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?

   As we highlighted in our testimony, the NAI believes that the COVID-19 Mobility Data Network (the "Network") provides an excellent example of a program that effectively balances utility for public health with individual privacy protections. The Network is a group of infectious disease epidemiologists at universities around the world working with technology companies to use aggregated mobility data to support government responses to the COVID-19 pandemic.

   The Network uses anonymized, aggregated location data sets from mobile devices to provide decision-makers at the state and local levels with daily updates on how well social distancing interventions are working, as well as analytic support for interpreting the location data. The Network is powered by a working partnership with multiple companies. Through direct connections with public health authorities at the city, state, and country-level, the Network provides tools that offer timely insights into the effectiveness of social distancing measures, a way to identify potentially high-risk zones, and assistance for planning the roll-back of restrictions.[1]

   The Network is also supporting government efforts to manage and adapt public services for the COVID-19 pandemic. For example, information supplied by the Network can help officials understand changes in essential trips that can then shape recommendations on business hours or inform delivery service offerings. Similarly, transportation hubs that continue to experience high traffic might indicate the need to add additional buses or trains in order to give essential workers who need to travel more space for social distancing. Ultimately, understanding not only whether people are traveling, but also

[1] For more information about the Network, see https://www.covid19mobility.org/.

trends in destinations, can help officials protect public health and provide for the essential needs of communities.[2]

However, the location and movement insights provided by the Network to public health authorities are not invasive to individual privacy, because participants in the Network adhere to the following principles that reflect their mutual commitment to privacy and data protection:

1. The use of data, including data sharing, aggregation, and analysis, for Covid19 response must speak to a clear need articulated by public health authorities, and for no other purpose.
2. The use of data must both be in compliance with existing laws and adhere to best practice principles of data governance.
3. Data should be aggregated to the lowest feasible resolution possible while maintaining its desired utility.
4. The use of data must be transparent, inclusive, and safeguarded against unintended consequences.[3]

In addition, NAI member companies have contributed aggregated or de-identified data sets to local governments and researchers to aid them in their efforts to identify when social distancing guidelines are being effectively implemented or to determine if additional restrictions would help stop the spread of COVID-19. These data sets protect user privacy by virtue of their aggregation; recipient researchers do not have access to user level data.

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 combating COVID-19 can also respect individuals' privacy?

   The NAI supports efforts to use data-driven science to fight the spread of COVID-19, and we are proud to have member companies who are contributing to this fight to protect American lives, to minimize the impact that stay-at-home orders are having on our

[2] Buckee, Caroline O., et al. "*Aggregated Mobility Data Could Help Fight COVID-19.*" *Science*, American Association for the Advancement of Science, 23 Mar. 2020, science.sciencemag.org/content/early/2020/03/20/science.abb8021.

[3] Id.

economy and the well-being of many Americans, and to implement and evaluate measures to limit the spread of COVID-19.

Privacy and beneficial uses of data are not mutually exclusive, broadly or in relation to efforts to combat COVID-19. As we highlighted in our testimony, if the data is shared in aggregate, de-identified or anonymized form, and use limitations are put in place, an effective balance can be reached between achieving desired public health outcomes and maintaining individual privacy. We expand on some of these policies and practices in greater detail in some of the following questions.

Regarding the granularity of personal data used to fight COVID-19, more granular data in some circumstances present greater risks to individual privacy, but this is not always the case. Regardless of the granularity of the data at issue, technical and administrative safeguards should be implemented to ensure that data -- whether granular or aggregated -- is not linked back to an individual.

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?

A federal law's potential effect on our efforts to use data to combat the spread of COVID-19 depends on data prohibitions or use restrictions contained within. With respect to a public health emergency like the current pandemic, it would be useful to analyze the location data of given devices and the devices they come into contact with over a given period of time. If a federal law contains an outright prohibition on the collection of such data, then it would not be available for this or any other purpose. If it discourages the collection of such data, then less of it would be available. This situation highlights two important issues. One, data is useful for multiple purposes so collection itself should not be banned; and two, not all data uses are acceptable and distribution of information, if sensitive, should be aggregated and de-identified to the greatest degree possible.

The NAI feels strongly that a U.S. national data privacy law should take these lessons into consideration and is necessary to provide additional clarity, consistency and certainty around responsible and acceptable uses of consumer data, including for public health purposes. As demonstrated by this hearing, policymakers and companies are working in real-time to develop best practices in the absence of clear federal standards. In addition, we are concerned that different approaches and definitions in state laws could raise challenges for companies to develop innovative data uses for fighting public health emergencies. The NAI is proud that its Code of Conduct serves as a foundation for our members and other companies to be good stewards of consumer data. But in order to apply these principles uniformly across all companies and sectors of the economy, particularly during times of crisis, a national data privacy law is essential.

Specifically, the NAI is a founding member of the Privacy for America coalition, and the model framework we developed would be instructive in this context. Privacy for America's framework fundamentally changes the way personal data is protected and secured in this country. It clearly defines and prohibits practices that put personal data at risk or undermine accountability, while preserving the benefits to individuals and our economy that result from the responsible use of data. The framework applies to virtually all companies doing business in the United States, and to all personal information, whether collected or inferred, that is linked or can reasonably be linked to a particular individual or device.

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' express consent. 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.

Lastly, the framework calls for substantially increased resources at the Federal Trade Commission (FTC), including the creation of a new Bureau, to ensure that the federal government has the tools, knowledge, and public servants necessary to tackle these challenging and complex technical and ethical questions. The FTC would play a pivotal role by enforcing the framework against any misuse of data, particularly data used in connection with a public health emergency.

We believe Americans' personal information – especially their most sensitive data – deserves protections that are far broader and stronger than those that exist today. We believe that Congress should act expeditiously to pass comprehensive legislation that delivers those consumer protections, thereby enhancing consumer trust in an ecosystem that is dependent on data for societal good, as in the current circumstances.

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?

As we highlighted in our testimony, the NAI encourages the use of anonymized, de-identified, and aggregate location data where practical to protect consumers' privacy. Anonymized or de-identified data is not linked or intended to be linked to an identified person or device, mitigating privacy risks. Aggregate data refers to a data set that refers only to population-level data and does not present any appreciable privacy risk to individuals.

Still, the use of de-identified, anonymized, or aggregate location data should be supplemented with organizational and technical measures to prevent identification, or re-identification, of any individuals through whom such data were obtained. This is particularly important for sensitive data such as location information. Some companies use privacy-enhancing technologies like differential privacy to further minimize the risk of individuals being identified.[4] In addition, aggregate data sets used for public health purposes should be interrogated for factors like bias, accuracy, and the kinds of decisions that may be made based on aggregate data. These aren't privacy concerns per se, but it's important to think about ways to maintain trust with consumers by taking steps to ensure that outcomes based on, e.g., the aggregate use of location data originating from their mobile devices will be fair, transparent, anonymous, and won't harm them.

Also, in order to maximize privacy and consumer choice, it is critical to gain consent from individuals for collecting Precise Location Information or other sensitive data. To this end, the 2020 Code also reinforces the requirement that consumers must have clear, timely notice about the reasons why Precise Location Information is being collected, and with whom it will be shared. In addition, such notices should include information on the anticipated use of the data, which could include research and/or public health. This allows consumers to make informed choices about whether to allow data from their mobile devices to be used and shared for those purposes. NAI members are also part of a larger ecosystem of companies that utilize data in their business models, and by adhering to best practices and standards for responsible data collection and use, NAI member companies encourage networked compliance to such standards by business partners and other participants in the ecosystem.

Beyond the technical and organizational measures private companies can take to prevent malicious actors from identifying or reidentifying people where they should not, law can dramatically increase the penalties for doing so.

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**

[4] Google is an example of a company that uses differential privacy. *See* Google Developers, "Enabling Developers and Organizations to Use Differential Privacy", September 5, 2019, https://developers.googleblog.com/2019/09/enabling-developers-and-organizations.html.

identifiable data, if applicable – collected by technology companies and the government for the purpose of addressing the public health crisis

Robust purpose limitations should accompany any use of consumer data for purposes of fighting the COVID-19 pandemic, particularly where the data was not originally collected for those purposes. Consumers should have confidence that even though aggregate location data sourced through their mobile devices may be used to help in a public health emergency, it will not be retained or used by government or other entities after that emergency purpose has been achieved. We encourage NAI member companies who are making any kind of advertising or marketing data available to help with this crisis to condition the use of that data on the prohibition of any secondary uses of the data by the recipient, and on a strict data retention period.

It's important to note that purpose limitations have value for sensitive data, such as data related to precise location or health. But aside from the current COVID-19 crisis, there are many opportunities where data in various degrees of de-identifiability, or aggregated data, can be used for other societal benefits, some of which may be unforeseen. Thus, purpose specification makes sense for sensitive data used in sensitive wats, but transparency may be a stronger principle for addressing more benign, unforeseen, but yet beneficial uses. Context is a crucial component of this analysis.

NAI member companies that collect properly-permissioned information from mobile devices for advertising purposes may continue to use the information for those purposes, consistent with applicable privacy disclosures to consumers, contractual obligations, and applicable laws and regulations.

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?

   Zoom Communications is not a member of the NAI and we are not in a position to comment on the adequacy of their consumer privacy disclosures. However, the NAI strongly believes that organizations must be transparent about the types of information they collect from consumers, why they collect it, and how they use or disclose it, particularly when used to make decisions about the individual. These principles are the foundation of our Code of Conduct.

