Enlisting Big Data in the Fight Against Coronavirus

Testimony from

Leigh Freund
President and Chief Executive Officer
Network Advertising Initiative (NAI)

before the

United States Senate Committee on Commerce, Science, and Transportation

April 9, 2020

I. Introduction

Dear Chairman Wicker, Ranking Member Cantwell, and members of the Committee. Thank you for inviting me to testify today on "Enlisting Big Data in the Fight Against Coronavirus." Americans are thinking of little else during this critical period than our collective efforts to stem the spread of this dangerous pandemic, and the NAI appreciates the opportunity to highlight our members' important work on this effort and the importance of ensuring the proper balance between societal benefits and consumer privacy. We hope that the members of this Committee, their staff, and their constituents are safe and well – our thoughts are with those who are suffering, and we look forward to a time when this crisis passes and we can work together on these issues, in person.

The Network Advertising Initiative (NAI) is the leading self-regulatory organization dedicated to responsible data collection and use governing third parties engaged in Tailored Advertising and Ad Delivery and Reporting (ADR)[1] in the United States. The NAI, a non-profit self-regulatory organization and trade association, was formed in 2000 and has over 100 member companies, each of which is required to adhere to the strong digital advertising best practices set forth in the NAI Code of Conduct ("Code" or "NAI Code"), which the NAI enforces through annual compliance reviews, and which implements stringent consumer privacy protections. The Code is rooted in the widely accepted Fair Information Practice Principles (FIPPs)[2], and it applies those principles to the digital advertising ecosystem by, among other things, instituting robust notice and choice requirements and restrictions on the use and sharing of data. The Code heightens restrictions and requirements for more sensitive data types. For example, Precise Location Information requires Opt-In Consent accompanied by detailed, just-in-time notice about the collection, use, and sharing of such information.

Our members include a wide range of businesses such as ad networks, exchanges, location data aggregators, platforms, and other technology providers. Across websites, mobile applications,

---

[1] Tailored Advertising is defined by the NAI Code as the "use of previously collected data about an individual, browser, or device to tailor advertising across unaffiliated web domains or applications, or on devices, based on attributes, preferences, interests, or intent linked to or inferred about, that user, browser, or device." Ad Delivery and Reporting is "separate and distinct from Tailored Advertising, and it refers to the collection or use of data about a browser or device for the purpose of delivering ads or providing advertising-related services, including, but not limited to: providing a specific advertisement based on a particular type of browser, device, time of day, or real-time precise location; statistical reporting, traffic analysis, analytics, optimization of ad placement; ad performance, reach, and frequency metrics (including frequency capping); sequencing of advertising creatives; billing; and logging the number and type of ads served on a particular day to a particular website, application or device. ADR does not include data collection and use for security and fraud prevention." *See* Network Advertising Initiative, 2020 NAI Code of Conduct § I.A, I.Q (2020), https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf [hereafter 2020 NAI Code of Conduct].

[2] *See* Fed. Trade Comm'n, Privacy Online: A Report to Congress 7 (1998), https://www.ftc.gov/sites/default/files/documents/reports/ privacy-online-report-congress/priv-23a.pdf; see also Fed. Trade Comm'n, Privacy Online: Fair Information Practices in the Electronic Marketplace (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

and connected televisions, our member companies form the backbone of the digital advertising ecosystem—helping advertisers reach audiences most likely to be interested in their products and services while allowing consumers to receive ads and content that are tailored to their interests.

While our Code 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 companies utilizing data to promote societal benefits, such as mitigating the harmful outcomes of the deadly COVID-19 pandemic. In this testimony, we explain the types of data that are currently being used for this objective, highlight some examples of NAI member companies working collaboratively with public health officials to achieve positive outcomes, and detail the key precautions businesses and governments can undertake to ensure that these outcomes can be achieved while minimizing threats to the privacy and civil liberties of U.S. citizens. In summary, this testimony highlights the following key points:

1. The NAI Code has extensive and detailed requirements for privacy, transparency, and accountability that go beyond existing U.S. privacy laws in many ways, and it is continually updated and expanded to account for new technological developments. While NAI member companies voluntarily subject themselves to the NAI's Code restrictions because they care about privacy, its principles serve as a set of best practices for all companies.
2. During this public health emergency, NAI member companies can, and should, apply the NAI Code of Conduct as a foundation for decisions about how to use data to help public health officials and researchers better respond to the coronavirus pandemic without sacrificing important privacy protections. We believe society can benefit from the use of data while keeping privacy protections in place for the future.
3. Questions around how data is used during the coronavirus response illustrate the need for a comprehensive national data privacy law that clearly defines and makes illegal practices that may harm consumers. The law should encourage the use of aggregate or anonymized data for research purposes, and create guidelines to ensure that companies and governments balance the societal benefits of data shared for the public good, with guardrails to prevent harms to privacy and civil liberties.

II. Even in times of crisis, privacy considerations and precautions remain essential, and the NAI Code provides a foundation for balancing privacy with beneficial uses of data.

