ML STRATEGIES

Cantwell-Cassidy Exposure Notification Privacy Act – A Bipartisan Bill on Disease Contact Tracing

June 09, 2020 | | By **Christian Tamotsu Fjeld**, **Christopher J. Harvie**

Last week, Senators Maria Cantwell (D-WA), the Ranking Member of the Senate Committee on Commerce, Science, and Transportation, and Bill Cassidy (R-LA) introduced the **Exposure Notification Privacy Act**, which would regulate the collection and use of consumer health data by disease contact tracing technologies. The proposed legislation is the third such bill that has been introduced in response to the use of exposure notification applications to monitor and control the spread of the coronavirus disease 2019 (COVID-19). Earlier in May, Senator Roger Wicker (R-MS), the Chairman of the Commerce Committee, along with Senators John Thune (R-SD), Jerry Moran (R-KS), Deb Fischer (R-NE), and Marsha Blackburn (R-T) introduced the **COVID-19 Consumer Data Protection Act**; while Senators Richard Blumenthal (D-CT) and Mark Warner (D-VA) and Representatives Anna Eshoo (D-CA), Jan Schakowsky (D-IL), and Suzan DelBene (D-WA) followed by introducing the **Public Health Emergency Privacy Act**.

These bills are in reaction to, in large part, the development of contact tracing applications that could soon be widely available to American consumers. Earlier this year, Apple and Google announced its initiative to modify its iPhone and Android mobile platforms (respectively) to develop an application programming interface (API) that will allow a phone's installed app to use Bluetooth technology to log information about other phones with which the user/phone was in contact. In so doing, such apps will reportedly take into account distance and length of contact with other phones. When a user reports (through the app) that he or she has contracted COVID-19, the phones that were previously in contact with that user's phone will be notified, and those users can take appropriate action (such as self-isolation).

Public health experts believe that if contact tracing apps are widely adopted and used, they will significantly help control the spread of the coronavirus. However, given the collection and transmission of large amounts of personal health information, lawmakers have responded with proposed legislation aimed at safeguarding consumer privacy.

The Cantwell-Cassidy bill introduced last week differs significantly from the Wicker and House-Senate Democratic bills introduced in May. It is narrower in scope and requires cooperation with public health officials with regard to the operation of exposure notice services. The bill also significantly differs from Senator Wicker's bill with regard to consent, enforcement, and preemption. The differences among the three bills reflect similar policy disagreements that were on display in various comprehensive privacy bills introduced or circulated for comment last year before the current pandemic.

Scope and Application

The Cantwell-Cassidy bill applies to online services, defined as "automated exposure notification service", that are specifically for "the purpose of digitally notifying, in an automated manner, an individual who may have been exposed to an infectious disease". This is a more narrow universe of affected entities than those in the Wicker bill, which applies to "covered entities" that collect, process, or transfer (or determine the means thereof) data involving geolocation, proximity, a persistent identifier and personal health information. The House-Senate bicameral bill broadly applies to "covered organizations" that collect, use, or disclose "emergency health information" by wire or radio or an online service that tracks, screens, monitors, contact traces, mitigates or otherwise responds to the COVID-19 pandemic.

The Cantwell-Cassidy bill applies to data that is linked or linkable to a person or device and is in connection with an automated exposure notification service. Like the Wicker bill, it excludes aggregated data, but not de-identified data, nor data that a covered entity may use to determine whether an individual (*e.g.*, an employee or visitor) can enter a facility, both of which are carved out in the Wicker bill. And it differs from the bicameral bill, which applies to a relatively extensive universe of information that includes data linked or linkable to a person or device, but also to inferred data that can broadly include "physical or behavioral health" and the "provision of health care". Furthermore, the Cantwell-Cassidy bill also confines data applicability by requiring exposure notification service operators to collaborate with public health authorities in the operation of the service. In so doing, the bill only applies to data with regard to a diagnosis of an infectious disease as authorized by the public health official.

Consent

Like the Wicker and House-Senate Democratic bills, the Cantwell-Cassidy bill requires “affirmative express consent” from consumers, but ties the consent to enrolling in an automated exposure notification service, which is narrower than the bicameral bill’s prohibition on the collection, use, and disclosure of emergency health data without affirmative express consent. The Wicker bill consent obligation applies when covered entities collect, process, or transfer covered data for a COVID-19-related purpose. The Cantwell-Cassidy bill also explicitly prohibits exposure notification services from inferring consent from inaction (similar to the bicameral bill and unlike the Wicker bill) and further requires consent to be “non-conditioned”. Non-conditioned consent could prevent an entity – that qualifies as an operator of an automated exposure notification service (as defined in the bill) – from, for instance, denying employment at a company or entrance into a facility, the latter of which the Wicker bill explicitly allows for its broader range of covered entities.

Use and Security

The Cantwell-Cassidy bill is similar to the Wicker and bicameral bills in restricting the use of collected data for the purposes of automated exposure notification, but the three bills differ in their stringency and prescriptiveness. All three bills also require transparency on the use of data, as well as data minimization, accuracy and security obligations, though they similarly differ in prescriptiveness. Both the Cantwell-Cassidy and House-Senate Democratic bills have explicit anti-discrimination provisions.

Enforcement and Preemption

All three bills empower the Federal Trade Commission (FTC) and state attorneys general to enforce the bills’ provisions with the authority to, among other measures, seek civil penalties. The Cantwell-Cassidy bill also allows a state to designate “an official or agency” to enforce the act, similar to the bicameral approach that empowers “any other officer of a state that is authorized by the state”. The bicameral bill differs from the other two bills by further providing the FTC with rulemaking authority under the Administrative Procedures Act, as opposed to its existing rulemaking authority under section 18 (also known as the Magnusson-Moss procedures), and creating a private right of action.

In stark contrast to Senator Wicker’s bill, both the Cantwell-Cassidy and House-Senate bicameral bills explicitly preserve all state laws; the Cantwell-Cassidy bill additionally and explicitly preserves common law and state statutory causes for action. The Wicker bill explicitly preempts state laws, regulations and standards related to the covered purposes of the bill.

Next Steps

It is not clear how the differences between these three bills will be resolved. Prior to the pandemic, Members of both the House and Senate, including the authors of these bills, were engaged in negotiations on comprehensive federal privacy legislation that affected a much larger universe of consumer information. Then, Members and their staff were trying to forge a compromise that overcame public policy differences on scope, application, enforcement and preemption. In order for a more narrowly focused COVID privacy bill to become law, House and Senate negotiators will have to similarly overcome these same differences with different flavors.

Authors

Christian Tamotsu Fjeld, Senior Vice President

Christian Tamotsu Fjeld is a Vice President of ML Strategies in the firm’s Washington, DC office. He assists a variety of clients in their interactions with the federal government.

Christopher Harvie