King & Spalding
Client Alert

MAY 27, 2020

Congress Introduces Two Privacy Bills to Regulate COVID-19 Related Data

Competing proposals would protect certain data collected during the COVID-19 public health crisis.

For more information, contact:

J.C. Boggs
+1 202 626 2383
jboggs@kslaw.com

Phyllis Sumner
+1 404 572 4799
psumner@kslaw.com

Scott Ferber
+1 202 626 8974
sferber@kslaw.com

Mike Dohmann
+1 202 626 9263
mdohmann@kslaw.com

King & Spalding

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

As greater amounts of data are being collected to track and mitigate the spread of COVID-19, concerns about personal privacy have led lawmakers in Congress from both parties to introduce legislation to ensure appropriate usage and privacy protections.

On May 7, Republican members of the Senate Commerce Committee introduced the "COVID-19 Consumer Data Protection Act." Sponsored by committee chairman Roger Wicker (R-MS), and Sens. John Thune (R-SD), chairman of the Subcommittee on Communications, Technology, Innovation, and the Internet; Jerry Moran (R-KS), chairman of the Subcommittee on Consumer Protection, Product Safety, Insurance and Data Security; and Marsha Blackburn (R-TN), the bill would put in place rules regarding the collection, processing, and transfer of geolocation data, proximity data, persistent identifiers, and "personal health information" during the COVID-19 public health emergency, subject to certain exceptions and exclusions.

One week later, on May 14, a group of Democratic lawmakers, led by Sens. Richard Blumenthal (D-CT) and Mark Warner (D-VA), and Reps. Anna Eshoo (D-CA), Jan Schakowsky (D-IL) and Suzan DelBene (D-WA), introduced the "Public Health Emergency Privacy Act," which also restricts the collection, usage, and disclosure of certain data during COVID-19, but defines covered data more expansively and contains stronger protections for individual rights, including a private right of action and a non-preemption clause.

Many of the key requirements in both the Republican and Democratic bills may look familiar, as they are analogous to those found in the California Consumer Privacy Act of 2018 (CCPA) and the European Union's General Data Protection Regulation (GDPR), including the requirements

to post a clear and conspicuous privacy policy, to obtain affirmative advance consent to collect covered data, and to maintain reasonable data security policies and practices. However, the proposed measures cover narrower categories of protected information and are time-limited (*i.e.* during the COVID-19 public health emergency).

The **COVID-19 Consumer Data Protection Act** applies to any entity that is subject to the Federal Trade Commission Act or is a common carrier that collects, processes, or transfers covered data. Service providers are excluded from the definition. Covered data includes geolocation data, proximity data, persistent identifiers, and personal health information. However, data that has been aggregated, de-identified, or made publicly available would not be considered "covered data" under the proposal. "Employee screening data" also is excluded from the definition of covered data, "provided that such data is only collected, processed, or transferred by the covered entity for the purpose of determining, for purposes related to the COVID–19 public health emergency, whether the individual is permitted to enter a physical site of operation of the covered entity." In addition, the bill excludes employees, contractors, and visitors permitted to enter a physical site of operation of a covered entity from the definition of covered "individual."

The legislation makes it unlawful for a covered entity to "collect, process, or transfer the covered data of an individual" without prior notice and express consent unless necessary to comply with a legal obligation. This requirement applies to processing covered data to track the spread, signs, or symptoms of COVID-19; to measure compliance with social distancing guidelines or other COVID-19-related requirements imposed by federal, state or local governments; and to conduct contact tracing of cases of COVID-19.

Under the bill, "covered entities" are required to delete or de-identify covered information when it is no longer being used for the purpose for which it was initially collected, processed or transferred. Entities also need to minimize their collection, processing, and transfers of data to "what is reasonably necessary, proportionate, and limited" to the initial purpose. Covered entities must provide individuals with the "right to opt-out" or an effective mechanism that allows them to revoke their consent. Upon receiving an opt-out request, a covered entity has 14 days to discontinue collecting, processing, or transferring the covered data or it must de-identify the data.

The legislation further requires covered entities to publish a privacy policy about the entity's data transfer, data retention, and data security practices. In addition, the bill mandates that covered entities "establish, implement, and maintain reasonable administrative, technical, and physical data security policies and practices to protect against risks to the confidentiality, security, and integrity" of the data covered by the law.

During the COVID-19 public health emergency, covered entities are required to issue a "public report" not later than 30 days after the Act's enactment and every 60 days thereafter that includes: the aggregate number of individuals whose data the entity has collected, processed or transferred; the categories of data that were collected, processed or transferred; the purposes for which data was collected, processed or transferred; and those to whom it was transferred.

