April 16, 2020

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

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

RE: Letter for the Record re: Hearing on Enlisting Big Data in the Fight Against Coronavirus

Dear Chairman Wicker and Ranking Member Cantwell:

Data and technology are playing a crucial role in the fight against COVID-19. We commend the Committee for focusing on the important role that data can and should play in the current health crisis, and for convening a paper hearing that addresses the important privacy and security considerations that attend those uses. Our companies have long recognized that data must be used in ways that respect individual privacy and promote security. We appreciate the Committee's leadership on these issues, including through developing comprehensive federal privacy legislation. We believe that a strong, comprehensive federal privacy law can further promote private and secure uses of data, both in connection with the COVID-19 response and more broadly.

BSA | The Software Alliance is the leading advocate for the global software industry before governments and in the international marketplace.[1] Our members are enterprise software companies that create technology used by other businesses – including to facilitate remote workplaces, to securely store data in the cloud, and to manage their human resources functions and their customer relationships. Our companies compete on privacy, and their business models do not depend on monetizing users' data.

I. Data Can Be Effective and Important in Combatting COVID-19

Data is a critical tool in the fight against COVID-19. Public health authorities, academic researchers, and government policymakers all rely on data to make crucial decisions about

[1] BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

how to combat the current health crisis. Those decisions can be based on many different types of data, including data about the molecular makeup of the coronavirus that causes COVID-19, statistics reported by local governments about the number of residents infected in a particular community, aggregated health information collected from individuals concerning their self-reported health symptoms, and sensitive information including precise geolocation information of individuals who have been diagnosed with the disease.

Different types of data may be fit for different purposes by these different actors. Indeed, while data about the molecular makeup of the virus is extremely valuable for discovering a vaccine or treatments, it is unlikely to be the type of data needed by government officials trying to determine how to allocate their finite resources among the healthcare facilities in their community combating COVID-19. Different types of data also raise different privacy and security concerns, which will turn on the sensitivity of that data and the different uses to which that data is put. In combatting COVID-19, then, each use of data must be subject to privacy and security safeguards that reflect the sensitivity of that data and the purpose for which it is used.

A strong, comprehensive federal privacy law can help to establish the right set of safeguards for these different uses. That law should apply well beyond uses of data to combat COVID-19, but would provide a clear set of expectations for individuals whose information may be useful in fighting this virus, as well as a clear set of obligations on the companies and other actors using that information.

II. Data Must Be Used in Ways that Respect Individual Privacy and Promote Security

Companies that use data to address COVID-19 must do so responsibly, in ways that respect individual privacy and ensure robust security.

In some cases, technologies will be useful in combatting COVID-19 only if people trust that their information will be used responsibly. For example, there are many efforts globally to create voluntary programs for individuals to share data related to COVID-19. These include proposals by public health officials in some countries to work with mobile application developers to create contact-tracing applications, so that individuals using those mobile apps can be notified when they have been near an individual diagnosed with the disease.[2] As the witnesses in this hearing have explained, contact tracing efforts can create a range of privacy considerations, based on the type of data used (e.g., cell site location information, Wi-Fi, Bluetooth) and the parties with which it is shared.[3] Still, one uniting feature of these voluntary

---

[2] *See, e.g.*, Government of Singapore, *Help Speed Up Contact Tracing with Trace Together*, March 21, 2020, *available at* https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether (explaining voluntary Bluetooth-based mobile app used for contact tracing); Pan-European Privacy-Preserving Proximity Tracing, *available at* https://www.pepp-pt.org/content (explaining initiative by European scientists and technologists to develop interoperable Bluetooth-based technology that can assist national initiatives in privacy-preserving contact tracing); Apple Newsroom, *Apple and Google Partner on COVID-19 Contact Tracing Technology*, April 10, 2020, *available at* https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology (announcing joint effort by Apple and Google to enable the use of Bluetooth technology for contact tracing, first by releasing APIs for use by mobile apps of public health authorities and then by building that functionality into the iOS and Android operating systems).