NAI members are well suited to apply the Code and other key privacy principles to balance data usage with privacy. Below, we highlight different types of data based on the definitions used in the NAI Code of Conduct, the associated requirements for consumer transparency and control

established in the Code, and other guidance the NAI provides to its members in connection with their collection, use and sharing of Precise Location Information.[3]

A. Understanding Different Data Types

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 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 Code. They are intended to address Tailored Advertising specifically, but they also provide useful concepts for data that is also used for non-advertising purposes. 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 some 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."[5] The FTC defines de-identification as achieving a reasonable level of

[3] Precise Location Information is defined in the NAI Code as "data that describes the precise geographic location of a device derived through any technology that is capable of determining with reasonable specificity the actual physical location of an individual or device, such as GPS-level latitude-longitude coordinates or location-based radio frequency signal triangulation. *See* 2020 NAI Code of Conduct § I.I. (2020).

[4] *See* 2020 NAI Code of Conduct at § I.F.

[5] *See* 2020 NAI Code of Conduct § I.E (2020).

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.[6]

While the NAI Code does not define or refer to "anonymized data," the term is widely recognized, particularly in these cases, 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.[7] 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. 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.

B. Notice and control is critical for consumers

The NAI has also set the standard across the industry for how location and other sensitive data may be collected for advertising purposes. Under the NAI Code, the following data types require Opt-In Consent prior to their use for Tailored Advertising or Ad Delivery and Reporting purposes: Precise Location Information, Sensitive Information (which includes sexuality and sensitive health-related data), Personal Directory Information, and Sensor Information (camera, microphone, or other sensor that may collect biometric data from a device). In addition, users from whom Opt-In Consent is obtained must have access to detailed notice of the intended uses of such data, including data sharing.

[6] *See* Fed. Trade Comm'n., Protecting Consumer Privacy in an Era of Rapid Change, (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[7] *See* 2020 NAI Code of Conduct app. at 20.

The NAI recently released Guidance[8] for its members, clarifying the Code's requirement to provide notice when obtaining Opt-In Consent for those enumerated categories. Members must take steps to ensure, either directly, through their partners, or through technical integrations, that consumers receive detailed, just-in-time notice, clearly describing advertising as one of the proposed uses for the collection of the data. Users offering consent for their data, including Precise Location Information, should know how their data is being used and with what types of parties the data will be shared.

On the other hand, our Code does not require member companies to provide consumers with separate notice describing any sharing of de-identified or aggregated data. That is because De-Identified Information (including aggregated data) is not associated with any particular consumer or device. However, to further promote transparency, the NAI still recommends that all companies disclose to consumers that De-Identified Information may be shared with other third parties, when that is the case. Doing so helps alleviate heightened concerns around the use of location data collected from mobile devices (even in de-identified or aggregated form). This best practice recommendation shows how self-regulatory regimes like the NAI can respond quickly in the face of new developments.

C. Application of the NAI Code to non-marketing purposes, including public health purposes

The NAI Code is focused primarily on the use of data for advertising and marketing. However, the Code does apply to non-advertising uses of data in certain circumstances—to protect against consumer harm, it has clear prohibitions against non-marketing eligibility uses of data collected for advertising purposes.[9] But the Code does not prohibit the use of data collected for advertising purposes to be shared or used for public health purposes, such as sharing with public health authorities to fight the COVID-19 pandemic. The NAI applauds our members who are using data in privacy-protective ways to combat this pandemic. After all, our members are generally not collecting advertising data for the separate purpose of making it available to public health authorities in an emergency, and efforts to allow its use in such an emergency should be encouraged. Finally, as discussed in the next section, certain NAI members are currently sharing aggregated and de-identified data with public health authorities in order to minimize privacy risks.

NAI members are ideal candidates for bringing their data resources to bear on a public health crisis because they have already demonstrated their commitment to good data stewardship. For example, during the NAI's annual compliance review of its member companies, compliance staff routinely assist companies with accountability measures they can take to protect the data in their systems. The combination of Code requirements and recommended best practices includes providing consumers with access to their data while limiting the access by company

[8] *See* Guidance for NAI Members: Opt-In Consent (2019), https://www.networkadvertising.org/sites/default/files/final_nai_optinconsent-guidance19_final.pdf.
[9] *See* 2020 NAI Code of Conduct § II.D.2 (prohibiting the use of advertising data for credit eligibility, insurance eligibility and other non-marketing eligibility purposes).

employees to consumer data and limiting the retention of data after it is no longer useful. Privacy by Design must inform the development of technologies and products, and training and oversight is essential. Data minimization is a recommended practice, and providing for appropriate security of the data is fundamental.

In all cases, including when collecting location data from a third-party source, NAI members are required to take due diligence steps to ensure the reliability of the source of the data. It is essential that these other sources of data have secured the appropriate informed consent that such data might be shared and for what purposes.

