FLASTER GREENBERG
Attorneys at Law | A Professional Corporation

Exposure Notification Privacy Act: What Companies Should Expect If Passed

Legal Alert

June 10, 2020

Krishna Jani & Donna Urban

On Monday, June 1, 2020, federal lawmakers proposed the Exposure Notification Privacy Act ("ENPA"), a piece of bipartisan legislation aimed at protecting consumer privacy and promoting public health in the development of exposure notification technologies as a way to combat the spread of COVID-19. The legislation makes participation in commercial online exposure notification systems voluntary and grants consumers control over their personal data. Moreover, the Act would limit the types of data that may be collected, as well as how that data can be used.

This legislation was introduced on the heels of competing privacy bills proposed by Republicans and Democrats respectively—the "COVID-19 Consumer Data Protect Act of 2020" and the "Public Health Emergency Privacy Act."

What differentiates the EPNA from the other proposals?

- This Act would prohibit any automated exposure notification service not operated by, or in collaboration with, a public health authority. The Act would require that automated exposure notification services allow only submission of medically authorized diagnoses of infectious diseases. Unlike the other proposals, this Act would not prohibit data retention for public health research purposes.
- Moreover, this Act would cover only operators of "automated exposure notification services," defined as any website or mobile application designed for use or marketing to digitally notify an individual who may have become exposed to an infectious disease, whereas the previously proposed Acts would cover both symptom tracking and other apps.
- This Act also encompasses a broader definition of personal data than the previous bills. For example, the new proposal covers all data linked or "reasonably linkable" to any individual or device that is collected, processed, or transferred in connection with an automated exposure notification service. The CDPA, by contrast, specifically defines covered data as health information, geological data, and proximity data.
- Unlike the other two proposals, the EPNA would require the Privacy and Civil Liberties Oversight Board to issue a report within one year after enactment that assesses "the impact on privacy and civil liberties of Government activities in response to the public health emergency related to" COVID-19. It would also require the Board to make recommendations for how the Government should mitigate threats posed by the current pandemic and similar emergencies in the future.

How is this Act similar to the others?

Like the Democratic and Republican proposals, many of the bipartisan proposal's key requirements are consistent with existing federal or state privacy requirements or norms, including public reporting, posting a clear and conspicuous privacy policy, and maintaining reasonable data security policies and practices.

- As with both the Republican and Democratic proposals, the EPNA would grant enforcement power in the form of litigation authority to both the Federal Trade Commission and state Attorneys General.
- This Act would also require affirmative express consent to enroll individuals in automated exposure notification services.
- This Act would also expressly prohibit workplace discrimination against people who decline to utilize contact-tracing technology, similar to the Public Health Emergency Privacy Act.

Takeaways

This is the third in a series of COVID-related federal data privacy bills meant to tackle the difficulties posed by collecting data to combat the spread of infectious disease with the public's increasing concerns with the privacy and cybersecurity of their data.

We will continue to monitor this legislation and provide updates accordingly.

If you have any questions, please feel free to reach out to Donna Urban, Krishna Jani, or any member of Flaster Greenberg's Telecommunications or Privacy & Data Security Groups.