

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive
Advertising Bureau

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?

RESPONSE: During these challenging times, businesses, government entities, public health officials, and other stakeholders must collaborate to find effective ways to address the COVID-19 pandemic. Despite the present circumstances, businesses are doing what they can to help their communities and all Americans, all the while keeping consumer privacy at the forefront of their considerations. Our member companies, both large and small, are offering connectivity, content, and services to consumers for free or at a reduced cost.¹ Our member organizations are also helping Americans get the latest news, online food deliveries, entertainment, access to digital conference calls, and many other essential services. Online advertising is helping to keep the world connected, both professionally and personally. In the context of data privacy, IAB is a founding member of a self-regulatory program known as the Digital Advertising Alliance (“DAA”). DAA offers tools to provide consumers with transparency and control over data collected online. This program and its web and app-based, privacy-focused tools make data privacy and consumer notice and choice fundamental considerations for entities operating in our industry. We believe that DAA serves as a useful model for how to respect individual privacy rights and enable beneficial advertising services.

- 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**

¹ See Dave Grimaldi, *Good Works: IAB & Tech Lab Members vs. Coronavirus* (Mar. 25, 2020), located at <https://www.iab.com/blog/good-works/>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

balance is protection of individual privacy, which is believed to be threatened by greater surveillance of individuals by the government.

Is this an accurate view of the situation? Are privacy and effectiveness always part of a trade-off, such that the most effective public health measures will come at the expense of privacy, and vice versa? Or do you believe that the most effective policies for combatting COVID-19 can also respect individuals' privacy?

RESPONSE: IAB strongly believes that data and privacy are not mutually exclusive. The collection and use of data, subject to responsible data stewardship and reasonable privacy practices, can power insights to improve our efforts to respond to the coronavirus.

It is because of this belief that consumer trust is foundational to the digital economy that IAB supports Privacy for America, a new framework for nationwide privacy legislation that would fundamentally change the way personal data is protected and secured in this country. This framework is intended to provide a new option to policy makers for their consideration as they address this important issue. Unlike existing domestic and international approaches to privacy regulation, the framework would not rely on burdensome "notice and choice" schemes to protect personal data. Rather, it would clearly define and prohibit 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.

Notably, the new framework would shift the burden away from individuals to read hundreds of lengthy privacy policies to protect themselves and toward a common set of data privacy and security norms. We encourage Congress to act to provide nation-wide privacy protections for all Americans consistent with Privacy for America's framework.

- 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?

RESPONSE: We agree that it is time for nationwide privacy protections. It is the reason IAB supports Privacy for America.

Privacy for America is working with Congress to support enactment of comprehensive federal consumer data privacy and security legislation. We propose a bold new paradigm

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

for a national law that would make personal data less vulnerable to breach or misuse and set forth clear, enforceable, and nationwide consumer privacy protections for the first time.

The framework would apply to virtually all personal information collected and used in the United States and virtually all companies doing business here. It would give the FTC expanded authority over nonprofits and common carriers for purposes of the new law. In addition, the framework would apply broadly to all personal information, whether collected or inferred, that is linked or can reasonably be linked to a particular individual or device.

Importantly, the framework would prohibit outright, rather than allow consent for, a range of practices that make personal data vulnerable to misuse. Many of these prohibitions would apply not only to companies that engage in these harmful practices directly, but to suppliers of data who have reason to know that the personal information will be used for these purposes. The framework would provide new protections by prohibiting the use of sensitive data without express consent. This prohibition would apply to a range of sensitive information including health, financial, biometric, and geolocation information, as well as call records, private emails, device recordings, and photos.

- 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?

RESPONSE: Data brings tremendous value to society. It has the power to facilitate useful insights and trends that can inform policymaking, crisis response, and the discovery of cures, as well as keep citizenry informed and enable access to vital services and communication channels. Like many industries, the digital advertising industry is a critical piece of our nation's response to the health pandemic, particularly as a subsidizer and supporter of content like news, public health alerts, and announcements individuals receive about COVID-19. Subject to appropriate privacy protections, advertising and data can play a significant role in supporting the fight against the coronavirus.

One way in which companies are addressing privacy concerns is by making available anonymized, de-identified, and aggregated data set or insights derived from collected data. In this context, data may be used to derive powerful insights that inform and help structure strategies to respond to and prevent the spread of COVID-19 while limiting how data, including individually identifiable information, is shared. The benefits of data

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

anonymization, de-identification, and aggregation have been recognized in many prominent U.S. privacy laws.

The IAB and its members have been at the forefront of promoting responsible data practices, such as data anonymization and de-identification, and consumer trust is vital to our member companies' ability to operate successfully in the marketplace. This commitment to consumer trust, and recognition that data is essential for business success, is best exemplified through IAB's integral role in the creation of the self-regulatory systems administered by the DAA. The DAA is an industry body convened more than a decade ago to create a self-regulatory code for all companies that collect or use data for interest-based advertising online. Today, the DAA Principles provide consumer transparency and control regarding data collection and use of web viewing data, application use data, precise location data, and personal directory data. The DAA Principles are independently monitored and enforced by accountability programs. To date, more than 100 compliance actions have been publicly announced, and additional investigations have occurred without being made public.

Industry privacy programs must evolve with new technologies and preferences in order to maintain consumer trust. Since its inception, the DAA has responded to changes in the marketplace by updating its self-regulation and guidance to account for Multi-Site data, mobile data, cross-device data, and political advertising. More recently, the IAB announced Project Rearch, an initiative to engage stakeholders from across the digital advertising and media supply chain to work together to re-architect digital marketing in a way that balances personalization and consumer privacy.²

Industry efforts to promote responsible data practices will persist as entities find new ways to use data to combat COVID-19. The DAA Principles—and the strong privacy protections they afford consumers—apply even in times of crisis. Public-private partnerships to discover beneficial uses of information that can strengthen the public health response will be of considerable importance during this unprecedented time. Now more than ever, data can provide individuals with direct benefits by offering government stakeholders key insights they can use to develop strategies to stop the spread of the virus. Central to such uses of data will be maintaining consumer trust and committing to responsibly using information in ways that will improve the public response to COVID-19.

- 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**

² See Dennis Buchheim and Jordan Mitchell, *Project Rearch: An Industry Collaboration to Rearchitect Digital Marketing* (Feb. 12, 2020), located at <https://www.iab.com/blog/project-rearch-an-industry-collaboration-to-rearchitect-digital-marketing/>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

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

RESPONSE: The IAB and its members have been at the forefront of promoting responsible data practices, and consumer trust is vital to our member companies' ability to operate successfully in the marketplace. Companies should collect, use, and maintain data in a manner that is consistent with existing laws and industry codes of conduct including in a manner that is consistent with notices and permissions acquired at the time of collection. The use of anonymized or de-identified data provides meaningful privacy protections for individuals while offering useful insights to public health professionals. Privacy laws such as the Health Insurance Portability and Accountability Act (HIPAA) have recognized the benefits of anonymization and de-identification techniques. The Privacy for America framework also provides de-identification standards. We invite you to consider our proposed framework at <https://www.privacyforamerica.com/overview/principles-for-privacy-legislation-dec-2019/>.