[3] *See, e.g.*, Testimony and Statement for the Record, Stacey Gray, Senior Counsel at Future of Privacy Forum, Testimony Before Senate Committee on Commerce, Science, and Transportation, at Paper Hearing on Enlisting Big Data in the Fight Against Coronavirus, April 9, 2020; Statement, Michelle Richardson, Director of Privacy and Data Project at the Center for Democracy and Technology,

mobile applications is that they are effective in combatting COVID-19 only if they are adopted by a significant percentage of the population.[4] Without enough individuals voluntarily providing their data to such a mobile app, the app would only identify a small fraction of the potential instances a user was exposed to the disease.[5] Consumer trust in technologies can therefore be a critical aspect of fighting COVID-19.

More broadly, privacy and security must be maintained as companies, governments, and academic researchers across the world use data to combat COVID-19. This pandemic illustrates both how critical data can be in addressing societal issues and the importance of safeguarding the privacy and security of that data.

III. A Strong, Comprehensive Federal Privacy Law Can Promote Private and Secure Uses of Data

BSA supports enactment of a strong, comprehensive federal privacy law that provides confidence to consumers that their data must be used responsibly – and ensures that companies that violate their obligations are subject to strong enforcement. We believe federal privacy legislation should achieve three goals: (1) give consumers the right to know, the right to control, and the right to choose what happens to their personal information, (2) impose strong obligations on companies to safeguard consumers' data and prevent misuse, and (3) provide strong, consistent enforcement.[6]

BSA appreciates the Committee's leadership in developing comprehensive federal privacy legislation, including the United States Consumer Data Privacy Act of 2019 (Discussion Draft) ("USCDPA") and the Consumer Online Privacy Rights Act ("COPRA"). Below we highlight eight features of a comprehensive federal privacy law that can both increase consumer trust in technology, by ensuring that data is used in line with a consumer's reasonable expectations, and create clear and strong obligations for companies handling consumer data. While these aspects of a comprehensive privacy bill should apply broadly — to a wide range of uses covered by a federal privacy law — they would also provide important protections for consumers and companies in the narrower scenario you are focused on today, when data is used to fight COVID-19.

- ***Consumer Rights***. Consumers should have the right to know what data companies collect about them, and the rights to access, correct, and delete that information. Consumers should also be able to opt out of broad types of processing, not just the sale of their information. These rights can help provide consumers control over their information and increase their ability to both trust and verify how their data is used.

Testimony before Senate Committee on Commerce, Science, and Transportation, at Paper Hearing on Enlisting Big Data in the Fight Against Coronavirus, April 9, 2020.

[4] The success of mobile contact tracing applications will also turn on complementary efforts, including widespread testing and ensuring that any contact tracing apps used by a country's public health authorities are adopted nationwide, rather than adopting different and non-interoperable apps in different areas.

[5] *See, e.g.*, Clara Chong, *About 1 Million People Have Downloaded TraceTogether App, But More Need To Do So For It To Be Effective; Lawrence Wong*, The Straits Times, April 1, 2020, *available at* https://www.straitstimes.com/singapore/about-one-million-people-have-downloaded-the-tracetogether-app-but-more-need-to-do-so-for (quoting Singapore's National Development Minister as saying that in order for that country's voluntary contact tracing mobile app to be effective "we need something like three-quarters – if not everyone – of the population to have it.").

[6] *See* Testimony of Victoria Espinel, President and CEO of BSA | The Software Alliance, before the Senate Committee on Commerce, Science and Transportation, at Hearing on Policy Principles for a Federal Data Privacy Framework in the United States, February 27, 2019, *available at* https://www.commerce.senate.gov/services/files/1DECD81B-5947-4FEB-B3E1-E9DF65866321.

For example, consumers should have the ability to know whether companies collect their precise geolocation information — and the ability to opt out of that collection.

- ***Heightened Protections for Sensitive Personal Information***. Certain types of personal information, like medical information, precise geolocation information, and financial account information may be particularly sensitive and therefore should be subject to heightened safeguards, including requiring consent before processing. In the context of COVID-19, these protections would help ensure that companies using sensitive types of personal information take additional measures to protect the privacy and security of that information.

