Pandemic Has Congress Considering Data Privacy in 'Paper Hearing'

The Senate Commerce Committee seeks to balances data collection and use with privacy to control the coronavirus spread.

Melissa Harris

Tue, 04/14/2020 - 11:54

Photo Credit: elenabs/iStock

A panel of data and privacy experts virtually provided recommended actions and guardrails for the Senate Commerce, Science and Transportation Committee as lawmakers consider ways of utilizing big data to respond to the COVID-19 pandemic.

In the committee’s “paper hearing,” which began last Thursday with written opening statements and questions posted publicly for the witnesses to respond to, the panel of experts provided both potential uses and dangers that location data holds in combating the pandemic, while also contextualizing the outbreak in the larger obstacles of health data portability and need for a national data privacy framework.

The paper hearing is a hearing being conducted virtually as Congress follows the large majority of the nation that has moved to mass telework in an effort to prevent the spread of COVID-19 over the past month. These versions of hearings are reportedly not official and will only enter official record with unanimous consent when senators are again present in person.

Collecting consumer location in an anonymized way could allow officials to track and predict tends in COVID-19 spread and that leveraging artificial intelligence and machine learning with big data could help identify patterns, make diagnoses, and find other patterns in disease transmission.

“This location data is purported to be in aggregate form and anonymized so that it does not contain consumers’ personally identifiable information,” Committee Chair Sen. Roger Wicker said. “It is intended to help researchers identify where large crowds are forming and pinpoint the source of potential outbreaks. The data may also help predict trends in the transmission of COVID-19 and serve as an early warning system for individuals to self-isolate or quarantine.”

The witnesses further stressed the fine line that lawmakers must consider between leveraging big data to adopt precision measures against COVID-19 and providing the transparency and protection that will ensure privacy is maintained in collecting data across the country.

Pther countries compromised data privacy and transparency to monitor COVID-19, leading to extreme enforcement measures, noted Center for Democracy and Technology Privacy and Data Director Michelle Richardson. China, for instance, worked with industry to produce a smartphone app that dictates whether a person needs to be quarantined.

“The app not only determines in real time whether someone poses a contagion risk, it also shares information with the police,” Richardson said, adding that individuals’ “location appears to be sent to the system’s servers, possibly allowing the authorities to track people’s movements over time.”

University of Washington Law Professor Ryan Calo, however, said that there are ways to anonymize data when collecting and aggregating it. He cited the Google COVID-19 Community Mobility Report, which provides month-to-month information on how communities are traveling to work or using public transportation relative to a pre-coronavirus baseline.

“Google is using consumer location information, which is a highly sensitive form of data,” Calo said. “But because the data is aggregated and displayed only as a relative percentage, the risks to individuals are mitigated. Meanwhile, the data is useful to policymakers in determining where additional social distancing measures might be needed and to health officials in assessing the correlation between social distancing and rates of viral infection.”

Google’s report provides broad information about trends, however, while “the federal government is already looking into more granular data to implement more targeted stay-at-home or other social distancing measures,” App Association Senior Director of Public Policy Graham Dufault said. Moving forward, Dufault said COVID-19 contact-tracing apps should clarify that location data stays on users’ phones and does not go to a centralized server.

“Instead, when turned on, the app tracks the user’s location and stores it in an encrypted format — which it apparently sends, again encrypted, directly to other phones when queried,” Dufault suggested of contact-tracing apps for lawmakers to consider.

Richardson suggested other actions that lawmakers should apply to data-driven COVID-19 response measures, given that government and industry collection and use of data can easily slip to levels of hyper surveillance and privacy intrusion. Specifically, she recommended that when considering data use, lawmakers should:

- Focus on prevention or treatment rather than punishment or broad surveillance functions.

- Ensure accuracy and effectiveness in predicting, preventing and responding to COVID-19.
- Provide actionable information to inform individual, corporate or government behavior in constructive ways.
- Require government and industry to respect privacy by aggregating data, minimizing data collection and use, purposing data limitations, and deleting data when it's no longer necessary for the COVID-19 response.
- Build services that serve all populations.
- Empower individuals when possible, namely in making data-based programs voluntary.
- Be transparent to build trust.
- Establish a coordinated government response that rigorously oversees threats to personal privacy and liberties.

Even if Congress and agencies adopt these rules when using data in the national COVID-19 response, several witnesses stressed that the country's lack of federal data privacy laws is an underlying problem that complicates mass data use and security concerns in regard to and beyond the pandemic.

"In comparison to the European Union and other governments with comprehensive data privacy laws, the United States does not currently have a baseline set of legal protections that apply to all commercial data about individuals, regardless of the particular industry, technology or user base," Future of Privacy Forum Senior Counsel Stacey Gray said. "Instead, the United States has taken a sectoral approach that provides strong privacy and security protection for information collected in certain contexts, while leaving equally sensitive information about those same individuals largely unregulated."

Network Advertising Initiative President and CEO Leigh Freund further detailed specifics that lawmakers should incorporate into a federal consumer privacy law, given the concerns that have arisen both in COVID-19-related data collection and applications and preexisting anxieties about big tech opacity of data use.

“Under the framework, companies are prohibited from obtaining a range of sensitive information — including health, financial, biometric and geolocation information, as well as call records, private emails and device recording and photos — without obtaining consumers’ expressed consent,” Freund explained. “The framework gives individuals the right to request access to, or deletion of, the personal information that a company maintains about them, and to learn about the types of third parties with whom personal information has been shared.”

The Senate Commerce Committee’s paper hearing started shortly before Apple and Google announced that they would collaborate to create a contact-tracing solution that would use Bluetooth technology on smartphones to assist federal health agencies. Other governments, like the E.U., Singapore and India, have adopted similar Bluetooth proximity-monitoring solutions.

The two companies said that they will release application program interfaces that will allow contact tracing through public health authorities’ third-party apps, which users can download via app stores. Later, the companies plan to build a broader contact tracing tool that won’t require third-party app downloads.

The Senate Commerce Committee did not respond to comment on how Congress will approach projects like Apple and Google’s or if the committee will establish data collection and use guardrails to protect consumers as industry and governments respond to the COVID-19 pandemic.

View printer friendly version

COVID-19
coronavirus
data
privacy
data protection
mobile security
APIs
Standard