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?

RESPONSE: Over the last thirty years, the Internet has become entwined into our daily lives, transforming how we shop, communicate, connect, do business, and consume content. However, the vital role the Internet plays in every day life has become more acute as Americans engage in social distancing and work from home.

The Internet is perhaps the most powerful and empowering mode of communication and commerce ever invented, and the data derived through it creates untold opportunities for societal good and economic growth. Advertising has helped power its growth for decades by delivering innovative tools and services for individuals and businesses to connect and communicate and by underpinning the content and services individuals

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

expect and rely on, including video, news, music, and more. As a result of this advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits.

People, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to create their own platforms to reach millions of their fellow citizens. Individuals are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored experience. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. In fact, a DAA-commissioned Zogby survey found that consumers attributed a value of nearly \$1,200 a year to common online ad-supported services, like news, weather, video content, and social media.³ A large majority of surveyed consumers (85 percent) like the ad-supported model, and 75 percent said they would greatly decrease their use of the Internet were they required to pay hundreds of dollars a year for currently free content.⁴ Indeed, as the Federal Trade Commission (“FTC”) noted in its comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.⁵ This is particularly relevant in today’s economically challenging times when obtaining information about the coronavirus is critical.

To ensure every American can continue to share in the benefits of the Internet, it is vital that there be a national standard privacy standard. We strongly believe all Americans—no matter where they live in the country—deserve strong privacy protections. This is why IAB supports Privacy for America, an industry coalition of leading trade organizations and businesses that encompass a wide swath of the American economy and advocate for broadly applicable federal privacy legislation.⁶ We believe data privacy is best achieved through a new federal approach that comprehensively describes clear, workable, and consistent standards that consumers, businesses, and law enforcers can rely upon. While IAB cannot speak to any one company’s practices, we support the transparency requirements provided in Privacy for America as well as industry self-regulatory codes of conduct, such as the DAA Principles.

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

³ Zogby Analytics, *Public Opinion Survey On Value Of The Ad-Supported Internet* (May 2016) https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/ZogbyAnalyticsConsumerValueStudy2016.pdf.

⁴ *Id.*

⁵ Federal Trade Commission, *In re Developing the Administration’s Approach to Consumer Privacy*, 15 (Nov. 13, 2018) https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

⁶ *Privacy for America*, located at <https://www.privacyforamerica.com/>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

engaging in data minimization and strategic deletion practices after data is used or transferred?

RESPONSE: Currently, data privacy in the United States is regulated by sectoral privacy laws such as the Health Insurance Portability and Accountability Act (HIPAA), the Children’s Online Privacy Protection Act (COPPA), the Gramm-Leach-Bliley Act (GLBA) and others that provide legally enforceable requirements for maintaining consumer privacy. These sectoral laws serve as important safeguards that are in addition to the Federal Trade Commission’s ability to enforce against companies for failing to abide by their public promises related to data. This legal framework is complimented by self-regulatory codes of conduct backed by accountability programs including the DAA Principles, as enforced by the Better Business Bureau.

While self-regulation has been a useful mechanism to encourage responsible data use, federal leadership is now needed to ensure that robust consumer privacy protections apply consistently throughout the country. The time is right for the creation of a new paradigm for data privacy in the United States. To this end, IAB is a key supporter of Privacy for America, a broad industry coalition of top trade organizations and companies representing a wide cross-section of the American economy that advocates for federal omnibus privacy legislation.⁷ Privacy for America has released a detailed policy framework to provide members of Congress with a new option to consider as they develop data privacy legislation for the United States.⁸ The Privacy for America framework recognizes the importance of incorporating compliance plans to reduce privacy risks to individuals by requiring the development and implementation of a reasonable process to ensure compliance. Participants in Privacy for America have met with leaders of Congress, the FTC, the Department of Commerce, the White House, and other key stakeholders to discuss the ways the framework protects consumers while also ensuring that beneficial uses of data can continue to provide vast benefits to the economy and mankind.

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.**

⁷ Privacy for America, located at <https://www.privacyforamerica.com/>.

⁸ Privacy for America Releases Detailed Policy Framework to Provide Strong Data Privacy Protections for All Americans (Dec. 3, 2019), located at <https://www.privacyforamerica.com/detailed-policy-framework-to-provide-strong-data-privacy-protections/>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

- **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.**

RESPONSE: As explained in my testimony, data can play a significant role in our nation's response to the COVID-19 pandemic. Researchers, government officials, academicians, public health workers, and other stakeholders are harnessing the power of data to leverage the value it can provide in the response to the virus. There is also evidence of data being used in privacy protective ways to provide meaningful insights to the public. For instance, data can be used to show which public spaces are still attracting large crowds to better inform policies. With this data, for instance, public health experts, NGOs, academics, and governments can better understand how to structure stay-at-home orders and essential business exceptions, so communities are less at risk. Data can also be used to observe whether stay-at-home orders are having an impact through heat maps and foot traffic to enable analysis of aggregate, anonymous individual movements. This data can be vital to public health experts in understanding which policies work and to better protect citizens while preserving individual privacy. Companies that conduct and analyze location intelligence, with the appropriate care for user privacy and data sanitization, can be a critical ally in the fight against COVID-19.

IAB companies are using maps to help monitor movements of individuals affected by COVID-19, to discover patterns that are leading to the spread of the virus, and to also identify areas that could be affected. Aggregated mobility reports, issued by leading data companies, are broken down by location and display the change in visits to places like grocery stores and parks.⁹ These reports and maps help inform disease forecasting efforts and protective measures, and have become an indispensable tool for public health professionals on the front lines of COVID-19 analysis and prevention. As privacy technologists have highlighted, the use of aggregated location data by businesses and health experts from the examples above provides meaningful privacy protections for individuals.¹⁰

Data can also help government agencies, hospitals, and other critical organizations better manage the dramatic increase in demand that they are currently experiencing. For example, businesses are making available artificial intelligence and natural language processing services to assist workers in fielding the large volume of calls, emails, and inquiries that they are receiving, and efficiently prioritize the most urgent requests and

⁹ James Glanz, Benedict Carey, Josh Holder, Derek Watkins, Jennifer Valentino-DeVries, Rick Rojas and Lauren Leatherby, *Where America Didn't Stay Home Even as the Virus Spread*, N.Y. TIMES (Apr. 2, 2020), located at <https://www.nytimes.com/interactive/2020/04/02/us/coronavirus-social-distancing.html>.