If enacted, the COVID-19 Consumer Data Protection Act would be enforced by the Federal Trade Commission (FTC) and by state attorneys general who are authorized to bring civil actions against covered entities that adversely affect the interest of residents of their state. The legislation further authorizes the FTC to promulgate "guidelines recommending best practices" for data minimization.

Notably, the Republican bill does not provide for a private right of action and contains a preemption clause preventing states from adopting, enforcing, or continuing to maintain any law that is "related to the collection, processing, or transfer of covered data." Federal preemption has been a sticking point in other efforts to enact federal consumer data privacy legislation with positions coalescing along party lines (Republicans generally in favor and Democrats generally opposed).

The **Public Health Emergency Privacy Act** applies to organizations that collect, use, or disclose "emergency health data" or develop certain tools for responding to the COVID-19 public health emergency. "Emergency health data" is expansively defined as "data linked or reasonably linkable to an individual or device, including data inferred or derived about the individual or device from other collected data provided such data is still linked or reasonably linkable to the individual or device, that concerns the public COVID–19 health emergency."

Unlike its Republican counterpart, the measure does not exclude employees, contractors, and visitors from the definition of covered individuals. Indeed, it goes a step further by proscribing the use of emergency health data for discriminatory, unrelated, or intrusive purposes, including commercial advertising, e-commerce, or efforts to gate access to employment, finance, insurance, housing, or education opportunities. However, healthcare providers, persons engaged in *de minimis* collection or processing of emergency health data, service providers, persons acting in their individual or household capacity, and public health authorities are excluded from the definition of covered organizations.

Covered organizations must obtain affirmative express consent from individuals, unless the collection, use, or disclosure is necessary and for the sole purpose of: protecting against malicious, deceptive, fraudulent, or illegal activity; detecting, responding to, or preventing information security incidents or threats; or otherwise required by a legal obligation. Covered organizations must also provide an "effective mechanism" for revoking consent. After an individual revokes consent, the organization must cease collecting, using, or disclosing the individual's emergency health data "as soon as practicable," but in no case later than 15 days after receipt of the revocation.

The bill's reporting requirements also differs from its Republican counterpart. A covered organization that collects, uses, or discloses emergency health data of at least 100,000 individuals shall, at least once every 90 days, issue a public report—stating in aggregate terms the number of individuals whose emergency health data the covered organization collected, used, or disclosed to the extent practicable; and describing the categories of emergency health data collected, used, or disclosed, the purposes for which each such category of emergency health data was collected, used, or disclosed, and the categories of third parties to whom it was disclosed.

Like its Republican counterpart, the Public Health Emergency Privacy Act is intended to be a temporary measure that would terminate upon the end of the COVID-19 public health emergency. The two proposals require meaningful data security and data integrity protections and mandate deletion by data processors following the public health emergency. Finally, both bills would mandate that all data collected through contact tracing apps be limited to public health use.

While the FTC and state attorneys general are authorized to enforce the provisions of both bills, the Public Health Emergency Privacy Act does not preempt states from adopting or enforcing laws or regulations related to the collection, processing, or transfer of covered data. The Democratic bill also creates a private right of action, permitting individuals to bring a civil action for violations of the Act, with statutory damages ranging from $100 to $5,000 per violation, along with reasonable attorney fees and litigation costs, as well as "any other relief, including equitable or declaratory relief that the court determines appropriate." The Democratic bill expressly provides that a violation of the Act with respect to the emergency health data of an individual "constitutes a concrete and particularized injury in fact to that individual." It also invalidates pre-dispute arbitration agreements and joint action waivers. The issues of preemption and private rights of action have been a sticking point for previous federal consumer data privacy efforts and could prove contentious again here.

Lastly, while both measures require organizations to receive "affirmative express consent" from consumers before collecting, using or disclosing their health information and to allow users to opt-out of data collection, the Democratic bill also requires that the health information collected not be used to prevent people from voting based on their

medical condition and mandates regular reports on the impact of such data collection tools on civil rights. Both the Democratic and Republican COVID-19 privacy bills are motivated by an urgent need to build public trust in the use of personal data and to ensure that businesses are held accountable for any misuse of data collected to fight the COVID-19 pandemic. However, if history is any guide, that shared motivation will be insufficient to overcome the political and ideological differences that distinguish the two measures, particularly as we draw closer to the 2020 election.