The NAI is concerned about the development of a patchwork of consumer privacy laws. This approach would not serve the best interests of consumers, who would receive varying levels of privacy protections depending on where they live. It also would be burdensome to U.S. businesses and our economy, increasing compliance burdens and cost, and stifling innovation. For these reasons, we strongly support a national privacy framework that would establish a single set of general consumer privacy rules for the United States, and establish a clear set of rights and controls for consumers regardless of their state of residence.

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?**

Congress should enact a comprehensive federal privacy law to help ensure that all businesses adopt reasonable data minimization and retention practices that will enhance consumer data protection.

Regardless of whether a comprehensive federal privacy law is enacted in the United States, companies can, and should, demonstrate their commitment to good data stewardship by following rigorous self-regulatory principles governing data collection and use, like those established by the NAI Code, and subjecting themselves to accountability procedures to promote compliance. The NAI's own program is an example of an industry recognizing the need for strong self-regulation, and which requires broad agreement across many different market actors, some who are competitors to each other, working together to resolve an issue that is in the best interest of the industry, and society, as a whole. The NAI conducts an annual review of every member company's compliance with the NAI Code which includes specific questions that reveal what data is collected, how it is collected and used, how it may be shared, what measures are taken to minimize the data retained by members, and whether the data is protected. The requirements of the NAI Code and associated best practice recommendations shared with member companies by our compliance staff, include limiting consumer data access by company employees and restricting the use of data after it is no longer necessary for business operations. All entities that use consumer data should treat privacy as a foundation for their development or use of technologies and products, including privacy training and oversight. NAI obligations such as limits on data retention and the requirement to maintain reasonable data security (among others) are fundamental practices that ensure responsible data use and the protection of individual privacy.

However, as you identify, not all companies are required by law to adhere to data privacy principles like those required by the NAI Code. For this reason, the NAI strongly supports the establishment of a uniform national privacy law to ensure that all companies are held to a common set of requirements and standards. Specifically, we strongly support the Committee's discussion draft legislation that would establish FTC-certified compliance programs establishing industry specific standards and best practices to provide needed assurances of industry-wide accountability.[5]

8. **The country of Israel, through its internal security service, has reportedly used smart-phone 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 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.**

The use of data by public health agencies and academic researchers to study health outcomes and track diseases is not new, nor is it unique to the United States. In response to the health and societal threats posed by the pandemic, governments around the world are considering whether and how to use mobile location data to help contain the virus. However, the success of such measures in "flattening the curve," or preventing the spread of the virus, or for other critical purposes, will likely be unknown for some time, and recent reports suggest that some of the benefits initially anticipated may have been overstated.[6]

One factor in effectiveness is whether participation in data collection is mandatory or voluntary. As we have noted, the NAI Code requires consent for collection of precise location data, but if large numbers of people do not consent, the public health value is reduced. Mandatory approaches raise civil liberties concerns, and perhaps getting consent has much to do with trust, transparency, and good design. A second factor is the efficacy of the data. Contact tracing, for example, requires extremely precise data beyond the collection abilities of many companies or technologies. There is little point in raising privacy concerns over data that is of limited value.

The NAI does not have deep expertise in public health matters. Rather, we look to guidance and input from a broad range of public health experts to understand which practices could be most effective to stop the spread of the coronavirus, and perhaps more importantly, the insights that we have the greatest need to derive from data. Often, sharing insights and analysis from raw data, rather than sharing the data itself, is more effective in producing desired outcomes.

[5] *See* Senate Commerce, Science and Transportation Committee staff discussion draft legislation at 3 Sec.403.Approved certification programs.

[6] *See* Nile Bowie, *Cracks Show in Singapore's Model Covid-19 Response,* Asia Times (April 7, 2020), https://asiatimes.com/2020/04/cracks-show-in-singapores-model-covid-19-response/.

We agree with your assessment that location based contact tracing potentially presents significant privacy and civil liberty concerns. For these reasons, it is a critical best practice for all companies and governments to use aggregate, de-identified or anonymized data where possible. Government entities, health organizations and companies must continue to balance the opportunities to achieve positive outcomes for society as a whole, with protecting consumer privacy.

- **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.**

The NAI has limited knowledge about the effectiveness of contract tracing. However, if this technology is to be adopted in the United States, the NAI agrees that it should be done on a voluntary basis, where transparency and consent are critical for ensuring that consumers can weigh for themselves the benefits and privacy risks. Apple and Google recently announced that they are launching a comprehensive program that allows for contact tracing while maintaining strong protections around user privacy. This first of its kind program involves a phased approach; first, the release of APIs that enable interoperability between Android and iOS devices using apps from public health authorities. These official apps will be available for users to download via their respective app stores. A second step in the coming months will enable a broader Bluetooth-based contact tracing platform that builds this functionality into the underlying platforms. The initiative is intended to maximize the participation and effectiveness for individuals who choose to participate, as well as enable interaction with a broader ecosystem of apps and government health authorities.[7] Following are the key privacy protections that are built into the joint technology solution:[8]

- Explicit user consent required
- Doesn't collect personally identifiable information or user location data
- List of people you've been in contact with never leaves your phone
- People who test positive are not identified to other users, Google or Apple
- Will only be used for contact tracing by public health authorities for COVID-19 pandemic management

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.**

[7] *See Apple and Google Partner on COVID-19 Contact Tracing Technology*, Google Blog (Apr. 10, 2020), https://www.google.com/url?q=https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/&sa=D&ust=1586806797088000&usg=AFQjCNGV3tv8m6B_HuyQrWDJRRDxMqYfEQ.

[8] see https://www.blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing_Using_BLE.pdf

- **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?**

The NAI is not currently familiar with these websites and the proposed procedures to enable user self-screening. However, as highlighted in the joint announcement on April 10th, the companies are committed to balancing the goal to help health agencies and governments fight the spread of the virus, with privacy and security features.[9] The NAI looks forward to learning more details about this initiative in the near future.

- **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?**

With respect to safeguards to ensure that data collected for combatting COVID-19 is not used for other commercial purposes, the NAI strongly recommends that companies that develop these tools specifically to respond to COVID-19 do so with the NAI Code in mind. The Code has specific requirements for the sharing of data with business partners, and those requirements can help companies develop best practices for specific the collection and use of COVID-19 specific data, including:

- Appropriate Due Diligence - The NAI Code requires members to take steps to ensure the data they receive from third parties for Tailored Advertising or Ad Delivery and Reporting comes from a reliable source, including performing due diligence, implementing privacy questionnaires, and reviewing a company's marketing materials and privacy policies to ensure appropriate notice and choice mechanisms are in place.
- Downstream Data Restrictions - The NAI Code requires that members contractually prohibit any third parties with whom they may share data in a non-personally identified form from attempting to re-identify the data.
- Data Retention Policy - The NAI Code requires that member data only be retained so long as there is a legitimate business purpose. The Code further requires that members explicitly state how long this retention period may be. However, we recognize that at this time it may be difficult to determine what that period may be for combatting COVID-19.
- Data Use Restrictions - The NAI Code prohibits members from using data, or allowing data that has been collected for Tailored Advertising or Ad Delivery and Reporting purposes to be used for any non-marketing eligibility purposes. Such a requirement would fit well with current efforts to prohibit data collected for combatting COVID-19 to be used for separate commercial purposes.

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.**

[9] *See Apple and Google Partner on COVID-19 Contact Tracing Technology*, Google Blog (Apr. 10, 2020),

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?

Anonymized data is commonly recognized to be data that cannot be reasonably linked back to a specific individual. While there are different techniques for anonymizing data, the outcome is to effectively limit the possibility of tying data back to a specific person.[10] In an era of big data, super computers and highly sophisticated hackers, even using sophisticated anonymization techniques cannot completely prevent the possibility of anonymized data being associated with an individual. For this reason, it is necessary to also incorporate technical and administrative controls that protect against this unintended outcome, like strict data usage limitations, data minimization practices, employee training, and data retention restrictions.

The NAI Code guides member companies sharing data with others by, first, restricting member companies themselves from linking or merging De-Identified Information with Personally Identified Information without a user's express Opt-In Consent. Second, companies are required to contractually prohibit any parties with whom they share data from attempting to link or merge this data in a way that would identify an individual., thereby networking trust in data sets to downstream data partners.

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.

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

[10] *See ,e.g., Google Covid-19 Community Mobility Reports: Anonymization Process Description*, Cornell University, (last revision Apr. 9, 2020), https://arxiv.org/abs/2004.04145,

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?**

    As we highlighted in our testimony, while our Code of Conduct and associated accountability program are designed to govern the collection and use of data for advertising and marketing purposes, the principles established by the Code, including transparency, user choice and data use restrictions, also provide a privacy-protective foundation for any companies seeking to utilize data to promote societal benefits, such as mitigating the harmful outcomes of the deadly COVID-19 pandemic. As a best practice for upholding the highest standards for individual privacy and security, the NAI recommends that public health officials, researchers and other government entities ensure that the commercial entities providing data are subject to appropriately strong industry specific self-regulatory requirements and accountability measures that ensure their compliance.

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?**

    The utility of data depends largely on the objectives of its use. As discussed in our testimony and throughout our answers in this document, there are a range of valuable uses of data that is aggregate, de-identified or anonymized. With respect to efforts by public health officials to combat COVID-19, there is a strong case for relying only on anonymized and aggregate data to achieve many useful outcomes while minimizing privacy risks.[11]

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.**

    Are there any technologies that offer the opportunity to collect data that would be useful to a governmental pandemic response efforts, without resorting to surveillance methods that jeopardize individual privacy – like those which have been used recently by foreign governments?