¹⁰ See Jacob Hoffman-Andrews and Andrew Crocker, *How to Protect Privacy When Aggregating Location Data to Fight COVID-19*, EFF (Apr. 6, 2020), located at <https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

information.¹¹ And social media websites that have an understanding of social connections across different geographies can find aggregate trends to help researchers gain better insights about when and where the coronavirus might spread more quickly.¹² Together, these big data applications, and the countless others that are currently being developed, have significant positive benefits at this critical time. They empower first responders and healthcare workers to most efficiently use their limited resources to save the lives of the greatest number of individuals. They also enable researchers and public health officials to better anticipate health outbreaks and take appropriate preventative measures at the right time and place. And they facilitate all of this in the most efficient way that causes the least possible disruption to Americans lives and livelihoods. Applying big data to this crisis can help everyone involved in the coronavirus response take decisive actions and develop effective solutions based on real-time information at scale.

We encourage stakeholders to explore additional applications for data in preventing the spread of COVID-19 and ensure data is being applied in a way that is consistent with constitutional ideals, laws, and self-regulatory codes.

9. COVID-19 has caused private companies to seek out and utilize health data in an effort to protect users, employees, and the general public from the spread of the virus. Both Apple and Alphabet have released websites to help users self-screen for exposure to COVID-19. This data will be used to help public health officials. However, these tools also allow technology companies access to user's health information which the companies could in turn profit from in the future.

- **How are technology companies balancing the need for timely and robust reporting to prevent the spread of the virus with the confidentiality and privacy of the participants?**
- **What safeguards are in place to ensure data collected as part of the fight against COVID-19 are not sold to business partners or used for the development of other commercial products?**

RESPONSE: Data can be a vital asset for societal good. It has the power to facilitate useful insights and trends that can inform policymaking, crisis response, and the discovery of cures, as well as keep citizenry informed and enable access to vital services and communication channels. Like many industries, the data industry is a critical piece of our nation's response to the health pandemic. Public-private partnerships to discover beneficial uses of information that can strengthen the public health response will be of considerable importance during this unprecedented time.

¹¹ Melody Petersen and Emily Baumgaertner, *Bottlenecks in coronavirus testing mean excruciating wait times for the sick*, LA TIMES (Mar. 30, 2020), located at <https://www.latimes.com/business/story/2020-03-30/its-taking-up-to-eight-days-to-get-coronavirus-tests-results-heres-why>.

¹² Christina Farr, *Facebook is developing new tools for researchers to track if social distancing is working*, CNBC (Apr. 6, 2020), located at <https://www.cnbc.com/2020/04/06/facebook-to-help-researchers-track-if-social-distancing-is-working.html>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

Privacy and responsible data practices apply even in times of crisis. Consumers, businesses, and the broader public need clear standards. For this reason, IAB supports Privacy for America. Privacy for America has developed a new framework for nationwide privacy legislation that would fundamentally change the way personal data is protected and secured in this country. This framework is intended to provide a new option to policy makers for their consideration as they address this important issue. Unlike existing domestic and international approaches to privacy regulation, the framework would not rely on burdensome “notice and choice” schemes to protect personal data. Rather, it would clearly define and prohibit 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.

Notably, the new framework would shift the burden away from individuals to read hundreds of lengthy privacy policies to protect themselves and toward a common set of data privacy and security norms. To ensure widespread compliance and rigorous enforcement, the framework would significantly expand federal and state oversight of data practices, including by creating a new data protection bureau at the Federal Trade Commission (“FTC”), authorizing FTC rulemaking in certain key areas, and providing civil penalty authority to both the FTC and State Attorneys General.

10. Anonymization techniques are also critical for safeguarding consumers’ privacy. Truly anonymized data can protect a consumer’s personal information, like their geolocation, political opinions, or religious beliefs.

How do companies guarantee that every dataset they are storing contains truly anonymous data? And is the ability to re-identify data a part of the discussion in data-sharing arrangements?

RESPONSE: Data brings tremendous value to society. It has the power to facilitate useful insights and trends that can inform policymaking, crisis response, and the discovery of cures, as well as keep citizenry informed and enable access to vital services and communication channels. One driving force in this ecosystem is data-driven advertising. Advertising has helped power the growth of the Internet for decades by delivering innovative tools and services for individuals and businesses to connect and communicate and by underpinning the content and services individuals expect and rely on, including video, news, music, and more.

Companies maintain varying data sets, some of which may be anonymized while others are not. For example, an e-commerce platform may maintain a consumer’s billing and mailing information so that the consumer may transact and receive products from the e-commerce seller. Other data sets may involve anonymized or deidentified data. For instance, in recent weeks there have been public reports on how such data sets are helping to address COVID-19. IAB companies are using maps to help monitor movements of individuals affected by COVID-19, to discover patterns that are leading to the spread of the virus, and to also identify areas that could be affected. Aggregated mobility reports,

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

issued by leading data companies, are broken down by location and display the change in visits to places like grocery stores and parks.¹³ These reports and maps help inform disease forecasting efforts and protective measures, and have become an indispensable tool for public health professionals on the front lines of COVID-19 analysis and prevention. As privacy technologists have highlighted, the use of aggregated location data by businesses and health experts from the examples above provides meaningful privacy protections for individuals.¹⁴

Data can also help government agencies, hospitals, and other critical organizations better manage the dramatic increase in demand that they are currently experiencing. For example, businesses are making available artificial intelligence and natural language processing services to assist workers in fielding the large volume of calls, emails, and inquiries that they are receiving, and efficiently prioritize the most urgent requests and information.¹⁵ And social media websites that have an understanding of social connections across different geographies can find aggregate trends to help researchers gain better insights about when and where the coronavirus might spread more quickly.¹⁶

Together, these big data applications, and the countless others that are being developed at this time, have significant positive benefits during this critical period. They empower first responders and healthcare workers to most efficiently use their limited resources to save the lives of the greatest number of individuals. They also enable researchers and public health officials to better anticipate health outbreaks and take appropriate preventative measures at the right time and place. And they facilitate all of this in the most efficient way that causes the least possible disruption to Americans lives and livelihoods.

Applying big data to this crisis can help everyone involved in the coronavirus response take decisive actions and develop effective solutions based on real-time information at scale.

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

¹³ James Glanz, Benedict Carey, Josh Holder, Derek Watkins, Jennifer Valentino-DeVries, Rick Rojas and Lauren Leatherby, *Where America Didn't Stay Home Even as the Virus Spread*, N.Y. TIMES (Apr. 2, 2020), located at <https://www.nytimes.com/interactive/2020/04/02/us/coronavirus-social-distancing.html>.

¹⁴ See Jacob Hoffman-Andrews and Andrew Crocker, *How to Protect Privacy When Aggregating Location Data to Fight COVID-19*, EFF (Apr. 6, 2020), located at <https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19>.

