Data Privacy and Cybersecurity

Senators Introduce the Exposure Notification Privacy Act

By: David P. Saunders and Allison N. Glover

On June 1, 2020, Senators Maria Cantwell (D-Wash.), Bill Cassidy (R-LA), and Amy Klobuchar (D-Minn.) introduced the Exposure Notification Privacy Act (the ENPA), to establish privacy requirements for operators of infectious disease exposure notification services. Unlike the other, federal privacy proposals related to COVID-19 tracking and tracing, the ENPA is broader; applying to any infectious disease, and ENPA would not expire once the COVID-19 public health emergency ends.

Who is Covered by ENPA?

The ENPA would apply to any person or entity that operates an automated exposure notification service related to the tracking and tracing of an infectious disease. An automated exposure notification service, in layman terms, is a service that would notify an individual if they had been in proximity of someone who subsequently tested positive for an infectious disease. These services are more commonly referred to as tracking or tracing services. The ENPA would not, however, apply to any public health authority.

What Data is Covered?

Under ENPA, covered data includes any information that is linked or reasonably linkable to any individual or device linked or reasonable linkable to an individual and collected, processed, or transferred in connection with an automated exposure notification service. Covered data does not include aggregated data.

What Would ENPA Require?

Obtain opt-in consent for participation. The ENPA requires that operators of automated exposure notification services receive affirmative and informed consent from users for the collection of their information through the service. Consent cannot be implied, but must be demonstrated by some affirmative act of the user (*e.g.,* clicking a checkbox).

Provide an opt-out mechanism. Automated exposure notification service operators would be required to allow users to opt-out of the service at any time and for any reason.

Collaboration with Public Health Authority. ENPA prohibits any automated exposure notification service from operating *unless* it is operated by or in collaboration with a public health authority. A public health authority is defined as an agency or government authority that is responsible for public health matters as part of its office mandate, or a person or entity acting under a grant of authority from or contract with such public agency. The requirement that an exposure notification service collaborate with a public health authority is aimed, according to the ENPA sponsors, at giving the public a reason to trust the service. However, requiring that *all* such services sponsor with a public health authority will likely result in fewer services being available, further stretch the resources of public health authorities, and overall decrease the ultimate utility of notification services.

Diagnosis information. ENPA would prohibit a service from notifying users that may have been exposed to an infectious disease unless (1) the diagnosis has been confirmed by a public health

authority and (2) the user who was diagnosed consents to the use of the diagnosis for purposes of the service. As a practical matter, these requirements would seem to appear to dampen the real-time effectiveness of many of the tracking and tracing programs that are being used at present to tackle COVID-19.

Data deletion and recurring deletion. Potentially further reducing the efficacy of tracking and tracing services, the ENPA has a deletion requirement. Specifically, a covered entity, upon request of an individual, must delete or allow the individual to delete all of their covered data. The covered entity must also delete the covered data of participating individual within 30 days of receipt of such covered data, on a rolling basis, or at other times as required by public health authority requirements. This deletion obligation would flow through to service providers.

Data collection and use restrictions. Under ENPA, a covered entity would be required to only collect the minimum amount of data necessary and would also be prohibited from collecting or using data for any commercial purpose. The only exception is that data collected through the services governed by ENPA could be used for public health research purposes.

Privacy policy. ENPA would require that covered entities and platform operators account for the collection and sharing of information in their privacy policy. The required disclosures include (1) the identity and the contact information for the person or entity's representative for privacy and covered data security inquiries; (2) each category of covered data the person or entity collects and the limited allowable processing purposes for which such covered data is collected; (3) whether the person or entity transfers covered data and, if so, a detailed description of the data transferred, the purpose of the transfer, and the identity of the recipient of the transfer; (4) a description of the person or entity's covered data minimization and retention policies; (5) how an individual can exercise the individual rights; (6) a description of the person or entity's covered data security policies; and (7) the effective date of the privacy policy.

Data security. Under ENPA, a covered entity would be required to establish, implement, and maintain data security practices to protect the confidentiality, integrity, availability, and accessibility of covered data. The specific requirements include (1) assessing any reasonably foreseeable risks to and vulnerabilities in each system maintained by the entity processing or transferring covered data; (2) taking preventative and corrective action to mitigate any risks or vulnerabilities to covered data identified by the entity; and (3) maintaining plans for responding to security incidents involving covered data. If there is a security breach, ENPA would require a covered entity to notify the FTC as well as the individual whose data was compromised. The covered entity would also have to require its service providers to provide notice of any security breach of covered data immediately upon discovery.

Nondiscrimination and freedom of movement. ENPA would prohibit covered entities from segregating, discriminating against, or otherwise making unavailable to individuals the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation, as defined by the Americans with Disabilities Act, based on covered data collected or processed through an automated exposure notification service or an individual's choice to use or not use an automated exposure notification service.

How Will ENPA Be Enforced?

ENPA would be enforced by the FTC and State Attorneys General to pursue violations. A violation of ENPA would be treated as a violation under the FTC Act regarding unfair and deceptive act or practices. State Attorneys General would also have power to bring a civil action, if there is a violation of ENPA or reason to believe that ENPA is being violated. There is no private right of action under the ENPA, although the ENPA preserves all state causes of action.

What about State Preemption?

ENPA would not preempt any state law. That the ENPA would leave each of the states room to create their own tracking and tracing laws likely will serve to only create additional impediments to the roll out of useful and effective tracking and tracing services.

Conscious of the human, operational and financial strain that coronavirus is placing on businesses and organizations worldwide, Jenner & Block has assembled a multi-disciplinary Task Force to support clients as they navigate the legal and strategic challenges of the COVID-19 / Coronavirus situation.

For additional information and materials, please visit our COVID-19 / Coronavirus Resource Center.

Click here to visit our COVID-19 / Coronavirus Resource Center

Contact Us

David P. Saunders

dsaunders@jenner.com | Download V-Card

Allison N. Glover

aglover@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower

Chair

dbitkower@jenner.com

Download V-Card

David P. Saunders

Co-chair

dsaunders@jenner.com

Download V-Card