Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Road Map For A Cautious Approach To Contact Tracing

By **Boris Segalis and Jonathan Newmark** (April 30, 2020, 5:49 PM EDT)

It has become increasingly clear that a combination of COVID-19 testing and use of geolocation technologies for contact tracing will be essential for the nation to get back to life and work. With this realization came outcry that contact tracing is a leap to the surveillance society that would lead to significant deterioration of civil liberties.

While these concerns are justified in principle, they do not reflect the reality that privacy concerns are top of mind for state governments and private enterprise working together to develop contact-tracing technology.

That privacy is central to these efforts should not be a surprise. Legitimate businesses have been treading carefully on privacy for years, having learned that failing to handle sensitive personal information in a fair and transparent manner — especially in high-profile applications — can destroy businesses. At the same time, state governments traditionally have legislated to protect consumer privacy and are even more cautious now.

Privacy professionals who are advising governments and businesses have significant experience and tools to help develop and implement privacy-focused contact tracing, and there are a number of practical steps they can take to protect consumers.

Location Tracking for Contact Tracing

Contact tracing refers to tracking an individual's exposure to another person who may have the virus. Digital contact tracing relies on precise geolocation tracking and retention. When a user installs a contact-tracing app on a mobile device, they are prompted to enable the existing location services on that device, thereby permitting the app — solely at the user's direction — to continuously record his or her location.

Typically, contact tracing will require collection of both GPS and Bluetooth data to log whenever the user comes within close proximity of another individual. The use of GPS and Bluetooth facilitates analysis of the distance between the users and duration of the close contact, to flag only the types of contacts that — according to the Centers for Disease Control and Prevention — are likely to result in virus transmission.

This location data will remain in the hands of the app developers for a limited duration, only to be

leveraged should an individual user test positive for COVID-19.

At that moment, the app would notify all users with whom the infected individual recently had contact to inform them of potential exposure to the virus and encourage them to get tested. The alert may include general timestamp and locations, but otherwise would not provide the name or any contact information about the individual whose positive COVID-19 test triggered the alert.

The app — the business, state or a combination of the two, depending on the partnership — acts as a trusted third party that has everyone's location information, but discloses only in the instance of contact.

States' and Businesses' Focus on Privacy, Transparency, Fairness

Over the past half a dozen years, the U.S. experienced a slew of dramatic privacy controversies that reverberated throughout the world, ranging from the Edward Snowden revelations to the 2016 election interference. These controversies have slowly turned the tide on the American consumers' acceptance of personal data privacy as a key concern and the society's understanding of the power of personal data.[1]

The concerns about civil liberties that are being raised today in response to the development of contact tracing are positive signs of this new-found awareness. At the same time, many businesses and state governments have been hyper-cognizant of the risks of mishandling data for years, as a result of sustained focus on privacy by powerful forces that may not be apparent to consumers.

In the U.S., companies that have jumped in to develop contract tracing applications have in large part already built their business models on leveraging personal information. These companies value their reputation and know first-hand that failing to handle personal data in a fair and transparent way exposes them to significant financial and reputational risks; they also have now for years faced external pressures to follow privacy laws and best practices from investors, plaintiffs bar, regulators and consumer advocacy organizations.

These companies have also been great students of the privacy enforcement environment — both by regulators and in the court of public opinion. As a result, they know that the higher the sensitivity of the data they process and the higher the profile of the project, the likelier the companies are to face scrutiny and the more important it is to follow privacy best practices.

These companies also recognize that fairness and transparency in privacy practices is good for consumer trust and for their business.

State governments may be less fluent in privacy, which generally has made them very cautious in approaching privacy in the context of contact tracing. Historically, states that have legislative privacy have been pro consumer.

In addition to the California Consumer Privacy Act and Illinois Biometric Information Privacy Act, public utility regulations in Colorado and Minnesota, among other states, gave control of personal energy usage data to consumers, requiring them to opt in for utilities to share the data with third parties.

Other states have put in place measures prohibiting use of consumer reports in the employment context, prohibiting employers from asking candidates for social media credentials, requiring companies

to secure personal information, limiting the use and sharing of consumer financial information, and many other privacy protective measures. There is little reason or evidence to believe that — with COVID-19 contact tracing — states will seek to reverse this pro-privacy trend.

In implementing contact tracing, states are focused on privacy-by-design and data minimization, even as they recognize that mass participation in these programs is key to their effectiveness. States are approaching contact tracing with a caution that is driven not only by their inherent conservatism, but recognition that they need widespread adoption for an effective contact-tracing program, which has only solidified a commitment to privacy needed to induce a cautious public to participate in containment efforts at scale.

The incentives that states and private business stakeholders have in protecting consumer privacy should give comfort to advocates that there are entrenched economic and political forces that drive a pro-privacy approach to contact tracing.

With states leading on contact tracing, there is also concern that federal authorities may view the rich location data as another source of information, including in criminal investigations.

While the federal government's privacy record is not stellar, there is little reason to believe that contact-tracing data — specifically — will open a new front in federal government's access to personal information. The federal government already has access to location data, subject to the same due process protections that should apply to contact-tracing information.

Practical Steps for Privacy-Conscious Contact Tracing

From the privacy risk perspective, contact tracing is a high-profile effort to collect, use and share sensitive data. There are well-known tools in the privacy toolbox for this type of a project, built on years of dating platforms, pregnancy apps, patient assistance portals, privacy chats, people search engines, sales of personal data in bankruptcies, regulatory investigations, cybersecurity and privacy public relations battles and other technologies and issues that have prepared privacy professionals for this moment.

