

Ms. Stacey Gray, Senior Counsel, Future of Privacy Forum

Questions Submitted by Members of the Senate Committee on Commerce, Science, and Transportation

Enlisting Big Data in the Fight Against Coronavirus

April 9, 2020

Chairman Wicker

1. Many national and local governments around the world are seeking to use new technology to combat this unprecedented pandemic. Earlier this week, the German government launched an app that allows users to “donate” personal data collected by their fitness trackers or other health devices to help authorities analyze the spread of COVID-19. Authorities in Moscow have launched an app intended to be downloaded by those who test positive for COVID-19. Yet this app raises privacy concerns, as it would allow officials to track residents’ individual movements.
 - As governments seek to use new technologies in the fight against COVID-19, it is imperative that privacy rights be protected. Are there specific examples of app-based programs you can recommend to policymakers that are both useful in the fight against COVID-19 and respectful of individual privacy rights?

2. Much of the discussion surrounding the collection of private data to fight the spread of COVID-19 presents two goals – effectiveness and privacy protection – as mutually exclusive factors that need to be balanced. On one side of the balance, it is assumed that greater amounts of personal data, in more granular form, will allow authorities to track the spread of the virus more effectively. On the other side of the balance is protection of individual privacy, which is believed to be threatened by greater surveillance of individuals by the government.
 - Is this an accurate view of the situation? Are privacy and effectiveness always part of a trade-off, such that the most effective public health measures will come at the expense of privacy, and vice versa? Or do you believe that the most effective policies for combatting COVID-19 can also respect individuals’ privacy?

3. Today, the United States has numerous federal laws governing different types of data, such as health-care data or financial data. However, there is currently no federal privacy law that applies generally to all types of consumer data. As Chairman of the Commerce Committee, I have made it a priority to get a national data privacy law enacted as soon as possible.
 - If the United States had a national data privacy law in place before the COVID-19 pandemic began, what would the effect have been on efforts to use data to combat the spread of the virus? Would Americans’ privacy be more protected, and would companies be more incentivized to take privacy-protective approaches, if we had such a law?

Ms. Stacey Gray, Senior Counsel, Future of Privacy Forum

4. In the United States, the mobile advertising industry and technology companies are collecting consumers' smartphone location data to track the spread of COVID-19 and compliance with social distancing measures. The location data is purported to be in aggregate form and anonymized so that it does not contain consumers' personally identifiable information.
 - How can the use of anonymized, de-identified, and aggregate location data minimize privacy risks to consumers? And, what additional legal safeguards should be imposed on the collection of this data to prevent it from being used or combined with other information to reveal an individual's identity?
5. As technology companies share anonymized location data with the U.S. government to support COVID-19 response efforts, to what extent should purpose limitation principles apply to the use and analysis of this data? And, when the pandemic finally passes, what should be done with any anonymized or de-identified data – and identifiable data, if applicable – collected by technology companies and the government for the purpose of addressing the public health crisis?

Sen. Thune

6. More and more Americans all throughout the country are turning to online video services to conduct their jobs, education, and social interactions in an effort to practice social distancing. For instance, Zoom Communications had more than 200 million daily users last month. It was found that thousands of Zoom's calls and videos have been exposed to other users online and log-in information has been stolen resulting in many individuals' personal information being compromised.
 - Did Zoom's privacy policy clearly outline what types of information its platform would collect on individuals? If not, what transparency requirements should be in place for companies like Zoom?
 - Americans are connecting with each other via online services across all 50 states. Would a patchwork of state laws benefit consumers and better protect their privacy? Should the United States enact a national privacy standard to safeguard consumer's information?
7. Without a federal privacy law in place, the American people must rely on the promises of tech companies that all have varying degrees of commitment to maintain consumers' privacy.
 - How do we ensure that organizations are actively engaging in data minimization and strategic deletion practices after data is used or transferred?
8. The country of Israel, through its internal security service, has reportedly used smartphone location-based contact tracing to notify citizens via text that they have been in close proximity to someone infected with COVID-19, and ordering them to self-isolate

Ms. Stacey Gray, Senior Counsel, Future of Privacy Forum

for 14 days. A recent opinion piece in the Scientific American urged democratic governments to quickly follow Israel's lead (see ["As COVID-19 Accelerates, Governments Must Harness Mobile Data to Stop Spread"](#)).