    Public health officials and researchers are eager to put aggregate and anonymized data to use to help model and track the spread of the novel coronavirus. Rather than resort to collecting information on their own, much of this data can be gleaned from location-based features offered by mobile devices and apps that have been collected for

[11] *See*, e.g., *Aggregated Mobility Data Could Help Fight COVID-19*, Science Magazine (Apr. 10, 2020), https://science.sciencemag.org/content/368/6487/145.2.

commercial or other purposes.[12] The NAI strongly recommends that commercial companies employ privacy-protective measures to collect such data prior to sharing it with researchers, including consent flows, anonymization and de-identification techniques, and aggregation of any user level data. Additionally, as highlighted above in response to previous questions, companies, including NAI members, are introducing initiatives to attain additional data on a voluntary basis.[13] This approach, in many ways, is beneficial for mitigating concerns about government collection of data because it relies on partnerships and contracts that can be structured to limit the use of the data by public health officials or other government entities for pandemic-related solutions.

Sen. Cruz

14. **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?

    The NAI does not have expertise in public health matters, particularly the opportunities and viability of applying big data analytics to effectively forecast the spread of infectious diseases. We look forward to learning more about the opportunities and whether location data provided by NAI members could be effective in stopping the spread of the coronavirus or other infectious diseases.

15. **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**

[12] Location-based features are one of the key benefits offered by mobile devices and applications. Those features include customized local weather forecasts, integrated mapping technology, and the collection and use of location data to provide Tailored Advertising. In most cases, location data collected through mobile applications is shared with partners, such as NAI member companies, in order to provide tailored ads to users and for business analytics purposes. The revenue generated from those ads and analytics allow consumers to enjoy the use of those applications for free or for a lower cost. The collection of location data is usually accomplished through the use of Software Development Kits (SDKs), or software code integrated into the application.

[13] *See Apple and Google Partner on COVID-19 Contact Tracing Technology*, Google Blog (Apr. 10, 2020), https://www.google.com/url?q=https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/&sa=D&ust=1586806797088000&usg=AFQjCNGV3tv8m6B_HuyQrWDJRRDxMqYfEQ.

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?

Balancing positive outcomes, whether commercial or societal, with individual privacy and security protection is the core of the NAI's work, as well as its Code. We believe it is crucial to incorporate administrative and technical controls, such as data minimization, data use limitations, employee training, and strict data retention periods to help limit risks to privacy. We also strongly encourage both governments and private sector companies to utilize de-identified or aggregated data whenever possible. Finally, we strongly urge Congress to enact a comprehensive federal privacy and data protection law that applies to all companies and data uses, with strong protections for individuals, to engender trust in big data utilization, not only for public health but also for commercial and other uses. We look forward to the opportunity to comment on specific programs in the future.

16. **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?

    The NAI does not have expertise in public health matters. Rather, we look to guidance and input from a broad range of public health experts to understand what's most useful in terms of data usage, and perhaps more importantly, the insights that we can derive from the data provided. We are proud of our member companies that have stepped up to help in this unprecedented fight, not only by sharing data for valuable insights and analysis, but also to help Americans by delivering important public health messages, and by donating dollars, time, and services to those most in need.

    NAI member companies are donating their technologies to emergency response teams, call centers, and care management teams to maximize their limited resources, and creating online communities for researchers to collaborate and share insights on the fight against the pandemic, as well as providing aggregated data sets to their business partners to help them make operational decisions. They are also engaging in activities such as providing unlimited mobile data to customers, waiving fees, and donating data to public schools to help with distance learning. Finally, member companies are helping our communities fight the novel coronavirus by doing what they do best - advertising. They are serving public service advertising campaigns (PSAs) to help stop the spread of COVID-19, donating ad inventory to help raise awareness and mobilize resources related to mental health and public response efforts,[14] and donating graphic design and marketing services to organizations like the CDC to help promote the importance of staying home to reduce the spread of coronavirus.

NAI member companies form the backbone of digital advertising, an industry that has helped power the growth of the Internet by subsidizing the content and services Americans expect and rely on, including video, news, music, and more, and by underwriting the creation of innovative services and technologies that connect individuals and businesses.[15] Now, more than ever, Americans are dependent on trusted news sources for our collective understanding of this unprecedented threat and how governments and companies are addressing it, and on the connectivity and communication technologies that digital advertising has enabled. The digital content and tools that have become essential for all Americans during this crisis are dependent upon advertising to survive.

Like many industries, the digital advertising industry has been negatively affected by this pandemic. Despite the fact that more of us are online than ever, advertisers are drastically cutting ad spend, particularly in those sectors that have been most affected. This has caused disproportionate economic damage to news outlets. We would urge Congress to consider addressing support for this sector in upcoming relief efforts.

As we look ahead to brighter days, and the potential re-opening of American businesses, we would note the critical role advertising plays in a recovering economy. The NAI and our member companies look forward to serving the American people by getting back to what we do best - supporting critical online content and services by serving the advertising campaigns that will be vital to a full resurgence of our strong American economy, and to doing so with respect and appreciation for consumers that our so important to our recovery.

Sen. Fischer

[14] *See, e.g.*, David Cohen, *Verizon Media Donates $10M in Ad Inventory for Mental, Public Health Response to Covid-19*. AdWeek (Apr. 14, 2020), https://www.adweek.com/digital/verizon-media-donates-10m-in-ad-inventory-for-mental-public-health-response-to-covid-19/.

[15] NAI's 2019 consumer survey revealed that nearly 60% of respondents prefer their online content to be paid for by advertising, while another question sought feedback from consumers on how much they currently pay for online content and how much they would be willing to pay. Nearly 90% said they are unwilling to pay a significant amount of money to continue receiving apps and online content that they currently receive for free. The survey provided a strong affirmation that the ad-supported content model is ideal for most consumers. See, Blog | NAI

17. In your testimony, you stated that "aggregated data generally raises few privacy concerns because it represents large groups of people or devices, and isn't easily tied back to any individual," but that "it's particularly important for administrative and technical controls – applied both by companies and passed on contractually to governments, researchers, or other partners – to ensure this data is not combined with other data to link it directly to identifiable individuals." Could you please outline three or four key aspects for these "administrative and technical controls" to protect aggregate data from being linked back to identifiable individuals?

Administrative and technical controls are key components of a company's overall privacy program, and there are numerous methods that can be employed to protect consumer data. While the NAI does not require or recommend specific controls, we strongly encourage companies to employ best-in-class protocols to ensure that data in their possession is adequately protected. Encryption is commonly used as a technical means of data protection, at least for data at rest, because it prevents the data from being accessed at all. In addition, many companies employ data separation; keeping data sets in separate data systems or servers with different access credentials, to prevent unnecessary use or identification.

As for administrative controls, companies should limit data access by staff to only those that have a legitimate business reason for such access. In addition, companies should make sure that staff are properly trained on appropriate data protection practices.

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?

The NAI is a leading industry proponent of a federal consumer privacy standard, and we are grateful for the Committee's efforts to draft and consider legislation. Definitions are a critical element of any such legislation. In order to be effective, regulated personal data must be effectively defined and distinguished from other types of data that pose little or no threats to privacy. The NAI supports an approach that makes a clear distinction between personal data, and anonymized or aggregated data, or other categories of consumer data. We believe our Code exemplifies useful distinctions for many of the objectives of an effective consumer privacy law, and we would also direct you to the definitions provided by the Privacy for America Coalition's legislative principles.[16] Such distinctions allow for the beneficial use of data that pose little to no risk of harm to consumers, while placing strong restrictions, or even prohibitions, on certain uses of personal data, such as social security numbers.

With respect to defining a technical standard for preventing the identification or re-identification of data, this is a complex and evolving science. While there is value in recognizing various practices, it is important to avoid establishing a single standard or set of standards. While this would provide some certainty to businesses, the effectiveness of these standards is limited by the technology and methods that are currently available, and these methods and technology evolve over time, faster than legislation can adapt.

The NAI Code defines de-identified data in reference to what the company processing the data actually does, or intends to do, with it. This avoids prescriptive technical requirements for de-identification (which may quickly become obsolete, as some argue has been the case for the HIPAA safe harbor), and focuses on the actual behavior of the entities processing the data. Therefore, the NAI supports the suggestion that companies taking advantage of special provisions for de-identified data publicly commit that they will refrain from attempts to re-identify such data, and put in place controls to prevent such re-identification.

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. 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?**

The NAI is proud of the NAI member companies that have come forward to offer their innovative technologies and data-driven models to help in the fight against the COVID-19 pandemic, and we believe they have a societal and moral obligation to do so. It is important that we encourage innovation and advancement of technologies to benefit commercial interests and society, and incentivize companies to contribute knowledge, data, and expertise wherever it is beneficial to solve societal problems, such as the current pandemic.

Innovation and technological advancement are at the heart of U.S. economic growth over the last twenty years, and we believe that the government must continue to foster

[16] *See Principles for Privacy Legislation, December 2019,* https://www.privacyforamerica.com/overview/principles-for-privacy-legislation-dec-2019/.

innovation, promote economic growth, and enable the free flow of information, while also ensuring meaningful, market-based competition.

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?

This question assesses the long-standing, critical balance between achieving innovative and beneficial outcomes of data, while preserving privacy. To achieve this balance, there are shared responsibilities between industry and governments. Transparency and control are fundamental pillars for establishing consumer trust, ensuring that consumers are well informed about data collection and use practices and that they are enabled to make choices about the collection of their data and how it is used. To that end, the NAI has been a leader in establishing the base requirements for notice and choice on the internet, as it relates to Tailored Advertising. Further, the NAI has required affirmative Opt-In Consent for collection and use of certain categories of data, such as sensitive health data, sensor data, Precise Location Information, and other sensitive categories (like Sexuality). Most recently, the NAI published Guidance for NAI Members: Opt-In Consent.[17] This document elaborates on the requirements members must adhere to and offers examples for what language the NAI expects a user to see when they grant their consent for the use of Precise Location Information.

