Back to Business

Practical guidance for an ever-changing world

Competing Bipartisan COVID-19 Privacy Bills to Be Introduced

Two federal data privacy bills may soon be introduced before Congress — The COVID-19 Consumer Data Protection Act, introduced by Republican Senators, and the Public Health Emergency Privacy Act, introduced by a group of Democratic Senators and Representatives. The proposed bills would both create privacy requirements specifically for health and location information collected for the purposes of tracking and preventing the spread of COVID-19.

Since technology is emerging as a key tool in controlling the spread of the coronavirus, the bills seek to ensure that entities that collect and process personal information for COVID-19 purposes (for example, to create contact tracing apps or programs) abide by certain data transparency, notice and consent rules when developing and rolling out technologies that may be collecting sensitive health and location data.

Public Interest vs. Privacy: A Balancing Act

The Senators emphasized that the bills attempt to balance public interest in the collection and use of personal information to fight COVID-19 with the right of individuals to not have their privacy infringed by the misuse of such information.

The COVID-19 Consumer Data Protection Act

What's "Covered"?

The bill would apply to any Covered Entity that collects, processes or transfers Covered Data for Covered Purposes.

>> "Covered Data" includes precise geolocation data, proximity data and personal health information.

The Bottom Line

With pressures mounting to find new ways to fight the coronavirus and responsibly ease social distancing restrictions, the use of mobile and geolocation technologies may be key in this fight. Therefore, both The COVID-19 Consumer Data Protection Act and the Public Health Emergency Privacy Act may gain traction.

Businesses need to consider existing and new privacy laws before developing or implementing any new services.

>> A "Covered Entity" is any entity or individual regulated by the Federal Trade Commission (FTC) or any common carrier or non-profit organization that collects, processes or transfers Covered Data.

>> "Covered Purposes" includes using the Covered Data to track the spread of COVID-19, measuring compliance with social distancing guidelines or to conduct contact tracing.

Covered Entities would have to comply with certain obligations and restrictions on the use of Covered Data, including by:

>> Obtaining affirmative express consent from individuals before collecting, processing or transferring Covered Data;

>> Providing notice at collection of the purpose for such collection, processing or transfer;

>> Allowing individuals to opt-out of the collection, processing and transferring of such information or revoke their prior consent;

>> Publishing a privacy policy that includes categories of recipients of such information and a description of its data retention and security practices;

>> Following the practice of data minimization so that no data beyond what is reasonably necessary and proportionate is collected; and

>> Providing public reports every 30 days on the number of individuals whose information was collected, processed or transferred, and the categories, purpose and recipients of such information.

Additional Requirements

The bill also embraces standard privacy themes of reasonable security measures and data minimization. It would also require companies to delete or de-identify the data when it is no longer needed for COVID-19 public emergency purposes. The FTC would primarily be charged with enforcement of the Act. The bill would only impose these requirements as long as the Health and Human Services' declaration of COVID-19 as a public health emergency remains in effect.

Public Health Emergency Privacy Act

What's "Covered"?

The bill would apply to any Covered Organization that collects, uses or discloses Emergency Health Data.

>> "Emergency Health Data" means data linked or reasonably linked to an individual or device, including data inferred from such data, that concerns the COVID-19 Public Health Emergency, including healthcare data, or data collected to track, screen or monitor COVID-19 such as geolocation data, proximity data, demographic data, contact information or information collected from a personal device.

>> "Covered Organization" means any person, including a government entity, that:

1. Collects, uses or discloses Emergency Health Data electronically (or through wire or radio); or

2. Develops or operates a website, web/mobile/smart device application or mobile operating system feature for the purpose of responding to the COVID-19 Public Health Emergency. It does not include service providers, healthcare providers, public health authorities, people who process a de minimis amount of Emergency Health Data or does so in their individual or household capacity.

>> "COVID-19 Public Health Emergency" means the outbreak and public health response pertaining to the COVID-19 emergency declared by the Secretary of Health and Human Services.

Covered Organizations would have to comply with certain obligations and restrictions on the use of Emergency Health Data, including by:

>> Only collecting, using or disclosing Emergency Health Data as necessary, proportionate for a limited good faith public health purpose;

>> Taking reasonable measures to ensure the accuracy of such data and allow individuals to correct inaccurate information;

>> Adopting reasonable safeguards to prevent unlawful discrimination based on such data;

>> Only disclosing such information to a government entity if to a public health authority or only for a good faith public health purpose in direct response to exigent circumstances;

>> Establishing and implementing reasonable data security measures to protect such information;

>> Obtaining prior affirmative express consent from the individual to collect, disclose or use such data, except for:

1. Preventing or detecting fraudulent activity;

2. Responding to or preventing security incidents; or

3. For a legal obligation.

>> Allowing individuals to revoke their consent to collect, disclose or use such data, and comply with such revocation within 15 days, and destroy or anonymize such data within 30 days, of receiving such a request.

>> Providing a privacy policy that describes how and for what purpose such data is collected, used and disclosed, including the categories of recipients of such data, the organizations' retention and security practices and how they can exercise their rights and file a complaint to the FTC for any violations; and

>> Providing a public report every 90 days on the number of individuals whose information was collected, used or disclosed and the categories, purpose and recipients of such information.

Additional Requirements

The Public Health Emergency Privacy Act goes beyond the COVID-19 Consumer Data Protection Act and specifically prohibits the use of Emergency Health Data for marketing or discriminatory purposes.

It also requires the destruction of Emergency Health Data, either 60 days after the COVID-19 public health emergency declaration ends (as declared by the Health Secretary or State governor or chief executive) or 60 days after collection of such information, whichever is later.

The Public Health Emergency Privacy Act also specifically prohibits the use of Emergency Health Data to infringe on an individual's right to vote. The Act also calls for the United States Commission on Civil Rights to create a report on the civil right impact of the use of Emergency Health Data.

The FTC would also be the primary enforcer of this Act.

A Look to the Future

If either of these bills pass, they could further spur the move towards a national comprehensive data privacy law that would finally establish national privacy and data protection requirements beyond just COVID-19 specific-purposes.

Meanwhile, businesses are moving ahead in the fight against COVID-19, with Google and Apple recently launching its contact-tracing software.

These bills are yet another example of how governments are grappling with the balance of technology and privacy in the face of the pandemic.

DIGITAL MEDIA, TECHNOLOGY & PRIVACY

The Federal Communications Commission (FCC) made a declaratory ruling in March that COVID-19 qualified as an emergency under the Telephone Consumer Protection Act (TCPA), allowing health care providers and government officials to send automated calls or texts to individuals without their consent, but only for COVID-19 informational purposes.

The European Data Protection Board adopted guidelines in April that laid out how government and private actors could use location data and contact tracing tools for COVID-19 purposes in keeping with the General Data Protection Regulation (GDPR) and the ePrivacy Directive.

For More Information

Please contact the attorneys listed below or the D&G attorney with whom you have regular contact.

Gary A. Kibel
Partner
212.468.4918
gkibel@dglaw.com

Jean H. Shin
Associate
212.468.4857
jshin@dglaw.com