- Please provide your thoughts on smart-phone location-based contact tracing in light of the extraordinary privacy and other civil liberties concerns such an approach raises for U.S. citizens.
 - According to the [Wall Street Journal](#), MIT is developing a contact tracing app for COVID-19 patients and others who have not been infected by COVID 19 that can be voluntarily downloaded to a person's smart-phone. Please provide your views on this approach to contact tracing.
9. COVID-19 has caused private companies to seek out and utilize health data in an effort to protect users, employees, and the general public from the spread of the virus. Both Apple and Alphabet have released websites to help users self-screen for exposure to COVID-19. This data will be used to help public health officials. However, these tools also allow technology companies access to user's health information which the companies could in turn profit from in the future.
- How are technology companies balancing the need for timely and robust reporting to prevent the spread of the virus with the confidentiality and privacy of the participants?
 - What safeguards are in place to ensure data collected as part of the fight against COVID-19 are not sold to business partners or used for the development of other commercial products?
10. Anonymization techniques are also critical for safeguarding consumers' privacy. Truly anonymized data can protect a consumer's personal information, like their geolocation, political opinions, or religious beliefs.
- How do companies guarantee that every dataset they are storing contains truly anonymous data? And is the ability to re-identify data a part of the discussion in data-sharing arrangements?

Sen. Blunt

As you know, this committee has prioritized drafting federal privacy legislation for the purpose of creating clear, baseline definitions and standards for data collection, storage, and use across industry sectors. Similarly, the bills before this committee attempt to create definitions to meet appropriate levels of consent and transparency for protecting consumers' privacy and security.

In relation to COVID-19, the end users of specific data sets, like location data, are more likely to be governmental entities than commercial entities. Big data can be an incredible tool to better understand the spread of the virus, and the impact on communities across the country. Data can help identify resource deficits, inform governments and health care professionals to employ countermeasures at the appropriate time, and provide insight to the downstream economic effects of this pandemic.

Ms. Stacey Gray, Senior Counsel, Future of Privacy Forum

However, U.S. commercial entities that would likely be collecting this data have very few guardrails on the collection and distribution of this data. Similarly, there are few requirements or regulations at federal and state levels which guide methodologies for anonymizing or pseudonymizing data. De-identifying data may result in greater data privacy and data security for consumers or individual citizens but relies heavily on all of the entities involved in the collection and storage of that data making decisions based on best practices.

11. What efforts do you recommend that federal agencies undertake to ensure that data being used to track viral spread are upholding the highest possible standards for individual privacy and security?
12. Does data lose any utility when it is de-identified or anonymized? Is it possible to have large data sets that are not tied to individual's identities, but which would still be useful for governments or public health-related end users?
13. It is important to me that as government entities access commercially collected or publicly available data, that those efforts are giving reasonable consideration to protecting individual privacy and security.
14. Are there any technologies that offer the opportunity to collect data that would be useful to governmental pandemic response efforts, without resorting to surveillance methods that jeopardize individual privacy – like those which have been used recently by foreign governments?

Sen. Cruz

15. A little over two weeks ago, the Johns Hopkins Center for Health Security published a report titled *“Modernizing and Expanding Outbreak Science to Support Better Decision Making During Public Health Crises: Lessons for COVID-19 and Beyond.”* Although full of thought-provoking ideas, one of the most notable was a recommendation to establish a “National Infectious Disease Forecasting Center,” similar to the National Weather Service. Much like the National Weather Service, this new infectious disease forecasting center would have both an operational role—providing the best modeling and forecasting to policy makers and public health professionals before, during, and after a disease outbreak—as well as a research role—providing a venue for academic, private sector, and governmental collaboration to improve models and encourage innovation.
 - What do you all think of this idea, and what do you all think the positives and negatives would be if such a concept was operationalized?

Ms. Stacey Gray, Senior Counsel, Future of Privacy Forum

16. One of the big reasons weather forecasting works, if not the biggest, is how many observations—things like water temperature, barometric pressure, radio profiles of the atmosphere, etc.—are fed into the weather model. Now while collecting ocean temperatures from buoys, or pressure readings from weather balloons, doesn't really raise privacy concerns, collecting health observations almost certainly would.
 - How can we thread the needle—either in this concept or private sector modeling—of getting enough of the right kind of data to accurately model infectious disease outbreaks while still protecting the privacy and security of individuals?

