Benesch

May 7, 2020

BIWEEKLY ALERT

From Benesch's **Data Privacy Defense & Response Team**

Contact Tracing Armies Combat the Spread of COVID-19, but Create "Novel" Data Privacy Concerns

Imagine waking up to an email, or receiving a text message, that alerts you to the news that you have or may have been exposed to someone who tested positive for COVID-19. No, this is not a hoax and, no, your email and/or phone number has not been hacked. You have likely just encountered a member of the "contact tracing armies" that are being formed across the United States and elsewhere who, with government backing, seek to combat the spread of the novel coronavirus.

The idea behind "contact tracing" is simple: Find out who the known coronavirus patients are, find out who they have been in contact with during the last two weeks, find out who *those people* have been in contact with in the last two weeks, and so on until you have fully traced who has or may have the disease.

Different contact tracing "armies" are deploying different combat strategies. New York's system, for example, is being developed in partnership with Johns Hopkins University and former New York City Mayor Michael Bloomberg. Its "army" will be formed by those with healthcare backgrounds who rely on and utilize known-patient inputs to trace the spread of COVID-19 (i.e., after a person tests positive, they will be interviewed by a "soldier" about their contacts from the previous 14 days, and then those contacts will be contacted and interviewed).

By contrast, San Francisco's "army" is made up of volunteer recruits—including librarians, social workers, medical students, and even attorneys—who are being trained though partnerships with the University of California's San Francisco and Los Angeles campuses. Illinois (which has over 60,000 confirmed cases) is planning to invest $80 million in developing its own "army." In the United Kingdom, the National Health Service will be conducting a trial run of a smartphone tracing app. The app utilizes Bluetooth signals to detect when two phones come close to each other, and logs that data. Anyone who has or

(continued)

Please note that this information is current as of the date of this client bulletin, based on the available data. However, because COVID-19's status and updates related to the same are ongoing, we recommend real-time review of guidance distributed by CDC and local officials.

For more information, please contact one of the following members of Benesch's Data Privacy Defense & Response Team:

MICHAEL D. STOVSKY
Partner and Chair, Innovations, Information Technology & Intellectual Property (3iP) Practice Group; Chair, Data Security & Privacy Team; Chair, Blockchain & Smart Contracts Team
T: 216.363.4626 | mstovsky@beneschlaw.com

J. ERIK CONNOLLY
Partner and Vice Chair, Litigation Practice Group; Co-Chair, Securities Litigation Practice Group
T: 312.624.6348 | econnolly@beneschlaw.com

ALISON K. EVANS
Associate, 3iP Practice Group; Data Security & Privacy Team
T: 216.363.4168 | aevans@beneschlaw.com

WHITNEY M. JOHNSON
Associate, Litigation Practice Group
T: 628.600.2239 | wjohnson@beneschlaw.com

KATE WATSON MOSS
Associate, Litigation Practice Group
T: 312.624.6329 | kwatsonmoss@beneschlaw.com

KATHERINE A. SMITH
Associate, 3iP Practice Group
T: 216.363.4488 | ksmith@beneschlaw.com

Contact Tracing Armies Combat the Spread of COVID-19, but Create "Novel" Data Privacy Concerns

(continued from previous page)

reports symptoms of coronavirus can then notify the app, which then notifies those who were in physical proximity to that individual and who may be at risk. Both Google and Apple are developing similar apps.

While there is no debate over the need to fight against the spread of coronavirus, these and other contact tracing efforts have numerous data privacy implications:

- **How is the data stored?** Is the contact tracing data being stored on a centralized sever, or does it remain with the individual "army" members (who may or may not be working remotely over unsecured Wi-Fi networks)? Is the data anonymized or pseudonymized, or would that defeat the purpose of tracing?
- **Are there limitations on how the data can be used?** Once a record is made that someone has been or may have been exposed to a COVID-19-positive patient, what happens to that person's PII and PHI? Does it become part of his/her medical record? Can it be shared with third parties, including insurance companies or United States Immigration and Customs Enforcement?
- **Are there data destruction policies in place?** How long is the tracing data stored? How long should it be stored? Can those who have been contacted request that their PII be removed? If the data is stored on "army" members' personal laptops, are there data destruction policies in place so that those devices (and the extremely sensitive data they contain) do not inadvertently end up on eBay?

The answers to these questions will have serious impacts on data privacy laws and potential future litigation.

Feeling attacked? Curious about how contact tracing efforts can affect your business? Now is the time to take action. We invite you to participate in a complimentary 30-minute call with Benesch's data protection specialists. Benesch would be happy to provide you with our insight and guidance on these and other data privacy and protection best practices—including litigation avoidance strategies. We look forward to working with you to keep your data safe and secure.