¹⁵ Melody Petersen and Emily Baumgaertner, *Bottlenecks in coronavirus testing mean excruciating wait times for the sick*, LA TIMES (Mar. 30, 2020), located at <https://www.latimes.com/business/story/2020-03-30/its-taking-up-to-eight-days-to-get-coronavirus-tests-results-heres-why>.

¹⁶ Christina Farr, *Facebook is developing new tools for researchers to track if social distancing is working*, CNBC (Apr. 6, 2020), located at <https://www.cnbc.com/2020/04/06/facebook-to-help-researchers-track-if-social-distancing-is-working.html>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

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 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?

RESPONSE: Data privacy in the United States is regulated by sectoral privacy laws such as the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), the Gramm-Leach-Bliley Act (GLBA) and others that provide legally enforceable requirements for maintaining consumer privacy. These sectoral laws serve as important safeguards that are in addition to the Federal Trade Commission's ability to enforce under various laws. This legal framework is complimented by self-regulatory codes of conduct backed by accountability programs including the DAA Principles, as enforced by the Better Business Bureau.

While self-regulation has been a useful mechanism to encourage responsible data use, federal leadership is now needed to ensure that robust consumer privacy protections apply consistently throughout the country. IAB is a key supporter of Privacy for America, a broad industry coalition of top trade organizations and companies representing a wide cross-section of the American economy that advocates for federal omnibus privacy legislation.¹⁷ Privacy for America has released a detailed policy framework to provide members of Congress with a new option to consider as they develop data privacy legislation for the United States.¹⁸ Participants in Privacy for America have met with leaders of Congress, the FTC, the Department of Commerce, the White House, and other key stakeholders to discuss the ways the framework protects

¹⁷ *Privacy for America*, located at <https://www.privacyforamerica.com/>.

¹⁸ *Privacy for America Releases Detailed Policy Framework to Provide Strong Data Privacy Protections for All Americans* (Dec. 3, 2019), located at <https://www.privacyforamerica.com/detailed-policy-framework-to-provide-strong-data-privacy-protections/>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

consumers while also ensuring that beneficial uses of data can continue to provide vast benefits to the economy and mankind. Our proposed approach comprehensively describes clear, workable, and consistent standards that consumers, businesses, and law enforcers can rely upon. Without a consistent federal privacy standard, a patchwork of state privacy laws will create consumer confusion, present substantial challenges for businesses trying to comply with these laws, and fail to meet consumers' expectations about their digital privacy.

Privacy for America has developed a new framework for nationwide privacy legislation that would fundamentally change the way personal data is protected and secured in this country. Unlike existing domestic and international approaches to privacy regulation, the framework would not rely on burdensome "notice and choice" schemes to protect personal data. Rather, it would clearly define and prohibit 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.

Notably, the new framework would shift the burden away from individuals to read hundreds of lengthy privacy policies to protect themselves and toward a common set of data privacy and security norms. To the extent appropriate, we encourage the Committee to consider these principles as it develops legislation, and considers the nation's response to COVID-19.

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?

RESPONSE: Data brings tremendous value to society. It has the power to facilitate useful insights and trends that can inform policymaking, crisis response, and the discovery of cures, as well as keep citizenry informed and enable access to vital services and communication channels. In some contexts, de-identified data sets may not be effective because identifiable information is vital to the data use. For instance, when a company transacts with a customer online, it must collect the customer's mailing address in order to deliver the requested product. In other circumstances, the output from data may not need to include identifying information for it to be useful. For example, it has been reported that companies are monitoring movements of individuals affected by COVID-19 to discover patterns that are leading to the spread of the virus, and to also identify areas that could be affected. These aggregated mobility reports, issued by leading data companies, are broken down by location and display the change in visits to places like grocery stores and parks.¹⁹ The reports do not reveal identifying information, and would not alone enable the development of "contact tracing" systems that have been

¹⁹ James Glanz, Benedict Carey, Josh Holder, Derek Watkins, Jennifer Valentino-DeVries, Rick Rojas and Lauren Leatherby, *Where America Didn't Stay Home Even as the Virus Spread*, N.Y. TIMES (Apr. 2, 2020), located at <https://www.nytimes.com/interactive/2020/04/02/us/coronavirus-social-distancing.html>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

reported in other countries.²⁰ This use of aggregated information can show important trends and demonstrate useful patterns. With this data, for instance, public health experts, NGOs, academics, and governments can better understand how to structure stay-at-home orders and essential business exceptions for COVID-19, so communities are less at risk.

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?

RESPONSE: IAB represents media companies and supports them in engaging in responsible advertising practices and protecting consumer privacy. In response to the pandemic, the advertising industry has stepped forward to provide important assistance to support the government response to COVID-19. Industry members have facilitated vital public health messaging about the virus by donating ad inventory, contributing millions in media dollars, providing graphic design collateral, and offering marketing expertise.²¹ Media companies have provided a crucial public service of fostering a sense of community to unite people through effective social movements to keep our communities connected and healthy.²² Advertising technology providers are also supporting states and health organizations by preventing ad spend from reaching websites that disseminate false information regarding the COVID-19 emergency.²³

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—

²⁰ Jennifer Valentino-DeVries, *Translating a Surveillance Tool into a Virus Tracker for Democracies*, N.Y. TIMES (Mar. 19, 2020), located at <https://www.nytimes.com/2020/03/19/us/coronavirus-location-tracking.html>.

²¹ Marty Stewart, *The Ad Council’s COVID-19 Campaign Is Its Largest Effort Yet*, FORBES (Mar. 31, 2020), located at <https://www.forbes.com/sites/martyswant/2020/03/31/the-ad-councils-covid-19-campaign-is-its-largest-effort-yet/#7c40ef095c8e>.

²² Jeanine Poggi, *ViacomCBS Promotes Being “Alone Together” in COVID-19 PSA*, ADAGE (Mar. 17, 2020), located at <https://adage.com/creativity/work/viacomcbs-alone-together/2244816>.

²³ *Supporting Journalism During COVID-19*, AMOBEE (Apr. 2, 2020), located at <https://www.amobee.com/blog/supporting-journalism-during-covid-19/>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

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?

RESPONSE: IAB is supportive of exploring and considering all ideas and reasonable uses of data to address the COVID-19 pandemic. We would welcome efforts facilitating research into ways we can save American lives and stop the spread of the virus while engaging in responsible data practices.

- 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 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?

RESPONSE: The National Infectious Disease Forecasting Center idea is innovative, and we are supportive of such innovative thinking regarding ways to leverage the great asset that is data during this challenging time. In general terms, tactics such as pseudonymization, deidentification, anonymization, and aggregation can be helpful for discerning useful models while protecting consumer privacy. We encourage identifying ways for the public and private stakeholders to partner to leverage data in the fight against COVID-19.