17. To date the State of Texas has reported thousands of cases of coronavirus, and hundreds of deaths related to complications from infection. To mitigate the risk of infection in Texas and across the country, the administration has restricted international travel, provided more access to medical supplies by involving the powers of the Defense Production Act, and cut red tape to expand access to testing. Congress also passed the CARES Act which provided \$377 billion in emergency loans for small businesses and directed \$100 billion to hospitals and healthcare providers. However, I believe much still needs to be done to finish this fight and recover once this is behind us.
 - In your expert opinions, what more needs to be done to beat this virus, and how can federal, state, and local governments work with private companies to both mitigate spread of the virus—both now and later this summer or fall—and recover quickly once the threat of this virus has passed?

Sen. Moran

18. Many of the discussed proposals related to utilizing “big data” to fight against the spread against coronavirus rely upon the concepts of anonymized and aggregated data to protect the personal identity of individuals that this information pertains to and prevent consumer harms that could result. As such, many members on this Committee have spent significant time and energy drafting federal privacy legislation that tries to account for practices such as these that prevent harmful intrusions into consumers' privacy while also preserving innovative processing practices that could utilize such information responsibly without posing risks.
 - That being said, do the witnesses have any policy recommendations for the Committee as it relates to effectively defining technical criteria for “aggregated” and “anonymized” data, such as requiring companies to publicly commit that they will refrain from attempting to re-identify data to a specific individual while adopting controls to prevent such efforts?

19. Consumer data has tremendous benefits to society, as is clearly evident in the fight against the COVID-19 outbreak. Big data and the digitized processes and algorithms that technology companies are developing have led to an entirely new sector of the global economy.

Ms. Stacey Gray, Senior Counsel, Future of Privacy Forum

- Are you satisfied that the technology industry is striking an appropriate balance between producing services that better our ability to solve problems, as is clear in the fight against COVID-19, versus their production of products that increase their bottom line and generate profit? Are you satisfied that the United States government is striking an appropriate balance between supporting these companies in addressing COVID-19 versus ensuring we conduct adequate oversight of the industries' activities?
20. Consumer trust is essential to both the United States government and to the companies whose products we use every day. We need to work to maintain that trust and ensuring that the big data being used to analyze the COVID-19 outbreak was collected and processed in a manner that aligns with our principles is important to my constituents.
- How can we adequately ensure that the data being used to address COVID-19 is sourced and processed in a manner that ensures consumer trust is not being violated, while allowing the innovation and success we've seen continue to grow?
21. It is important to remember that the internet is a global network and that no matter how secure we make our networks, they remain vulnerable to bad actors, corruption, and misguided influence from around the world. Can you comment on the practices we've seen used by companies and international partners to ensure the data used to address COVID-19 is both accurately sourced and stored in a manner that is secure?

Sen. Blackburn

It's time that we align consumer expectations with reality. That holds true whether we are discussing the latest in wearables or the hot new videoconferencing app that helps people work remotely. Consumers have a reasonable expectation that their information will be kept private, and that the platforms they interact with will maintain adequate levels of security to bolster that effort.

We need to pass federal privacy legislation to set a national standard that will allow companies to innovate while protecting consumers. HIPAA was not designed to work with 21st century systems, yet consumers expect that all of their health-related information will be protected by those same standards. I'm afraid that the COVID-19 pandemic will only exacerbate these issues. Corona points out the need to update HIPAA, not to allow tech companies to exploit a crisis to gather even more personal data.

22. How do you see HIPPA interacting with your worldview of the tech industry?
23. How do you envision working with the CDC to develop the updated surveillance system (which was given \$500 million in the recently passed CARES Act) while protecting health information and thereby allow CDC to use their expertise – epidemiology that inherently seeks to protect health information – with big tech's powerful data collection and analysis tools?

