Public Knowledge

April 9, 2020

The Honorable Roger Wicker
Chairman
U.S. Senate Committee on Commerce, Science, and Transportation
555 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Maria Cantwell
Ranking Member
U.S. Senate Committee on Commerce, Science, and Transportation
511 Hart Senate Office Building
Washington, DC 20510

Re: Hearing on Enlisting Big Data in the Fight Against Coronavirus

Dear Chairman Wicker and Ranking Member Cantwell,

The proper use of personal data has the potential to have important benefits for public health as we face the COVID-19 crisis. Technology can and should play an important role during this effort to save lives, such as to spread public health messages and increase access to health care. However, efforts to contain the virus must not be used as a cover to usher in a new era of greatly expanded systems of invasive digital surveillance. Allowing access to personal data without guardrails threatens fundamental rights and liberties and opens the door for communities to be exposed to civil rights harms through the exploitation of their data.

One such guardrail should be that the collection and processing of personal data must be necessary and proportionate to the pandemic response as well as the protection of public health. All response measures should be temporary in nature, limited in scope, restricted to using anonymized aggregate data whenever possible, and adopted only if they are a necessary response to the COVID-19 crisis. The data collected and processed should be limited to the minimum necessary amount for the purposes of implementing measures for pandemic response. There must also be limits on processing newly collected or acquired personal data for purposes unconnected to public health and services. The personally identifiable data should not be kept or repurposed except in the case of narrowly defined medical research purposes and pandemic preparedness. For those specific uses, informed and explicit consent of the individual should be required.

Another guardrail would be requiring adequate security measures to protect personal data. Attempts to respond to this pandemic cannot be used as justification for

compromising people's digital safety; this crisis does not minimize the need for security protections in the context of pandemic response. Data must be maintained in a secure environment and transmitted through secure methods. And any claims that publicly shared data has been anonymized must be based on evidence and supported with sufficient information explaining the anonymization process.

Any use of digital surveillance technologies in responding to COVID-19, including big data and artificial intelligence systems, must include risk assessments that address concerns around discrimination and other rights abuses against racial minorities, people living in poverty, and other marginalized populations, whose needs and lived realities may be obscured or misrepresented in large datasets. We should bear in mind the last time mass surveillance power expanded was when Congress passed the Patriot Act. It was argued, as it is being argued now, that increased surveillance was necessary in order to protect Americans. Instead, the tools designed to address terrorism ended up being used by law enforcement during the course of ordinary investigations, which only exacerbated the difference in policing between white communities and communities of color.[1] We need to learn from these previous lessons and do our best to ensure that this expansion of data collection practices is limited, and that those limitations apply to both public and private entities. Also, all data collection efforts undertaken as a response to the pandemic should include means for active and meaningful participation of all relevant stakeholders, and, in particular, marginalized population groups.

The final guardrail is requiring accountability provisions for any pandemic responses that collect or process data. This is a fundamental safeguard against abuse. First, there must be transparency about the measures taken so that they can be scrutinized and, if appropriate, later modified, retracted, or overturned. Furthermore, any decision-making related to data collection and processing in the context of pandemic response must be informed by guidance and directions of public health authorities; therefore, the guidance and decisions must be made publicly available. Additionally, individuals must be given the opportunity to know about and challenge any COVID-19 related measures to collect, aggregate, retain, and use personal data. Individuals must have access to their data and be allowed to correct or delete their data when practicable. Finally, there must be real, commensurate consequences for governments' and companies' failure to protect personal data.

We have identified a few key areas where legislation would provide immediate privacy benefits and significantly reduce the harms as outlined in this letter. These include:

[1] Benjamin Wallace-Wells, *Patriot Act*, New York Magazine (August 26, 2011) https://nymag.com/news/9-11/10th-anniversary/patriot-act/.

1. **Creating Rules for Public-Private Data Sharing.** If governments enter into data sharing arrangements with other entities, those arrangements must be based in law and memorialized in writing. The existence of these agreements and information necessary to assess their impact on privacy must be publicly disclosed, with sunset clauses, public oversight and other safeguards by default. Businesses involved in efforts by governments to tackle COVID-19 must undertake due diligence to ensure they respect human rights. Any new data or processing for this purpose must be firewalled from other business and commercial interests. Furthermore, the results of any data-sharing should be made public in a machine-readable format, if the publicization of the results would not result in re-identification of the individuals whose data was collected. It would also have the added benefit of allowing others to iterate and innovate. Preference for these data sharing arrangements should not be given to large players in the data ecosystem; we've already seen increasing consolidation in the technology space,[2] and these initiatives should not add fuel to the fire.
2. **Closing the HIPAA Privacy Loophole.** HIPAA does not currently cover technology like health apps, direct-to-consumer genetic tests, and other consumer-focused health technology, like wearable fitness monitors. As it has become more difficult than ever to personally interact with a doctor or hospital, consumers are relying on these technologies to assess their risk, as well as to make and even participate in medical appointments. This means consumers are giving up their health data without adequate protection. Congress should give HHS the authority to promulgate clear and public rules regulating this growing industry to ensure that all Americans' health data is kept private and secure, no matter who is collecting it.
3. **Protecting Geolocation Data.** While federal law prevents cell phone network operators from disclosing geolocation data to anyone other than emergency services, mobile phone operating system providers and mobile applications can disclose this data to anyone. Geolocation data can reveal a person's politics, sexual preferences, religion, and other sensitive characteristics. The government having access to geolocation data, and all that it reveals, is deeply concerning. Americans should not need to make their highly sensitive location data available for exploitation as the cost of staying in touch with emergency services at all times. Congress must prevent our geolocation data from being exploited by any actor who has access to that information; therefore, we are asking that current geolocation data protections that apply to cell phone network operators be applied to phone operating systems.

We look forward to working with the committee to ensure that privacy protections are built into public health initiatives during this time of crisis.

---

[2] Alex Petros, *Acquisitions in the Time of COVID: Big Tech Gets Bigger,* Public Knowledge (April 7,2020) https://www.publicknowledge.org/blog/acquisitions-in-the-time-of-covid-big-tech-gets-bigger/

Sincerely,

Sara Collins

Policy Counsel

Public Knowledge

Cc: Senate Commerce Committee Members