Federal Privacy Law in Response to COVID-19 on the Rise: The COVID-19 Consumer Data Protection Act of 2020 vs. The Public Health Emergency Privacy Act

Insights
6.04.20

Over the years, Congress has put forth various legislative proposals regarding data privacy. None of the past legislation received the support necessary to enable passage of a comprehensive national data privacy law. However, data collection and analysis is becoming a key weapon in the fight against COVID-19 as companies and governments have sought to come up with effective and socially distant ways to keep close tabs on people's health status and movements. These methods often involve using technology to collect vital but potentially sensitive health and location information.

In response to the conflict between personal privacy rights and public well-being, legislators on both sides of the political spectrum have introduced legislation to strengthen data security and privacy protection for the public.

COVID-19 Consumer Data Protection Act

On April 20, 2020, a group of Republican Senators, led by Mississippi Senator Roger Wicker, introduced the COVID-19 Consumer Data Protection Act ("CCDPA"). As written, the CCDPA would require companies under the jurisdiction of the Federal Trade Commission ("FTC") to obtain affirmative express consent from individuals prior to collecting, processing, or transferring their personal health, geolocation, or proximity information for the purposes of tracing the spread of COVID-19. Companies would also be responsible for disclosing at the point of collection how consumer data will be handled, transferred, and retained, while permitting individuals to opt out of the collecting, processing, or transfer process. Companies subject to the CCDPA would also be responsible for deleting or de-identifying all personally identifiable information once it is no longer being used for COVID-19 purposes.

Public Health Emergency Privacy Act

Following on the heels of the CCDPA, on May 14, 2020 Senate Democrats introduced the Public Health Emergency Privacy Act ("PHEPA"), which, among other things, would protect personal data collected in connection with COVID-19 from being used for non-public health purposes. PHEPA provides for both public and private rights of action, permitting the FTC, state and public officials, and individuals alleging a violation of the Act to bring a civil action. Similar to the CCDPA, the PHEPA requires that companies obtain affirmative express (opt-in) consent from individuals prior to collecting, processing, or transferring their personal health, geolocation, or proximity information

for the purposes of tracing the spread of COVID-19. In addition, companies would also be responsible for disclosing at the point of collection how consumer data will be handled, transferred, and retained; permitting individuals to opt out of the collection, processing, or transfer process; and destroying or deleting any data collected after the conclusion of the COVID-19 public health emergency. Finally, PHEPA also prohibits government entities from using any collected personal health information to deny, restrict, or interfere with an individual's right to vote in a federal, state, or local election.

The following is a comparison of the key provisions of the two Acts:

	CCDPA	**PHEPA**
What is Covered?	· **"Covered Entities"** - A wide range of organizations, including businesses under the Federal Trade Commission's jurisdiction as well as non-profits and common carriers. · **"Covered Data"** - A variety of types of data, including geolocation data, proximity data, persistent identifiers such as IP addresses or device IDs, and personal health information. · **"Covered Purposes"** - Certain purposes or use cases, including the collection, processing, or transfer of covered data to (1) track the spread, symptoms, or signs of COVID-19; (2) measure compliance with social distancing guidelines; and (3) conduct contact tracing. The CCDPA **does not cover**, among other things, data that is already protected by HIPAA and data collected by employers to determine whether employees may enter a physical location.	· **"Covered Entities"** – Public and private entities that collect "Emergency Health Data" ("EHD"). · **"Covered Data"** – Referred to as EHD, data covered by the PHEPA includes personal health information, geolocation data, proximity data, demographic data, contact information, and any other data collected from an individual's personal device. PHEPA expressly **does not apply** to a covered entity or business associate under HIPAA. However, unlike the CCDPA, the PHEPA is not limited to private entities and would also regulate some governmental use, collection, and disclosure of EHD.
What is Required?	The CCDPA makes it unlawful for a covered entity to collect, use, or transfer covered data for a covered purpose unless three requirements are met: 1. Individuals receive notice prior to collection, use, or transfer of the data; 2. Individuals give affirmative express consent; and	The PHEPA imposes restrictions and compliance obligations similar to those set forth in CCDPA. 1. It limits the permissible purposes for collecting, using, and disclosing EHD, including reasonable safeguards to prevent unlawful discrimination based on EHD;

	3. The covered entity publicly commits to not collect, use, or transfer the data for any non-disclosed purpose. The CCDPA also requires covered entities to update their privacy policies, to use reasonable security to protect the covered data, to use principles of data minimization, to provide an opt-out mechanism for individuals who previously consented, and to delete the data when it is no longer needed for the covered purposes.	2. requires reasonable security to protect EHD; 3. requires reasonable measures to ensure EHD accuracy and a mechanism to correct inaccuracies; 4. requires certain privacy policy disclosures and, if an organization has collected data of at least 100,000 individuals, certain additional disclosures every 90 days; and requires deletion of EHD upon the occurrence of specified events. 5. The PHEPA generally also requires affirmative express consent prior to the collection, use, or disclosure of EHD (subject to limited exceptions) and requires a mechanism for individuals to revoke consent.
Who Enforces?	Either the Federal Trade Commission or state attorney generals would enforce the CCDPA.	Either the Federal Trade Commission or state attorney generals would enforce the PHEPA.
Is There a Private Right of Action?	The CCDPA does not provide a private right of action.	Unlike the CCDPA, the PHEPA provides a private right of action for violations that constitute a concrete and particularized injury in fact to the individual.

How Should Employers Prepare?

Although there may not be a consensus on the details, there seems to be bipartisan support for the concept of introducing federal privacy legislation to address the issues raised by COVID-19. As such, employers may want to consider the following before deploying newly available technology to track COVID-19 infection in the workplace.

- In addition to providing notice and obtaining consent, employers should consider implementing procedures where employees can: (1) opt out of data collection; (2) revoke consent; and (3)

request the deletion or de-identification of their personally identifiable information when it is no longer being used for the COVID-19 public health emergency.

- Employers should minimize the collection, processing, and transfer of data to only what is reasonably necessary, proportionate, and limited to the initial purpose of the collection.
- Employers should put into place administrative, technical, and physical cybersecurity protections to protect the confidentiality, security, and integrity of the data that is collected.
- Employers may also want to consider analyzing factors and questions relevant to how contact-tracing tools will be used in their workplaces:
    - Will the use of the contract-tracing tool be voluntary or mandatory?
    - If mandatory, how will employees who refuse to use the tool or "turn it off" be handled?
    - Will the tracking function be limited to work hours, and if so, how will this be accomplished?
    - Who will have access to the information collected?

While it is too early to tell what form any final legislation may take or whether either proposed bill will become law, the CCDPA and the PHEPA contain helpful guidance and potential best practices for employers that are planning to utilize new technology related to COVID-19 in the workplace.

Service Focus

Privacy and Cyber

Consumer Privacy Team