Data Privacy and Cybersecurity

Democrats Unveil the Public Health Emergency Privacy Act

By: David P. Saunders and Allison N. Glover

On May 14, 2020, Democratic Senators Mark Warner (D-Va.) and Richard Blumenthal (D-Conn.) along with Representatives Anna Eshoo (D-Calif.), Jan Schakowsky (D-Ill.), and Suzan DelBene (D-Wash.) unveiled a COVID-19 privacy bill, the Public Health Emergency Privacy Act (the PHEPA). Both the PHEPA and the Republican-led COVID-19 Consumer Data Protection Act of 2020 (the CDPA), which we discussed in our May 4 and May 11, 2020 client alerts, aim to put data privacy and cybersecurity regulations around the collection of personal data related to tracking and tracing the outbreak of COVID-19 in the United States. The PHEPA and CDPA are similar in many ways – attempting to regulate the collection of personal data related to COVID-19 remedial efforts – and therefore below, we highlight what we see as the key differences between the two Acts. These differences, in many ways, are similar to the differences that we have seen in the broader privacy debate in Washington, DC.

Scope of the PHEPA and CDPA

The PHEPA is broader than the CDPA. In addition to proposing regulations around the collection of data related to COVID-19 for tracking and tracing purposes, the PHEPA also includes a voting rights provision that would prohibit the use of covered data (discussed below) to deny or interfere with an individual's right to vote. Similarly, the PHEPA has a civil rights reporting provision, requiring the Department of Health and Human Services (HHS) Secretary, in consultation with the US Commission on Civil Rights, to produce regular reports examining the civil rights impact of the collection, use and disclosure of covered data.

Scope of Covered Data

The PHPEA is also broader than the CDPA with respect to what information would be regulated under the proposed legislation. Whereas the CDPA only applies to certain personal information collected for three specific purposes (tracking spread, contact tracing and compliance with state at home orders), the way the PHPEA is drafted, it could be read to reach "routine" data collection, not typically associated with remedial efforts surrounding COVID-19. Specifically, the definition of "emergency health data" – which is the information regulated under the PHPEA – is defined as information linked or reasonably linkable to "an individual, device, including data inferred from or derived about the individual or device from other collected data" and "that concerns the public COVID-19 health emergency." The definition continues, however, that "*such* data" (emphasis added) includes a host of data that one would ordinarily *not* associate with COVID-19 from genetic information to biometric information. Based on its express terms, within the scope of regulated data would be, for example, demographic or even contact information when collected in conjunction with biometrics or other health-related information. Thus, hypothetically, an entity that is already collecting biometrics and contact information from an individual could suddenly find itself regulated under PHPEA even though the collection activities have been ongoing since well before the COVID-19 pandemic and have nothing to do with it. In short, there seems to be a definitional issue in the PHPEA, which makes it far broader than was likely anticipated by its authors. This issue likely will need to be addressed going forward.

Scope of Covered Entities

The PHEPA also applies to a wider range of entities than the CDPA. Whereas the CDPA would only apply to FTC regulated entities, common carriers and non-profits that collect, process or transfer regulated data, the PHEPA would also apply to public entities such as the federal and state governments.

Prohibited Uses of Covered Data

Unlike the CDPA, the PHPEA expressly prohibits using regulated data for commercial advertising, including e-commerce or training of machine learning algorithms related to advertising; offers of employment, finance, credit, insurance, housing or education opportunities; or discrimination in any place of public accommodation. On its face, this prohibition may make sense. However, given the definitional issue discussed above regarding the breadth of regulated data under PHPEA, this prohibition could chill what might otherwise be permitted commercial activity.

Service Provider Carve Out in Definition of Covered Entities

Both the CDPA and PHPEA expressly exclude service providers from the definition of covered entity. However, they have different definitions of what constitutes a service provider. Under the CDPA, a service provider is an entity that processes or transfers regulated data on behalf of another. The PHPEA includes a broader definition, including not just entities that process or transfer regulated data, but also reaching those who develop or operate a website, web application, mobile application or smart device application for the purpose of tracking, screening, monitoring, contact tracing or mitigation, or otherwise responding to the COVID-19 public health emergency.

Differences in Public Reporting

Both the PHPEA and the CDPA would require covered entities to publish recurring public reports. Under the CDPA, required reporting would be every 30 days after enactment, and not less frequently than every 60 days thereafter. The required reporting would include the aggregate number of individuals from whom the covered entity collected, processed or transferred covered data; the categories of data collected, processed or transferred by the company; the specific purpose for each of the categories of covered data collected, processed or transferred; and to whom the data was transferred.

The PHPEA, on the other hand, would limit the number of entities making reports to those which collect, use or disclose emergency health data of at least 100,000 individuals. That subset of covered entities would be required to publish a public report every 90 days that would include the aggregate number of individuals whose covered data was collected, used or disclosed; the categories of covered data collected, used or disclosed; the purposes for each such category of covered data was collected, used or disclosed; and the categories of third parties to whom it was disclosed.

Enforcement and Private Right of Action

What is certain to be a major sticking point that will have to be overcome if we are to have any federal regulation of personal information related to COVID-19 remedial efforts is the proposed enforcement mechanism. While the CDPA and PHPEA both contemplate actions by the FTC and states against covered entities that violate the proposed laws, the PHPEA also expressly includes a private right of action. The proposed private right of action would include tiered remedies depending on whether the violation was negligent ($100 - $1,000 per violation), or reckless, willful or intentional ($500 - $5,000 per violation). The court could also award reasonable fees, litigation costs and any other relief that the court determines appropriate. The inclusion of a private right of action in PHPEA is potentially a trap for many companies given the definitional issue discussed above. That is, many more companies could find themselves the defendant in a PHPEA action for no other reason than they did not realize that their routine collection of data had somehow become regulated under a COVID-19 privacy bill.

Invalidation of Pre-Dispute Arbitration Agreements or Pre-Dispute Joint Action Waivers

Demonstrating the breadth of the PHPEA, it, unlike the CDPA, also addresses arbitration and class action waivers. Specifically, the CDPA would invalidate pre-dispute arbitration agreements or pre-dispute joint action waivers that would otherwise by applicable to a dispute arising under the PHPEA.

State Preemption

The other major sticking point in any effort to get a federal privacy bill has always been what level of preemption the bill would have over state laws. The dueling COVID-19 privacy bills are no different. The CDPA includes complete state preemption. On the other hand, the PHPEA does not preempt *any* state laws. This is an obvious issue that will require some compromise if a federal privacy bill is to pass. Practically speaking, it is difficult to envision a federal privacy bill that does not include *any* preemption whatsoever. If the federal government were to pass such a bill, it would leave companies open to 50 additional regulatory regimes in addition to the federal level and would likely result in *more* confusion and *less* compliance among companies than a bill that would create a uniform set of regulations. Indeed, one of the reasons that businesses have been advocating for a federal privacy bill more generally is so that they can operate in a world of a *single* regulatory regime as opposed to the contradictory and inconsistent privacy regime that currently exists in the United States.

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