These experiences suggest that key principles for rolling out contact-tracing technologies are:

Transparency and Clarity in Privacy Practices

- Define the mission: Start the privacy notice with a concise paragraph to describe the nature and purpose of the product or service to set the context for consumers' expectations for how the product or service will collect, use and share their data.

- Provide a short, bulleted privacy notice that articulates your privacy practices clearly, factually and without use of jargon.

- Recognize that data that identifies a device is personal and treat it as such.

- Include only what you need in the privacy notice; this is not the time to reserve any rights with respect to the collection, use, retention or disclosure of consumer data that your product will not and should not need.

- Avoid long, nuanced disclosures that consumers will either refuse to read or fail to understand; this is also the time to avoid nuance and hedging for the sake of transparency.

- Include in-time notices for any uses or disclosures of personal information that consumers would not expect in the context of contract tracing.

- Partner with marketing professionals to develop proper assurances and messaging to engender consumer confidence and promote widespread adoption.

- Consider appointing a privacy advisory board for the contact tracing product or service.

Minimization of Data Collection, Use and Retention

- Commit private and public actors to use consumer information solely for the purposes of contact tracing and related COVID-19 containment efforts.

- Leave the bulk of data collection and processing with legitimate private players.

- Anonymize or delete location data on a rolling basis as a matter of course, mitigating against use of the personal data for purposes unrelated to contact tracing in any meaningful way.

- Do consider potential future uses of the data the product or service collects, including use for public interest and research purposes that consumers will likely view as acceptable; recognize that — to be effective — public interest sharing may need to be narrow but not rely on opt-in consent.

Sensible Data Sharing

- Share only within the reasonable expectations of consumers.

- Take special care to only share information with third-party service providers needed to provide the services to support contact tracing.

- Be sure to vet service providers' information security and data retention practices; seek to rely on established, existing service provider relationships.

- Avoid sharing data for advertising and other commercial purposes unrelated to contact tracing.

- Provide government partners with only the minimum amount of data needed to facilitate pandemic-response efforts.

Online Tracking and Advertising

- Carefully consider use of cookies and tracking technologies; consider retaining only true service provider analytics providers that commit to not use device data for their own purposes.

- In using advertising technologies to promote the products and services, take special care to understand the terms of the advertising partners to make sure not to engage with partners that

will use the data for other purposes. If in doubt, contact the potential partners even if the typical engagement is via click wrap terms.

- Do not include commercial advertising on contact tracing websites or in mobile apps.

- Minimize email response tracking to what is necessary to provide the product and service; verify that tracking service providers will not use tracking data for their own purposes.

Communications

- Limit electronic communications to what is necessary to provide the product or service.

- Rely on in-app notifications over email or text.

- Obtain users' opt-in consent for texting; limit texting to what is reasonably necessary.

Data Security

- Assume that contact-tracing information is sensitive and apply security measures that are appropriate for sensitive information.

- Limit access to the contact-tracing data to key employees and service providers, and monitor access.

- Use trusted third-party information security offerings, such as end-point security products and secure cloud storage; encrypt data in transit and at rest.

- Minimize retention of personal data, and pseudonymize data when feasible.

This list of privacy and security measures stakeholders is not exhaustive, but it offers the direction for approaching privacy for contact tracing from which the stakeholders can extrapolate other controls. The list reflects a direction that we expect to be acceptable to consumers, consumer advocacy groups and regulators, without detracting from the efficacy of contact tracing.

Hidden Risks to Civil Liberties

It is fair that the focus of the commentary on contract tracing has been on the privacy implications of the technology. Equally valid, however, is the debate on the effect on other civil liberties of allowing hype to prevent us from using technology to help us get back to normal.

The risks of inaction are real. We should learn at least two lessons from the tragedy of 9/11, the COVID-19 pandemic, and Russian election interference and many others.

First, we — the general, informed population — typically don't know what existential risks to our society are imminent.

Second, when these tragedies materialize, there is no scary music to warn us that something is coming; by the time we recognize the malaise, it's already happening to us or behind us, as was the case with the 2016 presidential election. There is no warning. And this lack of warning often dulls the society's

awareness of these not easily foreseeable risks, which are nevertheless ever-present.

Professor Laurence Tribe of Harvard Law School cautions us to beware of sacrificing our privacy values for the short-term gain of reopening the country through the use of contact-tracing technologies.[2] What he fails to consider in the context of civil liberties, however, is what is on the other side of a prolonged shutdown that destroys the U.S. consumer economy, leaves millions of people out of work, exacerbates political, social and racial divisions in the society, and consolidates power in leaders with authoritarian tendencies.

When we ignore the structural weaknesses of our society, it may be worth considering how many steps we are from turning into the imaginary Gilead in "The Handmaid's Tale." What other civil liberties are we willing to sacrifice for our privacy rights to remain intact?

We are living in an increasingly digital world, one that has developed technology capable of processing information in unprecedented ways. It is an invaluable asset that data-processing technology can also help control the spread of COVID-19. Our responsibility is to help deploy contact tracing in ways that respect the society's laws and norms, including in protecting consumer privacy.

Boris Segalis is a partner and vice chair of the cyber/data/privacy practice at Cooley LLP.

Jonathan Newmark is an associate at the firm.

[1] In an unprecedented move, even the federal government has stepped in to regulate foreign investment in data companies. https://www.law.com/newyorklawjournal/2020/02/28/risk-of-foreign-access-to-u-s-data-spur-government-to-act-but-economic-concerns-loom/.

[2] "Digital coronavirus data tracing would barter away American liberties," available at https://amp.usatoday.com/amp/3000576001.