In addition to transparency and control, consumers must be able to trust that their data is being used responsibly and in a privacy protective manner. While the Code offers industry-leading guidance on the responsible collection and use of data, it's important to note that not all companies engaged in the collection and use of consumer data are subject to the Code. A comprehensive federal privacy framework would provide clarity and consistency for all companies, and would go far in helping to establish necessary consumer trust in the ecosystem.

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?

Many of NAI's member companies are global, with advertising businesses throughout the world. Because data is crucially important to digital advertising, data security and

[17] *See Network Advertising Initiative, Guidance for NAI Members: Opt In Consent (2019),* https://www.networkadvertising.org/sites/default/files/final_nai_optinconsent-guidance19_final.pdf.

protection are key components of such companies' protocols. Many companies employ best-in-class data security technologies, such as encryption, data separation, and strict data retention and access policies in order to protect consumer data from bad actors. Companies use existing cybersecurity best practices (NIST, CIS controls, etc.), technology methods to protect data sent from the source, and algorithms that preserve the integrity of the data. In addition, it is important to note that many of our companies' international business partners are subject to stringent data protection laws in their own countries, which work to further enhance data security and protection. Public health authorities receiving this kind of data should also commit to purpose limitations and limited retention periods, and implement policies and procedures to ensure adherence to those commitments.

Sen. Blackburn

22. How do you see HIPAA interacting with your worldview of the tech industry?

HIPAA is an important sectoral privacy regulation in the United States and applies to the collection, use, access, and disclosure of Protected Health Information[18] by certain covered entities. This may include, in certain circumstances, researchers and their partners.

While the advertising activities of NAI members are generally not subject to the requirements set forth in HIPAA, our Code of Conduct still includes strong transparency and control provisions related to the use of health information. Regarding individual control, the NAI Code prohibits member companies from using an individual's sensitive health information for many advertising purposes without first obtaining that individual's opt-in consent. And regarding transparency, the Code requires member companies to publicly disclose the health-related audience segments they use.

However, because HIPAA does not apply to a wide range of activities across the technology sector that involve consumer data collected outside of the context of receiving or paying for health care, the NAI also supports a national privacy law that would preserve the protections established by HIPAA and establish additional protections for consumer health data, including a requirement to attain opt-in consent for the collection of sensitive consumer data. Sensitive consumer data could extend beyond HIPAA to include, for example, online health services or inferences about a sensitive health condition health of an individual based on other information obtained from or about that individual.

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 –

[18] "Protected Health Information" is defined as any individually identifiable health information collected by a covered entity related to the past, present or future physical or mental health of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual. *See* 45 C.F.R. § 160.103.

epidemiology that inherently seeks to protect health information – with big tech's powerful data collection and analysis tools?

The COVID-19 pandemic has revealed many challenges with respect to our country's collective approach to combating infectious diseases. Hopefully, the substantial additional funding in the CARES Act will help with both the short-term efforts to combat the current pandemic and ensure the United States, and the world, are better prepared to respond to future outbreaks. With respect to the $500 million that was allocated to improve state and local public health data infrastructure, we expect this to be a longer-term project, but an important one that can better facilitate cooperation and coordination between state and local governments and industry. To that end, we look forward to reviewing requests for information and assessing whether there are opportunities for NAI and our members to contribute our expertise as the CDC leads this initiative, with the goal to engage in collaborative efforts that leverage privacy-protective data sets and analytics capabilities from the private sector to achieve common public health objectives.

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?**

It is an utmost priority of the NAI and our member companies to not only work collaboratively with public health officials and researchers to help stop the spread of the deadly COVID-19 pandemic, and to get Americans back to work in order to support themselves and their families, but also to achieve these objectives while protecting the privacy of individuals. To that end, the NAI agrees that private sector data sharing initiatives should include both meaningful purpose limitations and data retention periods to preserve privacy and protect civil liberties.

Companies sharing data with public health authorities such as the CDC should include a restriction on secondary uses of the data as a condition of sharing it, as well as a requirement that the receiving entity securely delete or destroy the data after it has served the limited purpose it was shared for. These conditions on sharing minimize the risk that the data may be used in other ways that may surprise or harm consumers, even inadvertently. Public health authorities receiving this kind of data should also commit to purpose limitations and limited retention periods, and to implement policies and procedures to ensure adherence to those commitments.[19]

[19] *See Apple and Google Partner on COVID-19 Contact Tracing Technology*, Google Blog (Apr. 10, 2020), https://www.google.com/url?q=https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/&sa=D&ust=1586806797088000&usg=AFQjCNGV3tv8m6B_HuyQrWDJRRDxMqYfEQ.

As we expressed in our testimony, we believe NAI members are well suited to be leaders in privacy-protective cooperative data sharing initiatives because of their reliance on the NAI Code of Conduct as a foundation for data stewardship that promotes the use of de-identified, anonymous or aggregate data sets and to promote responsible practices such as data minimization.

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 may have 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?**

Public health officials worldwide are, rightly, interested in leveraging data to help understand and contain a virus that is so easily spread, particularly among infected individuals who may not have any symptoms. However, the success of such measures in "flattening the curve," or preventing the spread of the virus, or for other critical purposes, will likely be unknown for some time, and recent reports suggest that some of the benefits initially anticipated may have been overstated or not necessarily the ideal approach for all jurisdictions.[20]

Location-based contact tracing potentially presents significant privacy and civil liberty concerns. For these reasons, it is a critical best practice for all companies and governments to use aggregate, de-identified or anonymized data where possible. Government entities, health organizations and companies must continue to balance the opportunities to achieve positive outcomes for society as a whole, with protecting consumer privacy.

Sen. Lee

26. **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?**

Public health officials and researchers are eager to put aggregate and anonymized location data to use to help model and track the spread of the novel coronavirus, much of which can be gleaned from location-based features offered by mobile devices and apps. In most cases, these objectives are specifically seeking to avoid data that could present risks to privacy.[21]

Location-based features are one of the key benefits offered by mobile devices and applications. These features include customized local weather forecasts, integrated

[20] *See* Nile Bowie, *Cracks Show in Singapore's Model Covid-19 Response*, Asia Times (Apr. 7, 2020), https://asiatimes.com/2020/04/cracks-show-in-singapores-model-covid-19-response/.

[21] *See Aggregated Mobility Data Could Help Fight COVID-19*, Science Mag (Apr. 10, 2020), https://science.sciencemag.org/content/368/6487/145.2.

mapping technology, and the collection and use of location data to provide Tailored Advertising. In many cases, location data collected through mobile applications is shared with partners, such as NAI member companies, in order to provide tailored ads to users. The revenue generated from those ads allow consumers to enjoy the use of those applications for free or for a lower cost. Location data collected through mobile apps is also frequently used for business analytics. The collection of location data is usually accomplished through the use of Software Development Kits (SDKs), or software code integrated into the application, sometimes provided by third-party partners to enable key features of the application and to enhance advertising and marketing practices.

Location data collected from mobile apps is generally derived from three sources: GPS (global positioning system) capability built into mobile devices; wifi networks, from which location can be inferred based on proximity; or cell tower location, whose main function for telecommunications carriers is to provide cell service. These types of data have varying levels of accuracy and are used by different entities to achieve various functions of an application or mobile device.[22]

To date, the NAI is aware of several instances where member companies are engaging in data sharing initiatives, utilizing location data from the sources described above, to help in the fight against COVID-19. In these cases, NAI members are not engaging in novel data collection to achieve these purposes, but rather, they are utilizing data their mobile application partners have already collected for the purposes of supporting the functioning of mobile apps. As explained above in response to multiple related questions, NAI members are applying privacy-protective practices with respect to these partnerships with public health officials and researchers.

To date, other than the initiative recently announced by Apple and Google to provide COVID-19 contact tracing technology, the NAI is not aware of any cases where our members are collecting, or facilitating the collection of, data that they do not ordinarily collect to support these routine purposes described above.[23]

27. 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?**

NAI member companies utilize a number of different techniques to ensure that data cannot reasonably be linked to a specific individual. For example, some privacy protections are automatically built into the collection of location data from mobile

[22] James Ewen, *Best Guide To Location Data 2020 – All You Need To Know*, Tamoco, September 4, 2019, https://www.tamoco.com/blog/location-data-info-faq-guide/.

[23] *See Apple and Google Partner on COVID-19 Contact Tracing Technology*, Google Blog (Apr. 10, 2020), https://www.google.com/url?q=https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/&sa=D&ust=1586806797088000&usg=AFQjCNGV3tv8m6B_HuyQrWDJRRDxMqYfEQ.

devices because the data is often associated only with a random alphanumeric string of characters called a mobile advertising identifier (MAID) or an identifier for advertising (IDFA). These alphanumeric strings do not themselves directly identify a specific person. However, if the location data associated with them is precise enough and collected over time, it becomes possible to infer the identity of the individual using the mobile device. For example (and especially before widespread stay-at-home orders were put in place), precise location data showing an unidentified mobile device stayed in one location in a residential neighborhood from 10:00PM to 6:00AM most days, that could support an inference that the mobile device user resided in that neighborhood, or even at a specific address in that neighborhood (assuming the entity collecting the data can associate, e.g., GPS coordinates with residential addresses). Using similar information, one could infer a mobile device user's place of work. With enough information of that nature, it becomes feasible to infer that specific individual is associated with an MAID or IDFA.