Ms. Stacey Gray, Senior Counsel, Future of Privacy Forum

24. Today we are giving into state surveillance for the sake of saving thousands of lives that might otherwise be lost to coronavirus. The CDC is already relying on data analytics from mobile ad providers to track the spread of the disease. How can we ensure the data collection will only be done for the limited purposes of the emergency, with safeguards to ensure anonymity? On retention time, when should the data be deleted? Who has the right to that deletion – the federal government or the individuals themselves? Most importantly, what duty do tech companies owe to protect consumer privacy, even during a global pandemic?
25. Foreign countries like South Korea, Taiwan, Singapore, and Israel swiftly mobilized collection of cell phone location data to track the spread of the virus and map out infection hot zones. Israel just released an app that allows the public to track whether they have may visited a location that put them into contact with an infected individual. Is it even possible to adopt similar measures while still balancing protections for privacy and civil liberties?

Sen. Capito

26. If the government were to utilize a combination of public and private consumer data to create a COVID-19 Public Health Initiative, what barriers to implementation could arise with a patchwork of State privacy laws?

Sen. Lee

27. To date, what specific data (or types of data) are companies (or your company) currently collecting for COVID-19 related purposes? What specific data (or types of data) are governments and health officials seeking for COVID-19 related purposes?
28. Most tech companies currently claim that the data being gathered is being “anonymized” so that a specific person is not identifiable.
 - What specific steps are companies (or your company) taking to anonymize this data?
 - Certain data may not necessarily be considered personally identifiable, but with enough data points, you could identify a specific person. How can we ensure that data is truly anonymous and is not traceable back to an individual person?
 - Can effective contact tracing be conducted with “anonymized data”? Or will it require personally identifiable information?
29. Since the beginning of this COVID-19 crisis, has a federal agency, a state government, or local government requested a company or association to gather any specific consumer data?
 - To your knowledge, are there any current COVID-19 related data sharing agreements in place between governments and private sector organizations? To your knowledge, has any federal, state, or local law enforcement used private

Ms. Stacey Gray, Senior Counsel, Future of Privacy Forum

sector collected data to enforce any COVID-19 related government orders or requirements?

30. Ms. Gray, throughout your testimony you emphasize that the commercial data collected should be limited to data requested by public health officials. What line(s) should be drawn as to what type(s) of data should not be obtainable by public health officials? What underlying principles should inform the drawing of those lines?

Sen. Johnson

31. How does the pandemic shift the landscape for crafting and passing legislation? What would you say are the top 3 principles for striking the right balance between using consumer data for good during the pandemic and ensuring consumer's privacy rights are not violated? What do you see as the #1 priority (as far as using big data for COVID response) in a federal privacy bill? How do we ensure that pandemic-related data privacy provisions sunset appropriately?

Sen. Scott

32. For months, Communist China lied about the Coronavirus data, the spread of the virus, and their response. They silenced critics and those trying to alert the Chinese people to this public health crisis. The lack of usable data coming out of Communist China cost lives and put the world behind on response efforts, including here in the United States.
- As we work to keep American families healthy, how can we follow the lead of countries with low case counts, like South Korea, using technology and data collection, without infringing on our citizens' rights and privacy?

Ranking Member Cantwell

33. Science and technology will be critical drivers of our response to COVID-19, and we have seen many examples of data being used in positive ways – from the University of Washington's forecasts of hospital needs to Johns Hopkins' maps of disease spread. These are leading examples of how firms can innovate while protecting other equities, like privacy.
- What recommendations do you have to encourage further innovation to fight the virus? How do we encourage technologists to help people transition to regular life while preparing for future pandemic incidents? What are the best practices you have seen in innovating in the fight against COVID-19 that support privacy rights?
34. Frequently, data used to combat COVID-19 is described as “anonymized” or “aggregated” or “de-identified,” and these terms are meant to convey that data will be used or shared in a privacy-protective manner.
- How do you define “anonymized,” “aggregated,” and “de-identified” data? What are the best practices to ensure that the data remains anonymous?

Ms. Stacey Gray, Senior Counsel, Future of Privacy Forum

Sen. Blumenthal

35. Privacy for America, a coalition of advertising associations including IAB and NAI, have proposed a federal privacy framework that is focused on a set of prohibited data uses, transparency measures, and a limited subset of data rights found under the GDPR and CCPA. However, the Privacy for America framework also provides wide discretion for companies to use particular types of data or engage in particular activities without consent, as well as a self-regulatory safe harbor and broad state preemption.
- Would the Privacy for America framework provide Americans the full set of consumer rights and protections necessary to guarantee the privacy, security, and equitable use of their personal data, and the enforcement regime necessary to deter and punish the misuse of their information? Please elaborate on why or why not.

