Bloomberg Law®

INSIGHT: Contact Tracing Apps Can Trigger Workplace, Privacy Concerns

Edward H. Sadtler, Mark E. Brossman, John C. Garces, and Ryan P. Knox, Schulte Roth & Zabel

INSIGHT: Contact Tracing Apps Can Trigger Workplace, Privacy Concerns

Contributed By Edward H. Sadtler, Mark E. Brossman, John C. Garces, and Ryan P. Knox, Schulte Roth & Zabel

Striking a balance between protecting employees from exposure to Covid-19 and complying with workplace protection and privacy laws may prove to be delicate for employers considering using contact tracing applications, Schulte Roth & Zabel LLP attorneys say. They also note three Senate bills to watch.

Employers are evaluating strategies that will allow their employees to return to work while protecting against a Covid-19 resurgence. Among those is the use of technologies that track the movement of individuals to limit the spread of the virus, such as contact tracing applications.

Contact tracing applications are smartphone-based applications that, by tracking the proximity of users to each other, are able to notify users of potential exposure to other users who have self-reported as testing positive for Covid-19.

ADA, EEOC, Personal Devices Considerations

The deployment of contact tracing applications by employers raises serious concerns about workplace legal protections. Striking a balance between protecting employees from exposure to Covid-19 and complying with workplace protection and privacy laws 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 Equal Employment Opportunity Commission (EEOC) as a "direct threat," 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 may 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.

Inquiries expressly permitted under current EEOC guidance include employee body temperatures and other Covid-19 tests. Contact tracing applications may not, however, qualify as a business necessity, particularly due to the potential invasiveness of location tracking.

Employers may also be limited in their ability to require employees to use contact tracing

applications based on the device ownership and scope of tracking. While employers likely can mandate an employee use a contact tracing application on an employer-owned device, they may not be able to on employee- owned devices, including those used for bring-your-own-device programs.

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.

Privacy Considerations

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, the California Consumer Privacy Act, which went into effect on Jan. 1, imposes robust disclosure, opt-out, and deletion obligations on entities collecting personal information.

A way to limit such obligations would be to choose an application design that does not permit the employer access to the data collected, or access only to anonymized data, and relies on public health authorities and/or vendors to communicate with users.

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, certain companies 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.

Three Senate Bills

In addition to existing laws which may apply to contact tracing applications, employers should be aware of three privacy bills introduced in the Senate, the most recent of which (and the only bi-partisan proposal) being the Exposure Notification Privacy Act introduced by Democratic Sens. Maria Cantwell (Wash.) and Amy Klobuchar (Minn.) and Republican Sen. Bill Cassidy (La.) on June 1 (the Cantwell Bill).

While the Cantwell Bill and two other bills introduced in May have certain distinct requirements, they all generally regulate the collection and use of personal health, geolocation, proximity and other data collected and used by contact tracing applications by requiring operators to obtain express consent from users, minimize the information collected, publish a privacy policy and delete personal information if requested or when it is no longer in use.

If any of the bills were to pass, they would need to be added to the list of considerations for employers evaluating contact tracing applications.

The appropriate role of contact tracing applications in the workplace is an issue many businesses will need to confront as they reopen. In deploying any sort of application, employers will need to understand the technology's design and be cognizant of the workplace protection and privacy 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.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Author Information

Edward H. Sadtler is a Schulte Roth & Zabel LLP partner and head of the firm's Intellectual Property, Sourcing & Technology Group.

Mark E. Brossman is a Schulte Roth & Zabel LLP partner and co-head of the firm's Employment & Employee Benefits Group.

John C. Garces is special counsel at Schulte Roth & Zable LLP and practices in the firm's Intellectual Property, Sourcing and Technology Group.

Ryan P. Knox is an associate at Schulte Roth & Zable LLP and practices in the firm's Employment & Employee Benefits Group.