To mitigate the risk of re-identification described above, the NAI encourages companies to provide public health authorities with only aggregate location data whenever that is adequate for the purpose the data is intended to be used for. For example, aggregate data that does not include any unique identifiers has helped public health authorities identify where social distancing measures have been most effective -- authorities don't need to access any underlying unique identifiers to understand that mobile devices in certain locations tended to be closer together or further apart.

In addition, to further anonymize data, particularly for sharing with public health officials, researchers and governments, companies are using a range of differential privacy techniques to add carefully calibrated statistical noise to data sets that preserves the validity of key insights while making it much harder to make inferences about any individuals the data are based on.[24] The NAI applauds the efforts of businesses taking particular care to protect individual privacy while assisting with this pandemic.

- **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?**

It is true that in an era of big data, super computers and highly sophisticated hackers, even using sophisticated anonymization techniques cannot always completely prevent the possibility of anonymized data being associated with an individual. We included an example of how this is possible in certain circumstances above. For this reason, it is necessary to also incorporate technical and administrative controls that protect against this unintended outcome. As discussed above, differential privacy is one such technical measure. In addition, the NAI has always been a strong proponent of data minimization, including appropriate data deletion and retention requirements. In our Guidance for NAI Members: Determining Whether Location is Imprecise, we establish several technical methodologies for rendering location data imprecise, as well as a four factor analysis for companies to consider in determining whether location data is precise or

[24] *See, e.g., id,*; *Aggregated Mobility Data Could Help Fight COVID-19*, Science Mag (Apr. 10, 2020), https://science.sciencemag.org/content/368/6487/145.2; *Open DP,* Harvard University, https://projects.iq.harvard.edu/opendp.

imprecise.[25] In all cases, the methodologies require companies in receipt of precise location data to up-level that data in such a way that it is unable to determine with reasonable specificity the physical location of a user or device.

From an administrative perspective, the NAI encourages member companies who are making data available to help with this crisis to condition the sharing of data on appropriate use restrictions, limiting access as well as use cases, and limited data retention periods. And perhaps most importantly, the public health entities receiving this information should commit to never attempting to re-identify anonymous data. The theoretical question of how anonymous data could possibly be re-identified is less salient when the entities using the data have committed to never actually attempting to take those steps. By employing one, or several, of the methodologies described, companies can ensure that data cannot be traced back to an individual person.

- **Can effective contact tracing be conducted with "anonymized data"? Or will it require personally identifiable information?**

While efforts to deploy contract tracing to combat the spread of a pandemic is a new area of focus for many of us, contact tracing is not an area of expertise within the NAI. That said, the NAI is monitoring this issue to be ready to provide assistance for companies, public health officials and others that wish to explore uses of the technology that do not create risks to privacy and civil liberties of American citizens. That said, there is an opportunity for contract tracing to be conducted with the use of anonymized data, or data that is not linked or reasonably linkable to individuals. Such a service could be provided in a way whereby individuals are merely notified that they have been within proximity to an infected individual, without the provision of additional information specifying the person, or when or where the encounter occurred. Again, the NAI cannot speak to the effectiveness of various contact tracing practices, but this is a possibility that could provide benefits while minimizing privacy risks.

28. 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?**

While the NAI is not privy to the specific contracts or agreements member companies may have regarding COVID-19 related data sharing, we are aware that some of our members are working with public health authorities and university research groups to provide data to assist them in this crisis. In such instances, it is our understanding that the data they are sharing is aggregated or anonymized, minimizing consumer privacy risks, and demonstrating their commitment to the responsible use of data. Data sharing agreements may limit the scope of use, duration of retention, and strictly prohibit any

[25] See Network Advertising Initiative, *Guidance For NAI Members: Determining Whether Location is Imprecise* (2020), https://www.networkadvertising.org/sites/default/files/nai_impreciselocation2.pdf

attempts to disaggregate data, re-identify individual users, or infer the medical conditions of device holders.

- **To your knowledge, has any federal, state, or local law enforcement used private sector collected data to enforce any COVID-19 related government orders or requirements?**

The NAI is not aware of any federal, state, or local law enforcement entities using data collected from private sector companies to enforce any COVID-19 related government orders or requirements.

Sen. Johnson

29. **Given concerns with the spread of misinformation, and the advertising industry's massive role in getting accurate, up-to-date information out to the public, how is the industry proactively working to ensure advertisements are fact-checked, up-to-date, and accurate?**

Fraudulent advertising and misinformation is an ongoing challenge across the digital advertising ecosystem, due in part to the high volume of ad space across the internet, and a wide range of fraudsters and bad actors looking to deceive and take advantage of consumers. In difficult times like these, particularly when dealing with a global health crisis about which little information is known, ad fraud and misinformation is an even greater problem. For example, recent indicators have revealed that "malvertising" campaigns spiked in March, and that the U.S. has seen a significantly higher increase in malvertising over the last month.[26]

NAI members and industry leaders in the digital advertising industry apply their own techniques to identify and block fraudulent traffic and there are a number of third-party organizations that partner with these companies to bolster these efforts. Additionally, to address the ongoing challenge, leading advertising associations formed the Trustworthy Accountability Group in 2015. TAG launched its Certified Against Fraud Program in 2016 to combat invalid traffic in the digital advertising supply chain. Companies that are shown to abide by the Certified Against Fraud Guidelines receive the Certified Against Fraud Seal and use the seal to publicly communicate their commitment to combating fraud. By encouraging legitimate participants in the digital advertising supply chain to meet these standards, the TAG Certified Against Fraud Program has been shown to be an effective tool in reducing fraudulent invalid traffic in the digital advertising supply chain. The 2017 TAG Fraud Benchmarking Study, conducted by The 614 Group, found that the use of TAG Certified distribution channels for digital advertising cut the IVT rate to 1.48

[26] *See* Lara O'Reilly, *'Rats Out of the Sewers': Ad Fraudsters are Leaping on the Coronavirus Crisis*, Digiday (Apr. 2, 2020), https://digiday.com/media/rats-out-of-the-sewers-ad-fraudsters-are-leaping-on-the-coronavirus-crisis/?utm_medium=email&utm_campaign=digidaydis&utm_source=publishing&DM2=&utm_content=200402.

percent across more than 6.5 billion display and video impressions, reducing the level of fraud by more than 83% compared to the broader industry average.[27]

Sen. Young

30. Ms. Freund, once the pandemic has ended and life has returned to some semblance of normalcy and we have the opportunity to reflect on these difficult months that altered so many ways of life, what lessons do you expect us to take away?

On a personal note, I will certainly take away a much deeper appreciation for proper hand washing techniques! More seriously, I certainly hope that many of the things we've all learned over these difficult months will transform our routines, our businesses, and our personal lives for the better. I expect us to be more thankful for personal and business communities, to be more mindful of what connects us, and to respect each other more. I also expect our member companies to emerge from this crisis with a deeper appreciation for community service and a willingness to contribute technology and data to benefit society.

From a privacy perspective, I hope we can emerge from this crisis with humility about the complexity of privacy and data use, a deeper appreciation for existing privacy principles such as transparency, purpose specification, etc., and respect for the value of existing compliance regimes, such as the NAI Code, that incentivize and network good behavior. I want governments and businesses to be mindful that, in a complex world where absolutes like total anonymity and privacy are rare, we have to balance the value of privacy with other core values, and that the quest for that equilibrium is a constant challenge. I am optimistic that we can, collectively, retain a strong belief in the value of data for both societal and commercial benefit, and that its use can be governed by respect, rather than fear.

31. Ms. Freund, what type of reputational risk do businesses face by providing or processing consumer data or technology to assist in the response to coronavirus?

The NAI is tremendously proud of its member companies that are stepping up to help meet the incredible societal challenges posed by this pandemic, and doing so in privacy protective ways, using the Code as a foundation. Some privacy advocates take the perspective that any sharing of any consumer data is detrimental to consumer privacy, and thus, a business that helps combat the spread of coronavirus by processing and sharing consumer data will be subject to reputational risks insofar as those privacy advocates may criticize the good faith efforts being undertaken by companies. However, companies can help minimize such concerns, and reputational risks, by aggregating data so that individual information is not discernible from a broader group, or by removing any individual identifiers, including device IDs. Businesses can also place contractual restrictions and limitations on the data they share, by requiring deletion of the data after a certain period of time, limiting the permitted uses of the data to those that are pertinent to

[27] See Trustworthy Accountability Group (TAG), TAG Fraud Benchmark Study (2017), https://www.tagtoday.net/fraud_benchmark_research_us.

public health, or forbidding the re-identification of individuals. The NAI encourages its members to take these, and other steps to limit the privacy impact on individuals and to mitigate the reputational risks associated with sharing data with the government.

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?

    The NAI strongly recommends that commercial companies employ privacy-protective measures to collect such data prior to sharing it with researchers, including consent flows, anonymization and de-identification techniques, and aggregation of any user level data. Additionally, as highlighted above in response to previous questions, companies, including NAI members, are introducing initiatives to obtain additional data on a voluntary basis.[28] This approach, in many ways, is beneficial for mitigating concerns about government collection of data because it relies on partnerships and contracts that can be structured to limit the use of the data by public health officials or other government entities for pandemic-related solutions only.

    We are proud of our U.S. companies and their willingness to jump in to help combat this deadly disease, and we believe that one of the most critical tools our country can employ to protect its citizens from COVID-19 is information. Information promotes knowledge, and the free flow of information that has led to our tremendous economic growth and entrepreneurial spirit can also play a crucial role in our recovery.

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?**

[28] *See Apple and Google Partner on COVID-19 Contact Tracing Technology*, Google Blog (Apr. 10, 2020), https://www.google.com/url?q=https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/&sa=D&ust=1586806797088000&usg=AFQjCNGV3tv8m6B_HuyQrWDJRRDxMqYfEQ.