- 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?

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

RESPONSE: IAB strongly believes now is the time to consider new and potentially transformative ways that data can aid in the fight against COVID-19. IAB would caution against closing the door to specific data uses that could potentially have broad utility without fully considering those uses and exploring their possibilities. Congress and government agencies should continue to look for ways to partner with private industry to see what resources and assets can be leveraged to save lives and minimize the impact of the virus.

IAB also encourages Congress to act to provide consistent, enforceable, and clear privacy protections for all Americans. IAB supports Privacy for America, a new framework for nationwide privacy legislation that would fundamentally change the way personal data is protected and secured in this country. This framework is intended to provide a new option to policy makers for their consideration as they address this important issue. Unlike existing domestic and international approaches to privacy regulation, the framework would not rely on notice and choice schemes to protect personal data. Rather, it would clearly define and prohibit 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.

Sen. Moran

17. 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?

RESPONSE: IAB is a key supporter of Privacy for America, a broad industry coalition of top trade organizations and companies representing a wide cross-section of the American economy that advocates for federal omnibus privacy legislation.²⁴ Privacy for America has released a detailed policy framework to provide members of Congress with a new option to consider as they develop data privacy legislation for the United States.²⁵ Participants in Privacy for America have met with leaders of Congress, the FTC, the

²⁴ *Privacy for America*, located at <https://www.privacyforamerica.com/>.

²⁵ *Privacy for America Releases Detailed Policy Framework to Provide Strong Data Privacy Protections for All Americans* (Dec. 3, 2019), located at <https://www.privacyforamerica.com/detailed-policy-framework-to-provide-strong-data-privacy-protections/>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

Department of Commerce, the White House, and other key stakeholders to discuss the ways the framework protects consumers while also ensuring that beneficial uses of data can continue to provide vast benefits to the economy and mankind. As part of this framework, Privacy for America provides de-identification standards. We invite you to consider our proposed framework at

<https://www.privacyforamerica.com/overview/principles-for-privacy-legislation-dec-2019/>.

- 18. 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?**

RESPONSE: The United States is a global leader in the digital ecosystem for a reason. We have found ways to leverage data to create innovative products and services that have bettered consumers' lives and society. IAB and our members see the value and benefit data can bring in the current extraordinarily challenging circumstances.

To support efforts to combat the spread of the virus, advertising has enabled COVID-19-related information to reach audiences in specific communities, which can increase the impact of informational messages and their relevancy. For example, radio and other campaigns facilitated through the Ad Council's partnership with the New York government direct individuals to state-specific information about COVID-19.²⁶ U.S. Internet providers—through which we access news and information services—are also proactively supporting their communities. By giving away free, high-speed Internet to low-income families, educational content for children, and unlimited data, they too are working to keep us connected with friends and family while we remain physically isolated.²⁷

While IAB members are responsible stewards of data, IAB strongly believes Congress should enact uniform data privacy standards for the nation. In support of this goal, IAB is a key proponent of Privacy for America, a framework for federal privacy legislation that would clearly define reasonable and unreasonable data practices.²⁸ The framework would apply to virtually all personal information collected and used in the United States

²⁶ Ad Council, *Coronavirus Response Campaign Toolkit, New York State*, located at <http://coronavirus.adcouncilkit.org/newyork/>.

²⁷ David Matthews, *These are the internet providers offering free WiFi during coronavirus*, NEW YORK DAILY NEWS (Mar. 15, 2020), located at <https://www.nydailynews.com/coronavirus/ny-coronavirus-internet-providers-free-wifi-20200315-6k7pzukriffdfcic5odfizmnrri-story.html>.

²⁸ *Privacy for America*, located at <https://www.privacyforamerica.com/>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

and practically all companies doing business here. It would prohibit a range of practices that make personal data vulnerable to misuse, such as eligibility determinations, discrimination, fraud and deception, and stalking. Many of these prohibitions would apply not only to companies that engage in these harmful practices directly, but to suppliers of data who have reason to know that the personal information will be used for these purposes. Privacy for America would also provide special protections for individuals over 12 and under 16 years of age, and it would require express consent for certain “sensitive data,” such as health, biometric, and geolocation information.

19. 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?

RESPONSE: Consumer trust is vital to enabling data in the fight against COVID-19. Through our industry codes of conduct, such as the Digital Advertising Alliance Principles, our members are expected to comply with best practices by providing consumers enhanced transparency and control. We believe that lessons learned from self-regulatory codes’ approach to consumer disclosures, choices, and trust are vital during ordinary times as well as times of crisis.

20. 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?

RESPONSE: Data security is a critical part of business operations to help protect information from unauthorized access or acquisition. IAB is a key supporter of Privacy for America, a broad industry coalition of top trade organizations and companies representing a wide cross-section of the American economy that advocates for federal omnibus privacy legislation.²⁹ Privacy for America’s approach would require companies to implement a risk-based data security program. Such a program would vary based on the risks faced by a particular company, but would require certain essential elements such as risk assessment, employee training, and incident response.

Sen. Blackburn

21. How do you see HIPPA interacting with your worldview of the tech industry?

²⁹ *Privacy for America*, located at <https://www.privacyforamerica.com/>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

RESPONSE: HIPAA and other federal sectoral laws should be respected at all times, especially in times of crisis like the present. These sectoral laws will continue to apply as we move forward to identify innovative ways to leverage data to fight the spread of COVID-19, and they should be followed.

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

RESPONSE: We are aware of the CDC program from reports in the media, and we look forward to learning more about it as the program develops.

The IAB represents media companies that engage in and facilitate advertising. Our members strive to abide by existing law and self-regulatory codes of conduct, such as the Digital Advertising Alliance Principles, which provide consumers with transparency and choice regarding businesses’ use of data. We encourage public and private stakeholders to identify ways to work together in the response to COVID-19.

- 23. 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?**

RESPONSE: To provide protections for consumers during the pandemic, IAB would support Congress in establishing a strong national framework that offers consistent privacy protections for Americans. Specifically, IAB supports the Privacy for America framework for federal data privacy legislation. This approach would harmonize privacy protections for individuals across the country and would provide clear rules of the road for businesses by setting forth specific prohibited uses of data. The framework would acknowledge that other certain data practices are essential and expected in daily life—to protect individuals and property from harm, to further health and safety, and to enable individuals to obtain products and services they have specifically requested. The Privacy for America framework also encompasses data deletion and could therefore provide helpful guiding principles in relation to the use of data in the fight against COVID-19.

- 24. Foreign countries like South Korea, Taiwan, Singapore, and Israel swiftly mobilized collection of cell phone location data to track the spread of the virus and map out infection hot zones. Israel just released an app that allows the public to track whether they have may visited a location that put them into contact with an infected**

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

individual. Is it even possible to adopt similar measures while still balancing protections for privacy and civil liberties?