Sen. Schatz

36. Americans are concerned about the use of their data to track the COVID-19 pandemic, and today's hearing highlights yet another reason why we need a robust federal privacy law. Although many entities are making available anonymized and aggregated data to help officials study and forecast the pandemic, current law is limited in its ability to ensure that companies are protecting their customers' data as they use this data innovate new methods to track the virus's course.

The Data Care Act, which was reintroduced in December, imposes a requirement on companies that they not use customers' data in a manner that is harmful to those customers. This will ensure that companies carefully balance the reasonable expectations of their customers about the use of their data with other important interests.

How should we balance important prospects for using consumer data to address pressing public health concerns with protecting the privacy of individuals?

Sen. Markey

37. After reports emerged that federal government officials are engaging with technology companies to consider using location data collected from Americans' smartphones to track the coronavirus, I wrote a letter to the White House Office of Science and Technology Policy demanding answers about any plans it has to leverage information about individuals' location. Since then, new reports have emerged indicating that the Trump Administration is considering creating a vast surveillance network that may include health data relevant to the coronavirus pandemic. In response, I wrote to the White House with questions about this proposal and its potential to infringe on individuals' privacy. I urge this Committee to include meaningful transparency requirements for federal projects or partnerships that use individuals' location data or health data in any upcoming coronavirus legislation. Such requirements should apply to both the federal government and whatever private companies participate. And they

Ms. Stacey Gray, Senior Counsel, Future of Privacy Forum

should apply to the use of anonymized or aggregated data in addition to data that is linked to individuals.

- Ms. Gray, do you agree that at the very least the public and experts should know what types of data the federal government is using—either on its own or in partnership with private companies— during this crisis, what form that data is in, and how the federal government is using that data?

Sen. Peters

38. The one thing that has been absent from this discussion is that neither the federal government nor the private sector have adequately anticipated nor met the demands for personal protective equipment. Even basic things like masks and gloves have been inaccessible. Our nation has unparalleled resources in the supply chain and manufacturing space.

- From a data perspective—where have failures been and what improvements do you recommend?

39. Despite many structural challenges, Taiwan has fared better than many countries in dealing with the COVID-19 pandemic. Stanford Medical School documented 124 distinct interventions that Taiwan implemented with remarkable speed including community initiatives, hackathons, etc. Their “Face Mask Map” a collaboration initiated by an entrepreneur working with government helped prevent the panicked buying of facemasks, which hindered Taiwan’s response to SARS by showing where masks were available and providing information for trades and donations to those who most needed them, which helped prevent the rise of a black market.

- What specific initiatives like this should we be implementing here?

Sen. Baldwin

40. Emerging reports from many localities demonstrate that COVID-19 is having a disproportionate impact on African Americans and communities of color. For example, in my home state of Wisconsin, Milwaukee County reports that approximately 70% of those killed by coronavirus are African American, despite that community making up only 26% of the county’s population.

We know this about Milwaukee County because the local government is proactive about collecting and reporting data on race and ethnicity. Reporting indicates that this disproportionate impact exists in places with significant African American communities, including Chicago, New Orleans, and Detroit. But a lack of consistent, quality data nationwide means we do not yet know just how sizable this disparity is, and what we can do about it.

While I am encouraged that we are drawing on the massive amount of data about Americans held by the private sector to support the COVID-19 response, I worry that it may not include and represent all communities equally. For example, if we use mobility data from mobile phones or particular apps to inform our understanding of adherence to

Ms. Stacey Gray, Senior Counsel, Future of Privacy Forum

social distancing requirements, I am concerned how it might affect the usefulness of the dataset if members of certain minority communities less likely to own such a device or utilize such an app.

- For the members of our panel: how do you think “big data” can support efforts to strengthen our public health knowledge around COVID-19 and race, and how can we ensure that the methods and models through which “big data” supports our understanding of the epidemic take into account differences among communities?

41. I am also concerned about the impact of “big data” informing our COVID-19 response on rural communities. Again, I worry that some of these data sources may not be well-utilized in rural America – where connectivity is still a significant challenge – and thus may not reflect the reality of the pandemic in those communities. But I recognize that this information is vital to developing better predictive models that can inform our current response to COVID-19 and help us prepare for the future.