When NAI members pass such appropriately permissioned data along (whether aggregate or user-level), they must ensure that the downstream partners are also protecting the data and restricting use as directed. Other NAI obligations, such as data retention limitations and data security (among others) are fundamental practices that ensure responsible data use and the protection of individual privacy.

Overall, NAI member companies following the 2020 Code are well-situated to collect, use, and share location data of various granularity for public health or certain other non-marketing purposes. The updates to the 2020 Code also reinforce 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. This allows consumers to make informed choices about whether to allow data from their device to be used and shared for those purposes. NAI members are also part of an ecosystem, and a key element of such industry compliance regimes is that they network compliance, not only among members, but across the participants in the ecosystem who partner with NAI member companies.

III. NAI member companies can apply the NAI Code of Conduct as a foundation to help balance emergency public health uses of data (to help public health officials and researchers better respond to the coronavirus pandemic) without sacrificing important privacy protections.

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, much of which can be gleaned from location-based features offered by mobile devices and apps.[10] The NAI supports these efforts, and we are proud to have member companies who are contributors, because these efforts will help to protect American lives, minimize the impact that stay-at-home orders are

[10] 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.

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

One of the premier examples is the "COVID-19 Mobility Data Network," (Network) which is a network of infectious disease epidemiologists at universities around the world working with technology companies to use aggregated mobility data to support the COVID-19 response. The goal of the Network is to provide daily updates to decision-makers at the state and local levels on how well social distancing interventions are working, using anonymized, aggregated data sets from mobile devices, and to provide them analytic support for interpretation. This work is powered by a working partnership with multiple companies. Through direct connections with departments of health at the city, state, and country-level, the Network provides situation reports to decision-makers who are implementing social distancing interventions. These data are critical in providing timely insights into the effectiveness of social distancing measures, for identifying potentially high-risk zones, and for planning the roll-back of restrictions.[11]

This data can also help support governments' decision-making about how they can manage and adapt public services for the COVID-19 pandemic. For example, this information could help officials understand changes in essential trips that can then shape recommendations on business hours or inform delivery service offerings. Similarly, persistent visits to transportation hubs might indicate the need to add additional buses or trains in order to allow people who need to travel additional room to spread out for social distancing who need to travel. Ultimately, understanding not only whether people are traveling, but also trends in destinations, can help officials design guidance to protect public health and essential needs of communities.[12]

Additionally, 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. Companies are also working with researchers, who are looking into the effect that corporate dispersion has on COVID-19 information dissemination and reaction, e.g., whether employees in COVID-19 hotspots are more likely to stay home.

Finally, member companies are helping our communities fight the novel coronavirus by doing what they do best—utilizing their innovative advertising technologies to serve public service advertising campaigns (PSAs) to help stop the spread of COVID-19. For example, the Federation for Internet Alerts, a non-profit organization that is the largest distributor of mobile and web-based alerts globally and includes many NAI members, is helping the CDC market its

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

[12] 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.

#AloneTogether campaign about the importance of staying home to reduce the spread of the coronavirus.

NAI members embrace privacy as a core value. Therefore, the NAI encourages its members to subject their efforts and partnerships in this area to legal and ethical review and be guided by contractual controls that narrow the amount and granularity of data provided, restrict secondary uses or sharing of the data, and limit the timeframe the data are permitted to be used to achieve the approved research objectives.

IV. Questions about data use raised during the coronavirus response illustrate the need for a comprehensive national data privacy law that clearly defines and makes illegal practices that would harm consumers.

The NAI is a leading proponent of a federal consumer privacy framework, and today's hearing presents another key example of why this would benefit U.S. citizens, businesses, and society as a whole. As a founding member of Privacy for America, a coalition of top trade organizations and companies representing a broad cross-section of the U.S. economy, the NAI contributed to the coalition's comprehensive data privacy framework and supports the enactment of federal legislation consistent with its principles.[13] COVID-19 underscores the need for privacy legislation that protects consumers, allows for responsible uses of data, and protects innovation.

Consumers are currently relying on online services more than ever, for critical news and health information, to stay connected with family and friends, to ensure educators stay engaged with students, and to order and receive essential goods from the safety of their homes. A national privacy law should recognize the benefits these services provide, encourage the development of future consumer offerings, while at the same time offering important consumer protections.

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.

[13] For more information, see https://www.privacyforamerica.com/overview/.

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.

Lastly, the framework calls for greater resources and a new Bureau and substantially increased resources at the Federal Trade Commission to ensure that the federal government has the tools, knowledge, and public servants necessary to tackle these challenging and complex technical and ethical questions.

V. Conclusion

The NAI commends the Chairman and Ranking Member for organizing this hearing despite the very difficult circumstances facing our society, and we greatly appreciate the opportunity to provide testimony and inform this timely discussion. The NAI is proud of our Code of Conduct and self-regulatory efforts to promote privacy-protective practices throughout the industry that can not only serve to promote privacy in digital advertising, but can also serve as a foundation for our members and other companies to work collaboratively with public health organizations and researchers to balance the opportunities to achieve positive outcomes for society as a whole, while protecting consumer privacy.