RESPONSE: IAB believes that privacy protections can exist while enabling new and innovative uses of data to combat COVID-19. It is for this reason that IAB is a key supporter of Privacy for America. Privacy for America has developed a new framework for nationwide privacy legislation that would fundamentally change the way personal data is protected and secured in this country. This framework is intended to provide a new option to policy makers for their consideration as they address this important issue. Unlike existing domestic and international approaches to privacy regulation, the framework would not rely on burdensome “notice and choice” schemes to protect personal data. Rather, it would clearly define and prohibit 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.

Notably, the new framework would shift the burden away from individuals to read hundreds of lengthy privacy policies to protect themselves and toward a common set of data privacy and security norms. To ensure widespread compliance and rigorous enforcement, the framework would significantly expand federal and state oversight of data practices, including by creating a new data protection bureau at the Federal Trade Commission (“FTC”), authorizing FTC rulemaking in certain key areas, and providing civil penalty authority to both the FTC and State Attorneys General.

Sen. Capito

25. An increasing number of consumers are spending time online to make conference calls, complete school work, order groceries and supplies, and stay connected. We can expect bad actors and scammers to follow this trend.

What steps are you taking to ensure that the ad ecosystem is safe and free of fraud for users both young and old?

RESPONSE: IAB has long-supported efforts to combat fraud in the ad supply-chain. For instance, IAB is proud to support the Trustworthy Accountability Group (“TAG”), a first-of-its-kind cross-industry accountability program designed to create transparency in the business relationships and transactions that undergird the digital ad industry, while continuing to enable innovation.³⁰ TAG focuses its efforts on four core areas: eliminating fraudulent digital advertising traffic, combating malware, fighting ad-supported Internet piracy to promote brand integrity, and promoting brand safety through greater transparency. Working with key experts in the industry, TAG creates and maintains voluntary certification programs, tools, and protocols to help prepare companies in the digital advertising supply chain to effectively and collaboratively combat fraud. In addition, as noted in our testimony, advertising technology providers have worked to

³⁰ *Trustworthy Accountability Group*, located at <https://www.tagtoday.net>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

prevent ad spend from reaching websites that author fake news or misinformation regarding the COVID-19 pandemic.³¹

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?

RESPONSE: As known to us and noted in our testimony, companies are using data in privacy-protective ways to provide meaningful insights to the public about COVID-19. For example, IAB member companies have used aggregated data to develop mobility reports, which visually display the changes in visits to places like essential businesses or public spaces in a given location.³² These insights can help governments and health officials evaluate the efficacy of stay at home orders or identify patterns that could lead to further spread of the virus.

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?**
- **Certain data may not necessarily be considered personally identifiable, but with enough data points, you could identify a specific person. How can we ensure that data is truly anonymous and is not traceable back to an individual person?**
- **Can effective contact tracing be conducted with “anonymized data”? Or will it require personally identifiable information?**

RESPONSE: IAB represents media companies engaged in digital advertising. We know that providing visualization maps that show insights from data, rather than providing the data itself, is one meaningful way for governments and health officials to frame their responses to COVID-19.³³ This approach provides data insights from aggregated, anonymized data rather than individually identifiable personal information. Companies apply de-identification techniques like those promulgated by

³¹ *Supporting Journalism During COVID-19*, AMOBEE (Apr. 2, 2020), located at <https://www.amobee.com/blog/supporting-journalism-during-covid-19/>.

³² James Glanz, Benedict Carey, Josh Holder, Derek Watkins, Jennifer Valentino-DeVries, Rick Rojas and Lauren Leatherby, *Where America Didn't Stay Home Even as the Virus Spread*, N.Y. TIMES (Apr. 2, 2020), located at <https://www.nytimes.com/interactive/2020/04/02/us/coronavirus-social-distancing.html>

³³ James Glanz, Benedict Carey, Josh Holder, Derek Watkins, Jennifer Valentino-DeVries, Rick Rojas and Lauren Leatherby, *Where America Didn't Stay Home Even as the Virus Spread*, N.Y. TIMES (Apr. 2, 2020), located at <https://www.nytimes.com/interactive/2020/04/02/us/coronavirus-social-distancing.html>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

the Digital Advertising Alliance.³⁴ The techniques are often backed by contractual restrictions between partners limiting re-identification.

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?**

RESPONSE: The IAB is not aware of any specific arrangements or the details of any specific arrangements.

- **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?**

RESPONSE: To our knowledge, no federal, state, or local law enforcement has used private sector collected data to enforce COVID-19 related government orders or requirements.

Sen. Scott

29. 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?

RESPONSE: We believe that data is a vital and valuable asset in the response to COVID-19. The digital advertising industry is essential to the response to the pandemic. Our industry has offered services, content, and connectivity to consumers for free or a reduced cost, enabling individuals to receive news, public health alerts, and

³⁴ See e.g. DAA, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/seven-principles-07-01-09.pdf; DAA, *Self-Regulatory Principles for Multi-Site Data* (Nov. 2011), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/Multi-Site-Data-Principles.pdf; DAA, *Application of Self-Regulatory Principles to the Mobile Environment* (Jul. 2013), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/DAA_Mobile_Guidance.pdf.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

announcements related to COVID-19.³⁵ We believe that advertising and data can play a significant role in the response against coronavirus provided that it the data is used in a privacy protective manner.

Ranking Member Cantwell

30. Science and technology will be critical drivers of our response to COVID-19, and we have seen many examples of data being used in positive ways – from the University of Washington’s forecasts of hospital needs to Johns Hopkins’ maps of disease spread. These are leading examples of how firms can innovate while protecting other equities, like privacy. What recommendations do you have to encourage further innovation to fight the virus? How do we encourage technologists to help people transition to regular life while preparing for future pandemic incidents? What are the best practices you have seen in innovating in the fight against COVID-19 that support privacy rights?

RESPONSE: As noted in our testimony, data can provide meaningful insights to the public while also being used in a privacy protective way. For instance, our members have used data visualization to provide insights on the effect of stay-at-home orders and other policies while protecting individual privacy by enabling analysis of aggregate, anonymous individual movements. The use of aggregated data provides meaningful privacy protections for individuals while providing useful insights to public health professionals.³⁶ We understand that some data may be more useful in a non-anonymized form and when this is the case, this data should be used in a way that is consistent with the applicable legal requirements and mindful of individual privacy.

31. 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?