- For the members of our panel: how does “big data” ensure that the different experiences of rural, suburban and urban communities are taken into account when informing models that may guide the COVID-19 response?

42. It is important that public health, and local public health departments in particular, have the data they need to map and anticipate hotspots for infectious disease outbreaks such as COVID-19 or overdose patterns in a community, including data that may be generated by the private sector. It is also important that local health departments have the capability to leverage this information together with that available through traditional public health surveillance efforts.

- For the members of our panel: how can the private sector coordinate data efforts with public health and ensure that local health departments have the necessary capabilities to make full use of these efforts?

43. In speaking with experts in Wisconsin working on developing and refining predictive models around COVID-19, I heard that while there is a significant number of both public sector and private sector data sources to inform models, the data is not consistently easy to obtain and incorporate. As we rely on real-time models to inform the COVID-19 effort, as well as look to prepare for future infectious disease outbreaks, it is important that data-sharing be as seamless as possible.

- For the members of our panel: what are ways we can strengthen the data-sharing infrastructure for government, public health, academic and private sector sources?

Sen. Sinema

44. This virus affects communities across our country. If a small community reports a single positive case, it is important to both inform the community and protect the privacy of the infected individual. Technology can play a role in helping us map the virus, but it is more difficult to sufficiently anonymize personal health data in smaller populations.

- How do we ensure public health officials in underserved and unserved communities, especially in rural communities and Indian Country, are able to provide first responders and EMT dispatch with valuable information about the

Ms. Stacey Gray, Senior Counsel, Future of Privacy Forum

potential for exposure when firefighters or local law enforcement are responding to a call, while maintaining patient privacy?

45. Some states, including Arizona have limited testing capabilities and therefore limited testing. It is also widely reported that tests around the world have produced inaccurate results. How can we mitigate against inaccurate assumptions related to disease trends in situations in which we have limited or inaccurate data?
46. Many point to travel as a key factor in the spread of COVID-19. Contact tracing for travelers, specifically by plane, is a mechanism that can slow the spread of the virus. The data collected (full name, address while in U.S., email address, and two phone numbers) enables the government to contact individuals who may have come into contact with an individual who has tested positive. Once contact is established, individuals can start self-quarantining.
 - What is the best way to balance the need for this information to slow the spread of the virus and privacy rights?
47. How can big data help resolve challenges within the manufacturing supply chain to spur increased production and distribution of needed testing, personal protective equipment, and other resources to address this pandemic?
48. This pandemic has caused serious economic harm. Businesses of all sizes and their employees suffer as sales drastically fall or disappear altogether. State, tribal and local governments are under enormous strain as response costs increase and revenues drop.
 - How can big data assist in the better creation and execution of economic assistance programs like the Paycheck Protection Program, Treasury's lending facilities, business interruption or pandemic risk insurance, and state, tribal and local stabilization funds?

Sen. Rosen

49. Germany's national disease control center recently asked their citizens to donate data collected by their fitness tracker. This voluntary initiative has consumers download an app on their phones and contribute health information such as pulse rates and temperature that is collected by fitness tracking devices anonymously. Using machine learning, epidemiologists can analyze this data to better understand the spread of the coronavirus across the country and detect previously unknown clusters.
 - What are the advantages and pitfalls in using voluntarily donated data to improve responses during a pandemic?
 - How can we use donated data to support our response to this pandemic and future similar public health issues?
 - What privacy guardrails are needed to ensure that this data is collected and analyzed safely and anonymously?
 - What are the gaps we need to consider when analyzing such data?

Ms. Stacey Gray, Senior Counsel, Future of Privacy Forum

50. The National Science Foundation (NSF) is the only federal agency whose mission includes supporting all fields of fundamental science and engineering. The research and educational programs backed by NSF are integral to the continued success of our country's innovation, supporting scientific discoveries that have led to new industries, products, and services. Since 2012, NSF has funded research on the emerging field of data science through its BIG DATA program. Now, NSF's larger program – "Harnessing the Data Revolution" – will support research, educational pathways, and advanced cyberinfrastructure in the field of data science.
- Given NSF's leadership in data science research and development, what role do you think NSF can play in leading public-private partnerships for increased research on big data that could help address the COVID-19 crisis or future pandemics?