
The Public Health Emergency Act: What Companies Should Expect If Passed

Legal Alert

May 27, 2020

Krishna Jani & Donna Urban

On May 14, 2020, Democratic Congresspersons introduced the Public Health Emergency Privacy Act (“PHEPA”) as a counterproposal to the Republican Senate’s recently-proposed privacy bill, COVID-19 Consumer Data Protection Act of 2020 (CDPA). The Act would protect personal data collected in connection with COVID-19 from being used for non-public health purposes, and provides for enforcement if companies fail to comply.

How is this different from the other proposed federal data privacy bill?

Similar to the CDPA, the PHEPA would put temporary rules in place regarding the collection, use, and disclosure of emergency health data used to help combat the spread of the coronavirus. Both bills would only apply during the course of the Public Health Emergency as declared by the Secretary of Health and Human Services. Both bills contain rules to protect personal data collected from being used for non-public health purposes. Moreover, both the PHEPA and the CDPA require that the organization collecting the data obtain “express consent” prior to collection and allow users to opt-out of data collection altogether.

Specifically, the PHEPA would mandate that all data collected through contact tracing apps would be limited to public health use and prohibit the use of health data for any discriminatory, unrelated, or intrusive purposes, such as commercial advertising or efforts to bar access to employment, insurance, and the like. Companies collecting this data would also have to delete it within sixty (60) days of the end of the current public health emergency.

However, unlike the CDPA, the PHEPA provides the Federal Trade Commission (“FTC”) with resources and enforcement tools to carry out this data protection. In fact, the PHEPA specifically provides for FTC enforcement under Unfair or Deceptive Trade Practices and allows the FTC to promulgate rules with a notice and comment period. Moreover, the FTC would have the exclusive authority to commence or defend, and supervise the litigation of, any action for a violation of the PHEPA, and to handle any resulting appeals. Significantly, the PHEPA would allow for a private right of action by any individual alleging a violation and it bars the use of pre-dispute arbitration agreements.

All in all, this bill is intended to help individuals trust contact-tracing apps and proximity-tracing programs during this pandemic.

What are the implications?

Continued

Google and Apple released their contact tracing API (application programming interface) this month, and companies have already started to use it to develop contact-tracing apps. For this reason, it is crucial that those on both sides of the aisle reach an agreement as to which bill should be passed.

If the PHEPA passes, companies subject to this new law would have to comply with the specific data collection mechanisms, and limitations, in the new law. Furthermore, the PHEPA could serve as the basis of a federal comprehensive privacy law.

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.