RESPONSE: IAB believes that a federal privacy standard is necessary to ensure that all Americans benefit from uniform privacy protections, which may define these terms, while enabling the economic benefits that data use can provide. IAB is a key supporter of Privacy for America, a broad industry coalition of top trade organizations and companies that advocates for federal omnibus privacy legislation.³⁷ Privacy for America released a detailed policy framework to guide members of Congress as they develop

³⁵ See Dave Grimaldi, *Good Works: IAB & Tech Lab Members vs. Coronavirus*, (Mar. 25, 2020), located at <https://www.iab.com/blog/good-works/> (providing a partial list of the good works our IAB and IAB Tech Lab members are doing to help the world during this COVID-19 pandemic).

³⁶ See Jacob Hoffman-Andrews and Andrew Crocker, *How to Protect Privacy When Aggregating Location Data to Fight COVID-19*, EFF (Apr. 6, 2020), located at <https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19>.

³⁷ *Privacy for America*, located at <https://www.privacyforamerica.com/>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

federal privacy legislation. The framework proposed by Privacy for America provides prohibitions on certain kinds of harmful data uses and conduct while enabling uses that can inform responses to public health emergencies. The framework would prohibit a range of practices that make personal data vulnerable to misuse, rather than allow individuals to consent to harmful uses. By providing strong safeguards to individuals and providing clear guidelines to businesses, companies can use data for the benefit of all consumers.

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.”³⁸**
- **New York Times, “Twelve Million Phones, One Dataset, Zero Privacy.”³⁹**
- **Motherboard, “Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years.”⁴⁰**
- **Motherboard, “I Gave a Bounty Hunter \$300. Then He Located Our Phone”⁴¹**
- **Boston Globe, “Every step you take.”⁴²**
- **Vox, “Law enforcement is now buying cellphone location data from marketers.”⁴³**

32. 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

³⁸ <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>

³⁹ <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>

⁴⁰ https://www.vice.com/en_us/article/43z3dn/hundreds-bounty-hunters-att-tmobile-sprint-customer-location-data-years

⁴¹ https://www.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile

⁴² <https://apps.bostonglobe.com/business/graphics/2018/07/foot-traffic/>

⁴³ <https://www.vox.com/recode/2020/2/7/21127911/ice-border-cellphone-data-tracking-department-homeland-security-immigration>

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

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?

RESPONSE: The IAB played an integral role in the creation of self-regulatory systems administered by the Digital Advertising Alliance (“DAA”). The DAA is an industry body that creates a self-regulatory code for all companies that collect or use data for interest-based online advertising, based on practices recommended by the FTC in its 2009 report on online behavioral advertising.⁴⁴ These rules, known as the DAA Principles, provide transparency and consumer control over data collection and use of web viewing data, application use data, precise location data, and personal directory data.⁴⁵ The DAA Principles are independently monitored and enforced by the Council of Better Business Bureau National Programs’ Digital Advertising Accountability Program (“Accountability Program”). The Accountability Program processes thousands of consumer complaints each year and opens formal inquiries into companies that may be in violation of the DAA Principles. Since its inception in 2011, the Accountability Program has published the results of more than 100 actions applying the DAA Principles.⁴⁶

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.

⁴⁴ DAA, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/seven-principles-07-01-09.pdf; FTC, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009), located at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>.

⁴⁵ DAA, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/seven-principles-07-01-09.pdf; DAA, *Self-Regulatory Principles for Multi-Site Data* (Nov. 2011), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/Multi-Site-Data-Principles.pdf (hereinafter “MSD”); DAA, *Application of Self-Regulatory Principles to the Mobile Environment* (Jul. 2013), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/DAA_Mobile_Guidance.pdf (hereinafter, “Mobile”).

⁴⁶ BBB National Programs, Inc., *Accountability Program Decisions and Guidance*, located at <http://asrcreviews.org/accountability-program-decisions/>.

- 33. 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?**

RESPONSE: Data is an essential part of every business' operations and it is gathered in many different ways to provide products and services to consumers. In this time of crisis, the free flow of data plays an essential role in enabling millions of individuals to access important news and public health information for free or at a low cost, while providing government and public health officials with key insights regarding the spread of the virus. Our members receive data through various channels, means, and sources. For example, data may be available by a consumer during her engagement with a business such as shopping through an e-commerce platform or by using a service such as listening to music through a streaming service. We have not inventoried the data practices of each of our members. However, the DAA Principles require business engaged in online data collection to provide enhanced transparency and control with respect to the use of data for interest-based advertising. The DAA Principles also impose restrictions on the use of covered data for eligibility purposes.⁴⁷ While the IAB believes that self-regulation has been useful for encouraging responsible data use, we believe that it is time for federal legislation that would provide uniform privacy protections from state-to-state. IAB supports Privacy for America, a broad industry coalition of top trade organizations and companies representing a wide cross-section of the American economy that advocates for federal omnibus privacy legislation.⁴⁸ The framework proposed by Privacy for America would provide clear rules to prohibit practices that make personal data vulnerable to misuse while preserving the benefits to users and the economy that result from the responsible use of data.

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.

- 34. 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**

⁴⁷ DAA, *MSD* at 4-5 (Nov. 2011); DAA, *Mobile* at 31-32 (Jul. 2013);

⁴⁸ *Privacy for America*, located at <https://www.privacyforamerica.com/>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

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?

RESPONSE: IAB believes that data, when subject to appropriate privacy protections, can play an important role in supporting the fight against COVID-19. In order to do this effectively, a federal privacy standard is necessary to ensure that all Americans benefit from uniform privacy protections while enabling the economic benefits that data use can provide. IAB supports Privacy for America, an industry coalition of top trade organizations and companies representing a wide cross-section of the American economy that advocates for broadly applicable federal privacy legislation.⁴⁹ Privacy for America released a detailed policy framework to guide members of Congress as they develop federal privacy legislation. The framework proposed by Privacy for America provides prohibitions on certain kinds of harmful data uses and conduct while enabling uses that can inform responses to public health emergencies. The framework would prohibit a range of practices that make personal data vulnerable to misuse, rather than allow individuals to consent to harmful uses. The framework also calls for new safeguards for health-related data and services. By providing strong safeguards to individuals and clear guidelines to businesses, companies can use data for the benefit of all consumers.

Sen. Schatz

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

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

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

RESPONSE: IAB believes that a federal privacy standard is necessary to ensure that all Americans benefit from uniform privacy protections while enabling the economic benefits that data use can provide. IAB supports Privacy for America, a new framework for federal privacy legislation that would provide privacy protections for consumers in all fifty states.⁵⁰ The framework proposed by Privacy for America provides prohibitions on certain kinds of harmful data uses and conduct while enabling uses that can assist policymakers in their response to public health emergencies. The framework would

⁴⁹ *Privacy for America*, located at <https://www.privacyforamerica.com/>.

⁵⁰ *Privacy for America*, located at <https://www.privacyforamerica.com/>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

clearly define and prohibit practices that make personal data vulnerable to misuse, rather than allow individuals to consent to harmful uses. In turn, individuals and our economy can continue to benefit from the responsible use of data.