What are the best practices you have seen in innovating in the fight against COVID-19 that support privacy rights?

We strongly concur about the vital role of science and technology to help mitigate the many societal and individual challenges created by the COVID-19 pandemic. The NAI is grateful for the many public health officials, researchers and companies that have partnered in applying innovative technology and science. From the technology sector alone, dozens of companies responded rapidly to provide a wide range of innovative services to help Americans adapt to these unprecedented challenges.

From free access to IT platforms to tools supporting workers on the front lines and families at home, the tech sector has offered critical resources, information, telecommunications services and solutions that are essential to citizens trying to adapt at this difficult time, particularly for healthcare professionals and first responders, educators and students, governments and those individuals who are the most vulnerable.[29]

Unfortunately, transitioning back to our traditional style of life will not likely be easy for the foreseeable future. Therefore, the NAI supports policies that incentivizes companies to further expand on this initial set of offerings, and that provides an effective framework for public-private partnerships—not just for data sharing, but for deploying various technological solutions.

While this hearing is focused heavily on the need to balance the benefit of big data with privacy risks, many of these big data-enabled technology solutions have no privacy implications. But for those that relate to data for sharing with public health officials, researchers and governments, companies can look to a range of differential privacy techniques to add carefully calibrated statistical noise to data sets that preserves the validity of key insights while making it much harder to make inferences about any individuals the data are based on.[30] The NAI applauds the efforts of businesses taking particular care to protect individual privacy while assisting with this pandemic.

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?

    The privacy risk created by the collection or use of any consumer data depends largely on the type of data and how the data is used. This principle remains true now as companies

[29] *See* Cinnamon Rogers, *Tech For Good: How the Tech Sector is Stepping Up During the Coronavirus Crisis,* CompTIA (Mar. 26, 2020), https://www.comptia.org/blog/tech-for-good-how-the-sector-is-stepping-up-during-the-coronavirus-crisis.

[30] *See, e.g., id,*; *Aggregated Mobility Data Could Help Fight COVID-19*, Science Mag (Apr. 10, 2020), https://science.sciencemag.org/content/368/6487/145.2; *Open DP,* Harvard University, https://projects.iq.harvard.edu/opendp.

consider how their data sets can benefit the public during a time of crisis. Fortunately, private sector data companies, particularly NAI members, have the benefit of the NAI Code of Conduct to set out obligations and best practices for the sharing or use of data.

The following is an overview of data types that are defined by the NAI Code. They are intended to address the digital advertising ecosystem specifically, but they also provide useful concepts for data that may be used for non-advertising purposes like public health. We also explain how these correlate with other terms that are commonly used in this and other contexts.

Personally Identified Information – The NAI uses this term to refer to information that is linked, or intended to be linked, to an identified person. Examples include name, address, telephone number, email address, financial account number, and non-publicly available government-issued identifier. To maximize consumer privacy, the NAI Code places restrictions on how companies may collect this data, as well as associating it with Device Identified Information (DII), and in many cases requires prior Opt-In Consent before it may be collected.

Device Identified Information – The NAI uses this term to apply to data that is tied to a device, but not a particular consumer. DII may include unique identifiers associated with browsers or devices, such as cookie identifiers or advertising identifiers, and IP addresses, where such data is not linked to PII.4 This type of data is also widely referred to as "pseudonymous data." Under the NAI Code, device identifiers are a particularly important privacy protection because they allow companies to recognize a browser or device without collecting any data that directly reveals the identity of the individual using that device. Combined with other technical and administrative controls, it can provide insight into a device's physical movements without revealing the identity of the person using the device.

De-Identified Information – This type of data poses minimal privacy risks to consumers. The NAI defines this term as "data that is not linked or intended to be linked to an individual, browser, or device." The FTC defines de-identification as achieving a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device.

While the NAI Code does not define or refer to "anonymized data," the term is widely recognized to refer to data where processing techniques have been applied to remove or modify personally identifiable information; resulting in data that cannot be associated with or is not reasonably linked to any one individual.

Aggregate data – While not a defined term under the Code, this type of data also poses minimal privacy risks. The NAI considers aggregate data to be a type of De-Identified Information. Aggregate data is group data, such as monthly aggregate reports on an advertising campaign provided by NAI members to their clients. Aggregate data, or cross-sectional data, does not contain individual-level or device-level information that can be tied back to a specific individual or device. For example, this type of data could highlight how many people in any given city or county did not leave their homes on a given day, or provide a sense of whether many people travelled between Philadelphia and Washington during a given timeframe.

In summary, the NAI has always distinguished data types based on the level of risk of harm they present to consumers. De-Identified Information (also sometimes referred to as anonymized data) can be used for the public good in privacy-protective ways that still offer great insights for public health authorities. Similarly, aggregated data generally raises few privacy concerns because it represents large groups of people or devices, and isn't easily tied back to any individual or device. DII (often referred to as pseudonymous data) can also be effectively utilized with strong privacy protections. In these cases, it's particularly important for administrative and technical controls—applied both by companies and passed on contractually to governments, researchers or other partners—to ensure this data is not combined with other data to link it directly to identifiable individuals.

Sen. Klobuchar

35. **Reports released by the European Union indicate that Russia and China are conducting disinformation campaigns about COVID-19, which are intended to make other countries' responses appear weak while suggesting that Moscow and Beijing are providing superior aid. I worked with Senator Reed to include a provision in the 2019 National Defense Authorization Act to establish a Center at the Office of Director of National Intelligence to combat malign foreign influence campaigns like this, but this Administration has delayed in setting up the Center.**

    What additional steps do you think platforms could take on their own to stop the spread of disinformation campaigns related to COVID-19, and how can civil society groups and organizations support this effort?

    The spread of misinformation online is a very difficult challenge, but one we must collectively focus on to promote facts and helpful information--this challenge is not unique to the COVID-19 crisis, but it poses substantial new risks in these difficult times.

    NAI member companies form the backbone of digital advertising, an industry that has helped power the growth of the Internet by subsidizing the content and services Americans expect and rely on, including video, news, music, and more, and by underwriting the creation of innovative services and technologies that connect individuals and businesses. Now, more than ever, Americans are dependent on trusted news sources for our collective understanding of this unprecedented threat and how governments and companies are addressing it, and on the connectivity and communication technologies that digital advertising has enabled. The content and tools that have that all Americans are relying on during this crisis are often dependent upon advertising to survive.

It is because of this dependency that the advertising industry has an important role to play in supporting the fact-based journalism that our global community is relying on to provide accurate and timely information about this deadly pandemic. NAI members can help advertisers and marketers understand the brand safety value and engagement opportunities audiences on credible journalistic sites present, which in turn rewards and monetizes those sites with more valuable ad placements. In addition, NAI members are donating millions of dollars in crucial ad inventory to serve important public health announcements or ad campaigns that deliver vital messaging, like the CDC's #AloneTogether and #KidsTogether campaigns to encourage Americans to stay home to stop the spread of COVID-19.

Sen. Blumenthal

Location Data Sharing

In prepared remarks, NAI and IAB assured the Committee that location data collected by their members from users is used in an aggregate manner. However, the analysis discussed in remarks and seen in recent news articles, particularly tracking stay-at-home patterns, is based on the continuous monitoring of specific individuals, even if based on their device, and the categorization of the places they visit. Clearly, location data is being retained by NAI and IAB members in a granular and linked manner – and are not retained in an aggregate fashion.

In recent years, numerous media investigations and research from privacy organizations have identified cases where companies have sold or released identifiable and non-aggregated location datasets, including:

- **New York Times, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret."**[31]
- **New York Times, "Twelve Million Phones, One Dataset, Zero Privacy."**[32]
- **Motherboard, "Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years."**[33]
- **Motherboard, "I Gave a Bounty Hunter $300. Then He Located Our Phone"**[34]
- **Boston Globe, "Every step you take."**[35]

[31] *See* Jennifer Valentino-Devries, Natasha Singer, Michael H. Keller, and Aaron Krolik, *Your Apps Know Where You Were Last Night and They're Not Keeping It Secret*, The New York Times (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[32] *See* Stuart A. Thompson, Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy,* The New York Times (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

[33] *See* Joseph Cox, *Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years*, Vice (Feb. 6, 2019), https://www.vice.com/en_us/article/43z3dn/hundreds-bounty-hunters-att-tmobile-sprint-customer-location-data-years.

[34] *See* Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Vice (Jan. 8, 2019), https://www.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

[35] *See* Janelle Nanos, *Every Step You Take*, Boston Globe (2018), https://apps.bostonglobe.com/business/graphics/2018/07/foot-traffic/.

- **Vox, "Law enforcement is now buying cellphone location data from marketers."[36]**

36. NAI and IAB have held up their self-regulatory arrangements as models to protect consumers, however at least one company implicated in such articles is a member of one of your associations. Has NAI and IAB conducted investigations on the specific sales and conduct documented for each of the cited articles? If so, has it identified which specific companies had collected, made available, re-shared, or acquired the datasets for each of these cited articles? What specific companies did it identify as involved in these cited cases? If it did identify any such companies, what actions were taken?

NAI members, and participants in digital advertising in general, regularly collect and use advertising identifiers as the primary method for helping advertisers and marketers reach their intended audience. These random, alphanumeric identifiers are associated with a consumer's internet-connected devices or web browsing software, not directly with the consumer themselves. Further, advertising identifiers are designed to be easily reset or deleted at any time within device or browser settings, or through the use of industry-wide opt out tools such as the NAI's opt-out page.[37] For purposes of sharing location data with public officials to combat COVID-19, several NAI members have taken the additional steps of aggregating and anonymizing the data to further protect the privacy of consumers.

