of data protection, and one that has gained additional attention in recent years because of the enactment of the CCPA and other foreign data protection laws, relates to third-party service providers. In short, organizations that collect personal data are only as secure and reliable as the service providers that they use to physically store, transmit, and dispose of, such information on their behalf.

Accordingly, organizations should (or may be legally required to) regulate their service provider relationships with specific contractual clauses. In the United States, federal law mandates these third-party contracting obligations in certain business sectors (for instance, business associate agreements in healthcare), and state laws impose such obligations in much broader settings.

For instance, pursuant to Rhode Island Gen. Laws § 11-49.3-2(b), organizations that disclose or share "personal information about a Rhode Island resident to a nonaffiliated third party shall require by written contract that the third party implement and maintain reasonable security procedures and practices . . . to protect the personal information from unauthorized access, use, modification, destruction, or disclosure." The law notes that the "reasonableness" of the security procedures may depend upon the size and scope of the organization, the nature of the personal information at issue, and the purpose for which the information was collected. It is important to note that the term "personal information" includes medical information regarding an individual's medical history, physical condition, or medical treatment or diagnosis by a health care professional or provider, which may be collected as part of the employer's COVID-19 health and safety response program.

Similarly, the Oregon law referenced above[10] provides that in order to satisfy certain security standards set forth therein, organizations need to select service providers that are "capable of maintaining appropriate safeguards and practices, and requiring the service providers by contract to maintain the safeguards and practices."

In addition, Alabama, California, Maryland, Nebraska, and New York impose similar third-party contracting requirements, although all may not be relevant in the employer or COVID-19 response contexts.

Yet, even if these legal requirements are not applicable to an organization, it should still consider demanding that any third-party service provider that retains or processes data related to its employees, including health and medical information and contact tracing data, contractually agree to certain standards and criteria. For example, these contractual clauses should address circumstances wherein a government entity requests access to such data to facilitate their own public health goals or for other reasons (such as criminal or regulatory investigations). Similarly, these contracts should require the service provider warrant that it will:

- Not use the data for its own purposes;
- Store such data in the United States or any other applicable jurisdiction; and
- Certify that it will dispose of the data through certain defined means (for example, cryptographic erase) and timeframes (such as every 30 days, upon request, upon termination of the agreement).

In addition, organizations should require these third-party service providers to furnish security attestations or other documentary evidence describing their data security program and commit to providing assistance to data rights requests or data breaches in a mutually agreed upon manner.

Last, organizations may consider requiring their service providers retain their own cyber and privacy insurance to mitigate risks arising from a security incident pertaining to their employee data.

Conclusion

In addition to the other employment and labor, regulatory, and safety issues that organizations must address when implementing a health and safety program, they must also consider a broad range of privacy and

cybersecurity principles and laws. The new technologies being employed to facilitate the response to COVID-19 assist in bringing these data protection issues to the forefront, especially when such technologies involve highly intrusive data collection elements, such as physical tracking and health screening.

Notes

1. U.S. Senate Committee on Commerce, Science, and Transportation, "Committee Leaders Introduce Data Privacy Bill," May 6, 2020, *available at https://www.commerce.senate.gov/2020/5/committee-leaders-introduce-data-privacy-bill*.
2. *See, e.g., https://www.tracetogether.gov.sg/*.
3. *See, e.g., https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/*.
4. *See, e.g., https://www.healthytogether.io/legal/privacy*.
5. *See, e.g., https://www.npr.org/2020/05/08/852896051/your-boss-may-soon-track-you-at-work-for-coronavirus-safety?utm_medium=RSS&utm_campaign=news*.
6. *See, e.g., https://www.wired.com/story/can-an-infrared-camera-detect-a-fever/*.
7. Cal. Civ. Code § 1798.100(b).
8. Cal. Civ. Code § 1798.140.
9. 740 ILCS § 14/1-25.
10. Oregon Rev. Stat. § 646A.622(d).

Copyright © 2020 CCH Incorporated. All Rights Reserved.
Reprinted from *The Computer & Internet Lawyer*, July/August 2020, Volume 37, Number 7, pages 3–6, with permission from Wolters Kluwer, New York, NY, 1-800-638-8437, www.WoltersKluwerLR.com