Sen. Peters

- 36. 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?

RESPONSE: IAB represents media companies engaged in digital advertising in the United States. As a result, evaluating the response to the demand for personal protective equipment is beyond our expertise and we defer to others on this matter. We are supportive of businesses' efforts to help respond to the COVID-19 pandemic. Our members continue to offer connectivity, content, and services to consumers for free or at a reduced cost.⁵¹ In addition, our member companies are also helping individuals access the latest news, place online food deliveries, access digital conference calls, and provide many other essential services.

- 37. 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?

RESPONSE: We believe that data is a valuable asset, particularly in the fight against COVID-19, and it should be leveraged in ways that are mindful of consumer privacy. IAB member companies have used data to develop visualization maps to help monitor the movements of individuals affected with COVID-19, to discover patterns that lead to the spread of the virus, and to identify areas that could be affected.⁵² These reports use

⁵¹ See Dave Grimaldi, *Good Works: IAB & Tech Lab Members vs. Coronavirus*, (Mar. 25, 2020), located at <https://www.iab.com/blog/good-works/>.

⁵² James Glanz, Benedict Carey, Josh Holder, Derek Watkins, Jennifer Valentino-DeVries, Rick Rojas and Lauren Leatherby, *Where America Didn't Stay Home Even as the Virus Spread*, N.Y. TIMES (Apr. 2, 2020), located at <https://www.nytimes.com/interactive/2020/04/02/us/coronavirus-social-distancing.html>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

aggregated data to help public health professionals as they analyze efforts to respond to COVID-19. By using aggregated location data in this manner, our companies are able to provide useful information in response to COVID-19 while meaningfully protecting individual privacy. IAB is supportive of exploring and considering all ideas and reasonable uses of data to address the COVID-19 pandemic. We would welcome efforts facilitating research into ways we can save American lives and stop the spread of the virus while engaging in responsible data practices.

Sen. Baldwin

Data and Minority Communities

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.

38. 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?

RESPONSE: The IAB believes that this is an important and critical question to consider in the response to COVID-19. We would be happy to work with the government to address it going forward. Data can have many applications that can provide societal good. It has the power to help increase access to vital information and services for all communities and to facilitate egalitarian access to advancements in technology and data science.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

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.

39. 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?

RESPONSE: These are important considerations that policymakers must think about when responding to this crisis. Big data has the capacity to enable insights that could increase rural, suburban and urban communities’ access to the Internet. Technology companies, and advertising technology in particular, can be valuable for detecting geographical areas and segments where data coverage is low. These insights can help policymakers identify communities in which coverage must be subsidized or made more widely available to equalize opportunity to access to technology to fight pandemics.

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.

40. 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?

RESPONSE: The advertising industry is already providing value to healthcare professionals through their efforts to combat the virus. Data can help hospitals and other health organizations better manage the dramatic increase in demand that they are currently experiencing. For example, businesses are making available artificial intelligence and natural language processing services to assist workers in fielding the large volume of calls, emails, and inquiries that they are receiving, and efficiently prioritize the most urgent requests and information.

Question on Data Sharing

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

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

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.

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

RESPONSE: Public-private partnerships will be of critical importance in the fight against COVID-19. These relationships can be strengthened by enabling trust between all parties involved and by ensuring that consumer privacy remains a primary consideration as innovative data applications are developed.

Sen. Sinema

42. 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?

RESPONSE: The IAB represents media and technology companies that are engaged in digital advertising in the United States. As a result, this question is beyond our expertise and we defer to others in the scientific community to respond to this question.

43. 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?

RESPONSE: We believe that data is a valuable asset, particularly in the fight against COVID-19, and should be leveraged in ways that are mindful of consumer privacy. IAB member companies have used aggregated data to develop visualization maps to help monitor the spread of COVID-19 while respecting consumer privacy rights.⁵³ To ensure that consumer privacy protections are uniformly applied from state-to-state, we believe that federal regulation is needed. IAB supports the policy framework put forth by Privacy for America, which balances the need to protect consumer privacy while ensuring that data may be used in ways that continue to benefit both the economy and individuals.⁵⁴

⁵³ James Glanz, Benedict Carey, Josh Holder, Derek Watkins, Jennifer Valentino-DeVries, Rick Rojas and Lauren Leatherby, *Where America Didn't Stay Home Even as the Virus Spread*, N.Y. TIMES (Apr. 2, 2020), located at <https://www.nytimes.com/interactive/2020/04/02/us/coronavirus-social-distancing.html>.

⁵⁴ *Privacy for America*, located at <https://www.privacyforamerica.com/>.

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

44. 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?

RESPONSE: Data can provide incredible insights that can inform the public health response to COVID-19, keep individuals abreast of the latest guidance, and provide access to vital services. While we cannot specifically speak to challenges in the manufacturing supply chain, we believe that insights from data may assist in developing solutions to these challenges.

45. 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?

RESPONSE: From an advertising perspective, modeling data provides amazing insights that allow our members to create value while protecting consumer privacy. It is possible that such data sets could be helpful in executing economic assistance programs. Data-driven advertising provides significant benefits to businesses that are seeking to efficiently reach their audiences with information about the latest product offerings and other important information. Digital advertising has also been helpful in sharing important information from health organizations on measures to prevent the spread of COVID-19. The same tools may be helpful in providing important information about economic assistance programs. We would be happy to work with you on exploring opportunities.

Sen. Rosen

Benefits and Privacy Concerns of Donated Data

46. 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?**

Mr. Dave Grimaldi, Executive Vice President for Public Policy, Interactive Advertising Bureau

- **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?**

RESPONSE: Data can be an incredibly valuable asset in the response to COVID-19. Our member companies have used data to both educate the public and provide researchers with better insights about the spread of coronavirus and the effect of social distancing policies. We should continue to explore different ways to use data, including voluntarily donated data, that ensures the data is representative of the population and protective of consumer privacy. We believe that consumers should be provided with transparency and control over data collected online. The safeguards our industry has developed can serve as a useful model for how to respect individual privacy rights and enable beneficial data-driven services. IAB is a founding member of a self-regulatory program known as the Digital Advertising Alliance (“DAA”). DAA offers tools to provide consumers with transparency and control over data collected online. This program and its web and app-based, privacy-focused tools make data privacy and consumer notice and choice fundamental considerations for entities operating in our industry.

NSF Research on Big Data

- 47. 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?**

RESPONSE: We believe that data will play an essential role in the public health response to coronavirus and support the exploration of new ways to use data to address public health crises like COVID-19. We are not directly familiar with the National Science Foundation’s work in data science research and development. However, we believe that public-private partnerships to discover beneficial uses of information that can strengthen the public health response will be of considerable importance during this unprecedented time and can facilitate further important scientific advancements to help the United States better prepare for future pandemics.