Our self-regulatory program is designed to institute best practices for the responsible collection and use of data for digital advertising, and to provide education about online digital advertising practices, including its benefits both to consumers and the Internet as a whole. The NAI does this by requiring our members to provide appropriate notice as to how they collect and use data for Tailored Advertising and/or Ad Delivery and Reporting, as well as a mechanism (for example, our industry-wide Opt-Out) for consumers to prevent their data from being collected to influence the ads that they see on online. Importantly, exercising an opt-out on the NAI site does not mean that a consumer will not receive advertising at all, but rather that they will not receive an ad informed by data. We strongly believe in the importance of the ad-supported Internet, without which the amount and variety of content available to consumers would be dramatically reduced. Indeed, free and easy access to online news has never been as important as it is today, and our member companies provide the technologies that allow that ad-supported news to be delivered to Americans, even without paying for a subscription. Still, the NAI's goal is to support the digital economy while ensuring the data collected and used for digital advertising purposes is done in a privacy-protective manner.

Although the NAI Code is limited in scope to the collection and use of data for digital advertising, thereby not covering certain other uses of data, we believe all companies can, and should, apply the NAI Code of Conduct as a foundation for decisions about how to use data outside of digital advertising. The NAI is constantly focused on consumer expectations

[36] *See* Rani Molla, *Law Enforcement is Now Buying Cellphone Location Data From Marketers* (Feb. 7, 2020), https://www.vox.com/recode/2020/2/7/21127911/ice-border-cellphone-data-tracking-department-homeland-security-immigration.

[37] *See* Network Advertising Initiative, NAI Consumer Opt Out, optout.networkadvertising.org.

of privacy and changing technologies that enable novel business models and uses of data. Through its nimble self-regulatory program, the NAI is able to rapidly update existing requirements and guidance based on developments in policy and technology. In fact, over the past three years alone, the NAI has furthered privacy protection by publishing two updates to its Code of Conduct, and four new guidance documents relating to specific technologies and use cases. This includes detailed guidance on how to obtain informed opt-in consent from users before collecting or using their precise location information for digital advertising purposes..

The NAI is currently working with its members, as well as their business partners, to increase the information consumers have about the use of their location data at the place and time of collection. Rather than relying on the standard messaging provided by mobile operating systems, we are phasing in a requirement for member companies to ensure that consumers see a just-in-time notice explaining the proposed uses of the data before obtaining a user's consent to collect those data, including for certain uses of data such as analytics, research, and reporting, to which opt-in consent requirements had never previously applied.

As to any investigation of an NAI member, as a general matter, the NAI does not publicly reveal the details or results of an investigation into a member company's adherence to the NAI Code of Conduct if it the company's conduct did not result in a material violation of the NAI Code. Further, all NAI members are required to undergo a comprehensive compliance review every year conducted by experienced privacy attorneys on the NAI staff, regardless of whether those companies are under investigation for an NAI Code violation.

NAI members are required to continue their adherence to the NAI Code throughout each year they are in our membership. NAI staff also monitor and review public allegations of member conduct that implicates non-compliance with the NAI Code. Through this process, potential violations of the NAI Code are quickly investigated by our compliance staff. The NAI's policy of refraining from public disclosure of every issue that it investigates provides an incentive for members to be more candid during compliance reviews and investigations. This approach fosters an environment of mutual trust between the NAI and its members, and ultimately results in enhanced privacy protection for consumers as members become more open about potential shortcomings and more willing to participate in self-regulatory efforts.

That said, when the NAI staff discover member conduct that materially violates the NAI Code, it has the power to impose sanctions and other enforcement measures on member companies, which can include referral to the FTC. These powers function primarily as a deterrent against noncompliance and as a means of ensuring responsiveness from member companies, rather than as a demonstration of the NAI's compliance efforts through detailed public disclosure of every issue discovered by NAI staff.

NAI staff conducted three investigations of potential material violations of the Code during the 2019 compliance year. In each case, NAI staff found that the activities of the companies in question did not materially violate, or else fell outside the scope of, the Code. Sanction procedures were therefore not appropriate as a result of the investigations.

The NAI is proud of its members' strong record of compliance with the NAI Code, and we believe that high degree of compliance is due to a number of important factors. First, our member companies voluntarily submit themselves to the strict requirements in our Code because they care about privacy; they are leaders in privacy-enabling technologies and policies and set an example for the rest of the industry to follow. Second, we work very hard to craft a Code, and accompanying guidance documents, that are clear in their application to member business practices. Third, NAI staff teach companies how to comply with the Code, even before they are admitted to membership, by clearly setting expectations and conducting training. Finally, we work directly with companies on their annual review process to ensure clarity and consistent interpretation. We are mindful that compliance with detailed privacy requirements is a challenge with any law or regime, and we work hard to enable cooperation by our member companies.

Social Media Harvesting

In late March, StatSocial, a data broker that caters to advertisers, announced a "Crisis Insights" product, which claims to monitor consumer sentiments regarding the COVID-19 pandemic. StatSocial boasts that its analysis is "based on StatSocial's unique Silhouette social identity platform with its 85,000-segment taxonomy across 1.3 billion social accounts that connect to more than 70% of US households." StatSocial further elaborated that its dataset is sourced from "1.2 billion profiles sourced from 60 different platforms and more than a million websites, 300 million individual email accounts, and more than one billion IP addresses and mobile devices."

Clearly, StatSocial has not obtained consent, nor even awareness, from 70% of U.S. households to monitor their concerns and their families' wellbeing from their social media accounts and inboxes during the Coronavirus pandemic.

37. **Please list which members of your association harvest, process, or disclose to third parties (such as through SDKs or data sharing agreements) information gathered from social media accounts or email inboxes for the purposes of audience segmentation, building profiles, ad targeting, advertising analytics, or other commercial purposes not technically necessary for the provision of a service or product that an individual has requested?**

    Today, a broad array of rich content is available on the Internet, including information and news content, video and music streaming services, and interactive software services such as email and social networks. These have all experienced robust growth over the last decade, providing a wide array of transformative benefits to consumers for free, or for little cost, supported by digital advertising. Digital advertising, and Tailored Advertising in particular, has been fundamental to the success of the Internet and the digital economy, providing significant benefits to consumers by connecting them with products and services that are more relevant to their interests, and providing opportunities for American businesses large and small to connect with consumers.

Location-based features are one of the key benefits offered by mobile devices and applications. Those features include customized local weather forecasts, integrated mapping technology, and the collection and use of location data to provide Tailored Advertising. In most cases, location data collected through mobile applications is shared with partners, such as NAI member companies, in order to provide tailored ads to users. The revenue generated from those ads allow consumers to enjoy the use of those applications for free or for a lower cost. Location data collected through mobile apps is also frequently used for business analytics. The collection of location data is usually accomplished through the use of Software Development Kits (SDKs), or software code integrated into the application, sometimes provided by third-party partners to enable key features of the application and to enhance advertising and marketing practices.

NAI members generally obtain location data directly through SDK integrations with applications on mobile devices, through the bid stream, or through other means. Companies may use a variety of different sources or methods to obtain data.

In most cases, the "scraping" or "harvesting" of data from social media accounts and email inboxes violates the terms of service of the platforms providing those services to consumers. The NAI does not approve of any data collection that violates such terms. A violation of these ToS would effectively make it impossible to provide consumers with the notice the NAI requires at the point of data collection.

The NAI Code requires members to prominently display their privacy policies, which include detailed overviews of their data collection, use and sharing practices for Tailored Advertising and/or Ad Delivery and Reporting. All NAI member companies, as well as a short summary of their businesses and a link to their privacy policies are listed on the NAI membership site.[38]

Personal Health Data

While the Health Insurance Portability and Accountability Act (HIPAA) provides strong protections for protected health information, these rights are limited to collection by health care providers and their business associates. Since the passage of HIPAA, new markets and commercial use cases have arisen for this data, both beneficial as well as not, from consumer health products to marketing services. The recent CMS/ONC data sharing rules and COVID-19 pandemic has provided further examples of companies collecting sensitive health information that does not fall under these rules, and who have significantly different business models than health care providers.

38. **Which of your members collect and process health information or proxies for health information, such as risks or indicators of mental health or substance abuse disorders, about Americans that is not governed under the HIPAA privacy and security rules, and for what purposes do they collect or process this data?**

[38] See Network Advertising Initiative, NAI Members, https://www.networkadvertising.org/participating-networks/.

The NAI provides very strong consumer protections with regard to the use of health information for digital advertising, and has led the digital advertising industry in requiring NAI members to provide transparency into what health-related audience segments they use,[39] and in requiring NAI members to obtain a consumer's informed Opt-In Consent for any use of sensitive health information for digital advertising purposes. Inferences about an individual's mental health or substance abuse disorders would clearly qualify as sensitive health information under the NAI Code. In practice, these opt-in consent requirements function as a strong disincentive against the use of sensitive health data for advertising purposes and the NAI is not aware of any of its member companies seeking to obtain opt-in consent to use sensitive health information for advertising purposes. NAI members are also required to obtain a consumer's informed Opt-In Consent for the use of any biometric sensor data from their device, such as heart-rate or blood glucose information for Tailored Advertising or Ad Delivery and Reporting.

The NAI balances these strong protections with a belief that consumers stand to benefit from privacy-friendly advertising practices in the pharmaceutical and medical fields, and members may engage in practices such as demographic-based targeting. As an example, this allows members to target pharmaceutical ads to audiences based on gender for medical conditions that primarily affect men or women. Members may also target ads based on web browsing or app use for non-sensitive conditions such as common cold, flu, diet and fitness. Further, NAI members may enable contextual advertising. For example, this would allow a pharmaceutical company to advertise its product on websites specific to relevant health conditions, but NAI members do not need to retain any sensitive health information about a web user to enable this kind of advertising.

