A Path To Privacy Protections For Employee Contact Tracing

By **Kelly Belnick and Kenneth Jones** (May 12, 2020)

Kelly Belnick

Kenneth Jones

In the absence of a national coordinated effort to reopen America's economy and restart its workforce, private employers are investigating technological solutions to limit occupational exposure to COVID-19.

Unlike public health officials and local and state leaders who are considering contact tracing applications dependent on individual, voluntary buy-in, private employers are evaluating the use and legality of conditioning return to work on consent to monitor. This inevitably raises workplace privacy concerns.

In the context of contact tracing, the current pandemic is a stark reminder that this country lacks national comprehensive data privacy protection and that state-level regulation is sparse. Confronted with a deficit of guidance, employers will inevitably rely upon ad hoc approaches to instituting workplace contact tracing.

In the current climate, it is understandable and justifiable that companies are seeking to implement mandatory monitoring measures against coronavirus spread inside offices and throughout the workplace. A safe work environment includes a healthy workforce, which, in turn, maximizes productivity, minimizes costs, and limits the risk of a future shutdown.

Now is an ideal time to consider what nationwide adoption of substantive data protection could look like. In the absence of bright-line rules, there is inevitably confusion resulting in increased reliance on the courts to step in and determine what constitutes workplace invasion of privacy. The EU's General Data Protection Regulation and the recently enacted California Consumer Privacy Act provide a good overview of the key principles federal or state legislation should address.[1]

Employer electronic data collection is not new. It is standard practice for businesses to maintain automated logs that collect information on all data interactions and communications. This is especially true in the legal industry.

Consider the exponential rise in electronic discovery over the last decade, which is (at its most basic) a collection of a company's electronically stored information for use as evidence. Automated data collection permits detailed tracking of who is accessing client-sensitive data without interrupting workflow and enables firms, when required, to certify that data is not misused or impermissibly accessed.

Employee monitoring also informs management decisions regarding job performance, internal inefficiency, accountability and potential security threats. New-hire onboarding typically includes acknowledgement of permissible technology use, including bring-your-own-device guidelines and confidentiality agreements.

Tracking employee coronavirus exposure is just an extension of what is already done. Contact tracing, however, relies upon collection of personal health information, which implicates unique privacy considerations.

The emerging employee contact tracing app options collect data through either Bluetooth, GPS or Wi-Fi technology and will require download directly onto a user's phone. Some apps are question-oriented, asking people for personal information such as health status or recent travel; others automatically track employee movements; and a third group combines the two approaches.

Regardless of the foundational technology, enabling location service functionality, at all times, is necessary. With any downloaded app there is also a risk of inadvertent data collection, such as information gathered through cookies and other installed tracking technologies — a concern about which employers must be mindful.

The obvious difficulty with workplace deployment of these apps is gaining employee participation and trust. Employers should be prepared to educate employees about the type of information the app will collect, how the employer will use that information, who in the organization can access that information, when the collected information will be deleted, if app developers can share and sell what is collected and the rights employees will have to their information.

For example, can an employee access what is collected or ask that it be deleted? It may be helpful for employers to articulate the benefits of using contact tracing apps in the workplace (i.e., limiting workplace exposure, identifying individuals who may need to self-quarantine, keeping the workplace open by isolating effected individuals, etc.)

The data privacy standards and expectations articulated within the GDPR and the CCPA naturally require employers to address the issues outlined above. Under the GDPR the processing of all personal data is protected, whether by automated means or some other form of electronic filing.

Article 5 of the GDPR outlines eight data protection principles that all actors must implement: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.[2] The GDPR generally prohibits the processing of personal data that concerns health, unless the subject has provided "freely given, specific, informed and unambiguous consent" through affirmative action. Further, it is permissible to collect personal health data if it is necessary for "the purposes of preventive or occupational medicine."

The GDPR requires that when an individual's personal data is processed, the subject has a right to access the data and be provided with the following information: why the data was processed; the categories of personal data collected; the recipients of the personal data or to whom the data will be disclosed; and where possible the period for which the personal data will be stored. Where it is not possible to provide the storage time frame, the processor must provide the criteria used to determine the storage period.

Prior to any data collection that involves a specific privacy risk, such as disclosure of personal health information, an impact assessment is conducted that, among other criteria, examines the "risks to the rights and freedoms of data subjects." Violations of the GDPR can (and in some instances must) result in the assessment of monetary fines. Although not all fines are publicly reported, since the GDPR's passage fines have ranged from €118 (or $128) to €204.6 million (or $221.9 million).[3]

The GDPR also mandates governance of data location storage. Articles 44 through 50, relate to transfer of data to third parties or individual organizations. If entities use cloud storage services such as Amazon Web Services, they will need to identify where data is stored,

when it is transferred and the transfer dates. All of the actions required under these areas of the GDPR are only possible through creation of system logs that automatically track and file this information.

Within the U.S., the CCPA went into effect on Jan. 1 — although enforcement will not begin until July 1. After its original passage in 2018, the CCPA quickly became the go-to framework for other states looking to adopt comprehensive consumer data privacy protection. Similar to the GDPR, the CCPA addresses individual rights (which includes households) and business obligations to assure those rights, although its reach is much narrower in scope than the GDPR.

The law takes the position that personal information is owned by consumers and consumers have general rights with regard to their personal information:

- Right of access;
- Right of rectification;
- Right of deletion;
- Right of restriction;
- Right of portability;
- Right of opt-out;
- Right against automated decision-making; and
- A private right of action for a security breach.

The CCPA applies to for-profit businesses that collect and control California residents' personal information, do business in the state of California, and meet one of the following three requirements: have annual gross revenues in excess of $25 million; or receive or disclose the personal information of 50,000 or more California residents, households or devices on an annual basis; or derive 50% or more of their annual revenues from selling California's residents' personal information.

Unlike the GDPR the CCPA would not necessarily apply to all employer/employee relationships. It does not impose minimum data security requirements or require consumer opt-in for the sale or use of personal information. The CCPA does, however, establish a right of action for certain data breaches that result from a business's duty to implement and maintain reasonable security practices. Notably, "reasonably security practices" are not defined.

As employees return to work and employers seek to ensure a safe and sustainable work environment, a tangled web of regulatory obstacles (or the lack thereof) lies ahead. Decision makers must balance the competing interests of protecting data privacy with the need to stop the spread of coronavirus and its potentially devastating impact on people's lives and employer day-to-day operations.

Companies need to proactively consider whether or not instituting contact tracing applications is a viable option for their organization. Where the need exists, workplace contact tracing should be implemented reasonably; in a manner that minimizes privacy concerns and maximizes employee endorsement. The GDPR, CCPA and preexisting technology-based procedures, provide valuable insights on how to pave a path forward.

Kelly A. Belnick is an associate and Kenneth E. Jones is chief technologist at Tanenbaum

Keale LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Since its passage in 2018, the CCPA is quickly becoming the model framework for other states, however, only two other states (Nevada and Maine) had enacted comprehensive consumer data protection privacy laws as of April 16, 2020. See International Association of Privacy Professionals (IAPP), U.S. State Comprehensive Law Policy Comparison available at https://iapp.org/resources/article/state-comparison-table/ [last accessed on April 29, 2020].

[2] The full text of the GDPR is publicly available online at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679 [last accessed April 28, 2020].

[3] GDPR Enforcement Tracker available online at https://www.enforcementtracker.com/? [last accessed on April 28, 2020].