Data Privacy and Cybersecurity

COVID-19 Consumer Data Protection Act 2020

By: David P. Saunders and Allison N. Glover

On April 30, 2020, Senator Roger Wicker (R- Miss.), along with co-sponsors, Senators John Thune (R-S.C.), Jerry Moran (R-Kan.), and Marsha Blackburn (R-Tenn.), announced the COVID-19 Consumer Data Protection Act of 2020 (Act). The Act's purpose is to protect the privacy of consumers' personal health information, proximity data, and geolocation data during the COVID-19 public health emergency. The Act is meant to be temporary and would expire on the last day of the COVID-19 public health emergency as determined by the Secretary of Health and Human Services.

Who is Covered by The Act?

The Act would apply to any entity regulated by the FTC – and also common carriers and non-profit entities – that collect, process or transfer covered data. The definition of "collect" in the Act is broad, reaching not just what one would commonly think of as "collection" but also "buying, renting, gathering, accessing or otherwise acquiring any covered data."

What Data Is Covered?

Under the Act, covered data would include:

- **Personal health information**, which covers genetic information plus diagnostic and treatment details that connect to an individual. There are, however, exclusions for data already regulated under the Federal Educational Rights and Privacy Act of 1974 (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA), plus aggregated, de-identified and public data.

- **Precise geolocation**, which is information capable of "determining with reasonable specificity" the past or present "actual physical location" of an individual. Again, however, this category excludes aggregated, de-identified and public data.

- **Proximity data**, which is information that identifies who was close to what other person.

When Would the Act Apply?

Obviously, companies are already collecting information that fall into the "covered data" categories described below, and they are likely doing so for a wide variety of reasons. This Act, however, would govern the collection of "Covered Data" any time it is being used for one of three, express purposes:

(i) tracking the spread, signs or symptoms of COVID-19;

(ii) measuring compliance with social distancing or other COVID-related requirements; or

(iii) contact tracing

What Would the Act Require?

Obtain opt-in consent prior to collection. The Act adopts an opt-in regime. Unless the collection of covered data for a covered purposes is required by law, a covered entity must first inform an individual of the collection and then obtain *affirmative* consent from the individual for the collection. Unlike in other opt-in rubrics, the Act expressly provides that no passage of time, delay or failure to act after being informed can be inferred to be a form of affirmative consent.

Provide an opt-out mechanism. Unsurprisingly, covered entities not only have to obtain consent initially, but the Act would also require covered entities to then provide a mechanism whereby individuals can withdraw their consent.

Updated privacy policies. Covered entities will have 14 days from the effective date of the Act to publish revised privacy policies. These include not only the fact and purpose of the collection, but also a disclosure related to the ability of individuals to consent or opt-out, a disclosure as to whether the covered data is shared with third parties, a description of data retention practices related to the covered data, and a general description of data security measures at the covered entity.

Public reporting. In addition to revising privacy policies, the Act would require covered entities to publish, every 30 days, a report disclosing: 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.

Data minimization. The Act would require covered entities to delete the covered data it collects for a covered purpose when it is no longer needed for the covered purpose. Covered entities must also not collect any more covered data than is necessary to accomplish the covered purpose.

Data security. A mainstay in most privacy legislation, the Act would also require that covered entities adopt reasonable administrative, technical and physical safeguards to protect the covered data.

How Will the Act Be Enforced?

The Act would be enforced by the FTC. A violation under the Act would be treated as a violation under the FTC Act regarding unfair and deceptive acts or practices. States Attorneys General would also have power to bring a civil action, if the residents have been or are being adversely affected by engagement with the company and if the company is not subject to the enforcement authority of the FTC.

What about State Preemption?

One of the primary concerns with any federal privacy bill is that it will leave too much to the states to regulate, not actually improving on the existing patchwork of privacy legislation in this country. That does not appear to be an issue with the Act. It contains a broad preemption clause that would prevent states from adopting, maintaining, enforcing, or continuing to enforce any law, regulation, rule, requirement, or standard related to the collection, processing, or transfer of covered data used for the purposes outlined in the Act.

Contact Us

David P. Saunders

dsaunders@jenner.com | Download V-Card

Allison N. Glover

aglover@jenner.com | Download V-Card

Meet Our Team