The NAI's holistic and balanced approach helps to provide strong consumer privacy protection for sensitive health information while preserving the ability of pharmaceutical and medical advertisers to reach broad audiences based on demographics and for the targeting of ads for common, non-sensitive ailments.

Sen. Peters

39. **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?

    The NAI does not have expertise in medical equipment supply chain management and manufacturing, so we are not able to comment specifically on this question. We do believe, however, that the potential uses of aggregated data sets to show patterns, or gaps, in supply chains or stockpiles is enormous and we would encourage companies that have

[39] All NAI members must publicly disclose a full list of any standard audience segments tied to health or the human body, as well as a representative sample of the custom segments the member may create tied to these topics.

relevant aggregate data to employ it in the effort to prevent such shortages from recurring.

40. **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?

    The NAI does not have expertise in medical equipment supply chain management and manufacturing, so we are not able to comment specifically on this question. We do believe strongly, however, that innovation is at the heart of the technology industry, and the ability of U.S.-based technology companies to innovate and create exciting new products and services is unmatched. I would recommend maintaining incentives for technology companies to invest in research and development to evolve and expand their abilities to assist communities in responding to public health and other emergencies.

Sen. Baldwin

<u>Data and Minority Communities</u>

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 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.

41. 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?

The NAI is proud of its many member companies who have stepped up to help in the fight against COVID-19, particularly those that have donated ad inventory, time, money and expertise to help disseminate important public health information to citizens through PSA campaigns. This is a terrific example of companies doing what they do best to help support communities across the country.

While the NAI does not have expertise in big data analytics as applied to minority communities, we do believe that the opportunities and potential benefits of big data analytics are enormous. However, we must utilize our best skills, technologies and information to ensure that the results of such analysis are not biased and that they don't result in disproportionate outcomes for minority communities.

Data and Rural Communities

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.

42. 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?

It is certainly true that rural, suburban, and urban communities have vastly different characteristics, and because COVID-19 is affecting each area differently, the public health response must be tailored to each community in order to be effective, particularly as we start to emerge from stay at home orders and begin to open our economy. While the NAI does not have expertise in big data analytics as applied to rural communities, we do believe that use of aggregate data can, and should, weigh population density, connectivity saturation and availability of resources to develop predictive models that are tailored to each community.

Public Health and Private Sector Collaboration

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.

43. **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?**

    As we highlighted in our testimony and earlier in this questionnaire, the NAI believes that the COVID-19 Mobility Data Network (the "Network") provides an excellent example of a program that effectively balances utility for public health with individual privacy protections.

    The Network uses anonymized, aggregated location data sets from mobile devices to provide decision-makers at the state and local levels with daily updates on how well social distancing interventions are working, as well as analytic support for interpreting the location data. The Network is powered by a working partnership with multiple companies. Through direct connections with public health authorities at the city, state, and country-level, the Network provides tools that offer timely insights into the effectiveness of social distancing measures, a way to identify potentially high-risk zones, and assistance for planning the roll-back of restrictions.[40]

    The Network is also supporting government efforts to manage and adapt public services for the COVID-19 pandemic at the state and local level. For example, information supplied by the Network can help local officials understand changes in essential trips that can then shape recommendations on business hours or inform delivery service offerings. Similarly, transportation hubs that continue to experience high traffic might indicate the need to add additional buses or trains in order to give essential workers who need to travel more space for social distancing. Ultimately, understanding not only whether people are traveling, but also trends in destinations, can help local officials protect public health and provide for the essential needs of communities.

    The broad availability of privacy-protective data to researchers and public health officials is a valuable step. However, as you identify, there is ultimately a level of coordination and cooperation between international, U.S. federal, state and local health departments, many of which are seeking to achieve the same objectives.

<u>**Question on Data Sharing**</u>

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.

[40] For more information about the Network, see https://www.covid19mobility.org/.

44. **What are ways we can strengthen the data-sharing infrastructure for government, public health, academic and private sector sources?**

    The NAI supports the efforts of member companies who are making privacy-safe data sets available to researchers and public health officials, because these efforts will help to protect American lives, minimize the impact that stay-at-home orders are having on our economy and the well-being of many Americans, and implement and evaluate measures to limit the spread of COVID-19. However, as we discussed in our testimony and throughout this questionnaire, there are a series of steps and requirements that private sector companies need to undergo to limit the privacy risks of the data they are making available. In some cases this may well lead to partnerships and contracts where there are strict agreements in place regarding the intended uses of the data, as well a limitations on the use of the data set to ensure that it is only used for the identified purpose, and not used or shared with other entities after that purpose has been achieved.

Sen. Sinema

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?**

    The NAI focuses its limited resources on the privacy-protective and responsible collection and use of data for digital advertising, and therefore we are not in a position to offer an expert opinion on big data analytics applied to disease trends. However, we believe it is important to build predictive models and research projects that anticipate data limitations or inaccuracies. We understand that many of the models currently in use by researchers and health experts to help stop the spread of COVID-19 anticipate the use of aggregate data, rather than more precise data sets, and are therefore built to mitigate inaccuracies.

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?**

    Apple and Google recently announced that they will soon be jointly launching a voluntary contact tracing solution designed to maintain strong protections around user privacy. First, in May, both companies will release APIs that enable interoperability between Android and iOS devices using apps from public health authorities. These apps will be available for users to download via their respective app stores. And second, in the coming months, they plan to work to enable a broader Bluetooth-based contact tracing platform by building this functionality into the underlying platforms. This is intended to maximize the participation and effectiveness for individuals who choose to participate, as well as enable interaction with a broader ecosystem of apps and government health authorities.[41]

Following are the key privacy protections that are built into the joint technology solution:[42]

- Explicit user consent required
- Doesn't collect personally identifiable information or user location data
- List of people you've been in contact with never leaves your phone
- People who test positive are not identified to other users, Google or Apple
- Will only be used for contact tracing by public health authorities for COVID-19 pandemic management

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?

The NAI does not have expertise in medical equipment supply chain management and manufacturing, so we are not able to comment specifically on this question. We do believe, however, that we should employ all available resources, including any data that NAI member companies or other data companies can contribute, to dramatically increase the production and distribution of needed resources to address COVID-19, particularly as we work to understand the implications of lifting stay at home orders, and getting American back to work.

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?

Businesses across all sectors of the economy are under strain from the economic collapse precipitated by the pandemic, including NAI member companies who have suffered as spending on advertising has slowed dramatically. As with other industries, the employees of digital advertising companies have experienced pay cuts, furloughs, and layoffs as companies take emergency measures to stay afloat in these extremely difficult circumstances. The NAI supports the creation and enhancement of economic assistance programs like the Paycheck Protection Program and new lending facilities to provide

[41] *See Apple and Google Partner on COVID-19 Contact Tracing Technology*, Google Blog (Apr. 10, 2020), https://www.google.com/url?q=https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/&sa=D&ust=1586806797088000&usg=AFQjCNGV3tv8m6B_HuyQrWDJRRDxMqYfEQ.

[42] see https://www.blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing_Using_BLE.pdf

whatever assistance is possible to businesses. While the use of big data in connection with those programs is outside the expertise of the NAI, we would encourage all technology companies to employ their own innovative skills to help businesses, communities and individuals to get back on their feet and help the economy recover.

Sen. Rosen

Benefits and Privacy Concerns of Donated Data

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?**

The NAI supports efforts to use data-driven science to fight the spread of COVID-19, and we are proud to have member companies who are contributing to this fight to protect American lives, to minimize the impact that stay-at-home orders are having on our economy and the well-being of many Americans, and to implement and evaluate measures to limit the spread of COVID-19.

Privacy and beneficial uses of data are not mutually exclusive, broadly or in relation to efforts to combat COVID-19. As we highlighted in our testimony, if the data is shared in aggregate, de-identified or anonymized form, and use limitations are put in place, an effective balance can be reached between achieving desired public health outcomes and maintaining individual privacy. We expand on some of these policies and practices in greater detail in some of the previous questions.

With respect to the privacy guardrails, the NAI encourages the use of anonymized, de-identified, and aggregate location data where practical to protect consumers' privacy. Anonymized or de-identified data is not linked or intended to be linked to an identified person or device, mitigating privacy risks. Aggregate data refers to a data set that refers only to population-level data and does not present any appreciable privacy risk to individuals.

Also, in order to maximize privacy and consumer choice, it is critical to gain consent from individuals for collecting Precise Location Information or other sensitive data. To this end, the 2020 Code also reinforces the requirement that consumers must have clear, timely notice about the reasons why Precise Location Information is being collected, and with whom it will be shared. In addition, such notices should include information on the anticipated use of the data, which could include research and/or public health. This allows consumers to make informed choices about whether to allow data from their mobile devices to be used and shared for those purposes. NAI members are also part of a larger ecosystem of companies that utilize data in their business models, and by adhering to best practices and standards for responsible data collection and use, NAI member companies encourage networked compliance to such standards by business partners and other participants in the ecosystem.

NSF Research on Big Data

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?

We believe programs such as "Harnessing the Data Revolution" can play a vital role in shaping and defining the tremendous value that data brings to our society, and in continuing to support the innovative technology industry as it continues to lead economic growth, both here and abroad. We strongly believe that data will continue to drive large sectors of the American economy, and that public-private partnerships are essential to understanding how data can address societal problems both big and small. We look forward to supporting the NSF's terrific work, and to our companies playing a role in supporting data-driven solutions that can shape our response to future challenges.