May 4, 2020

Pandemic Privacy: Republican Senators Announce Plan to Introduce *COVID-19 Consumer Data Protection Act of 2020*

A group of Republican Senators have introduced a new privacy bill that would impose strict privacy obligations on contact-tracing apps operated by entities not subject to HIPAA. Most notably, the *COVID-19 Consumer Data Protection Act of 2020* would obligate such entities to obtain express affirmative consent from individual consumers before using their geolocation, proximity, or personal health data.

Significantly, geolocation, proximity or personal health information collected for other purposes, including for marketing or other for-profit uses would not be regulated. This focus on certain uses of data could give rise to commercial speech concerns because it potentially could be seen as viewpoint discrimination. Separate issues could arise from the bill's broad attempt at federal preemption, which may raise federalism issues and prove to be sticking points in the bill's progression.

Main Requirements

The COVID-19 Consumer Data Protection Act of 2020 establishes potentially onerous obligations for companies attempting to fight the coronavirus using personal data. The bill's provisions on consent, transparency, data deletion, data minimization and security are reminiscent of sweeping privacy regimes such as the EU's General Data Protection Regulation and the California Consumer Privacy Act. Significantly, the COVID-19 Consumer Data Protection Act would require those entities subject to this Act (also confusingly defined as "covered entities" as discussed below):

1. Provide prior notice to individuals of the reasons for collecting, processing, or transferring their geolocation, proximity, or personal health information;
2. Obtain affirmative express consent from individuals before collecting, processing or transferring their information for specified COVID-19-related purposes;
3. Inform individuals, through a privacy policy provided before or at the time of data collection, of the purpose and categories of data collected, with whom data are shared, and how the data will be stored and handled;
4. Issue a public transparency report at least every 30 days describing the data collected and related activities;
5. Allow individuals to opt out of the collection, use or transfer of their geolocation, proximity, or personal health information and stop such collection or de-identify the data upon receipt of an opt-out request;
6. Delete or de-identify an individual's geolocation, proximity or personal health information when no longer being used for a specified COVID-19-related purpose;
7. Establish data minimization requirements to collect, process or transfer an individual's geolocation, proximity or personal health information; and
8. Establish, implement and maintain reasonable administrative, technical and physical data security policies and practices to protect against security risks to the information collected.

Selective Coverage

Despite the bill's broad requirements, its impact would focus mainly on technology companies outside of traditional health care. For example, tech companies working on contact-tracing apps that employ individual geolocation data would be covered, but other organizations collecting similar information for advertising or other purposes would be excluded. The Act defines those entities, as well as the data, covered by the Act as follows:

Covered Entities: Significantly, the bill would apply only to personal health information *not* subject to HIPAA, meaning that HIPAA-covered entities would be excluded from its requirements. The Act uses the term "covered entities" to apply to (1) any entity or person subject to FTC enforcement, (2) nonprofits, and (3) common carriers who collect, process or transfer precise geolocation data, proximity data, or personal health information. Employers are not excluded.

Covered Data: Geolocation data includes any information capable of identifying an individual's past or present location. Proximity data refers to information capable of reasonably identifying the past or present proximity of one individual to another. Personal health information includes an individual's genetic information or "information relating to the diagnosis or treatment of past, present, or future physical, mental health, or disability of the individual," if such information identifies or is reasonably linkable to an individual.

As noted above, the bill excludes personal health information already subject to HIPAA from its requirements. This means that covered entities under HIPAA likely would not be subject to the requirements of the COVID-19 Consumer Data Protection Act. For example, a COVID-19 diagnosis or test results disclosed by an individual's health care provider would not constitute covered data under the Act to the extent that such provider is subject to HIPAA. In contrast, apps that rely on individual input of COVID-19-related health information such as self-diagnosis or data derived from another source not subject to HIPAA, would have to comply with the Act.

Covered Purposes: The legislation is further limited in scope because it applies only to data collected, processed or transferred for three specific pandemic-related purposes. The COVID-19 Consumer Data Protection Act would apply to the collection, processing or transfer of an individual's data to (1) track the spread, signs or symptoms of COVID-19, (2) measure compliance with social distancing guidelines or other legal requirements related to COVID-19, or (3) conduct contact-tracing for COVID-19 cases.

This means that organizations would still be free to use consumer geolocation or personal health information for other purposes, even if indirectly related to an individual's infection status, because the draft bill's restrictions apply only to uses specifically related to COVID-19. Nevertheless, the bill would not otherwise prohibit companies from selling geolocation, proximity or personal health information, or from using such information to make inferences about an individual's health status or to use it for advertising purposes.

Supporters, Enforcement and Preemption

The COVID-19 Consumer Data Protection Act of 2020 was introduced by U.S. Sens. Roger Wicker, R-Miss., chairman of the Senate Committee on Commerce, Science, and Transportation, John Thune, R-S.D, chairman of the Subcommittee on Communications, Technology, Innovation, and the Internet, Jerry Moran, R-Kan., chairman of the Subcommittee on Consumer Protection, Product Safety, Insurance and Data Security, and Marsha Blackburn, R-Tenn.

The proposed bill would preempt any state law related to the collection, processing or transfer of covered information for the purposes specified in the Act. This preemption provision may prove to be a contentious issue, as it may cut against the federalism/state prerogative concerns of other Republican senators and congressional representatives.

The FTC would be responsible for enforcement of the Act under its powers regarding unfair or deceptive acts and practices. Additionally, the Act authorizes State Attorneys General to bring civil suits on behalf of their states' residents to enforce the Act's provisions, enjoin practices that violate the Act, and obtain damages or other appropriate relief.