- ***Data Security.*** Data security is integral to protecting personal data and privacy. A federal privacy law should require organizations to employ reasonable data security measures designed to prevent the unauthorized access, destruction, use, modification, and disclosure of personal data. Those measures should be based on the sensitivity of the relevant data, the volume of that data, the size and complexity of the business using the data, the costs of available tools, and the nature of the business that holds the data. For example, companies that collect sensitive information like health information should use strong data security measures.

- ***Purpose Specification***. Companies that collect personal data should tell consumers the purpose for which they are collecting and using that information — and then only use that information consistent with their explanation. Companies that want to use data in other ways should obtain affirmative express consent to do so. For example, if a mobile application collects health information from users in order to give that information to public health officials combatting COVID-19, the mobile application should only use data for that purpose.

- ***Corporate Privacy Programs.*** Companies should adopt policies and practices governing their handling of personal data. These programs should include: (1) designating the person(s) responsible for implementing privacy safeguards, including employee training; (2) regularly monitoring and assessing those safeguards; (3) adjusting those safeguards to address new issues as they arise; and (4) adopting governance systems designed to ensure personal data is used and shared only in ways that are consistent with purposes stated to consumers.[7] These structural protections can help to ensure that companies have established mechanisms for addressing privacy issues — and do not wait until a crisis arises to identify the right decision-makers.

- ***Privacy Impact Assessments***. Companies that collect and use data should also conduct privacy impact assessments for activities that are likely to result in high privacy risks. These assessments require companies to identify privacy risks that may arise from their activities and identify ways to mitigate those risks. For example, under the EU General Data Protection Regulation ("GDPR") companies that determine the purposes and means of processing data must conduct data protection impact assessments for activities "likely to result in a high risk to the rights and freedoms of natural persons." In the context of COVID-19, these assessments can be

[7] Companies may also use voluntary risk management tools to evaluate and mitigate privacy risks. For example, the National Institute of Standards and Technology ("NIST") released a Privacy Framework earlier this year to help companies of all sizes protect consumer privacy. *See* NIST, *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, version 1.0* (Jan. 16, 2020), *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

helpful tools for companies in identifying and mitigating the privacy issues that may be created by their actions.

- ***Privacy-Enhancing Technologies***. A comprehensive federal privacy law can encourage the use and advancement of privacy enhancing technologies like differential privacy, federated learning, and homomorphic encryption. These technologies can help companies analyze data in privacy-protective ways, including by enabling them to use machine learning techniques on data while it remains encrypted, or increasing privacy protection of a dataset by adding "noise" to the data that makes identifying a particular data subject more difficult. For example, a multi-institutional team of researchers developed an app that allows individuals to self-report certain symptoms and leverages differential privacy techniques to make data available to researchers while protecting participants' individual identities.[8]

- ***Clear Obligations for All Companies, Based on Role***. Federal privacy law should ensure that all companies are subject to strong obligations to safeguard the privacy and security of data they handle. Those obligations should also reflect the company's role in handling consumer data, including whether the company determines the purpose and means of collecting data (and therefore acts as a "data controller") or instead process data on behalf of another company and pursuant to that company's instructions (and therefore acts as a "data processor" or "service provider"). This fundamental distinction is critical to a host of privacy laws worldwide, which recognize that both types of businesses have important responsibilities and obligations, and those obligations must reflect how the company interacts with consumer data to avoid creating new privacy and security risks for consumers. For example, a cloud storage service provider should be obligated to adopt reasonable security measures to safeguard data it stores on behalf of medical researchers — but any obligations about the collection and use of that data are appropriately placed on the researchers who collect and use the information.

IV. Open Data Initiatives Can Further Support Data-Based Decision-Making in Combatting COVID-19

More broadly, as this Committee focuses on the role of data in combatting COVID-19, it is also important to recognize the critical role that data sharing initiatives are playing in enabling the unprecedented collaboration we have seen among public health authorities, researchers, and government officials. Many of these initiatives also leverage information that is publicly available, or that may not be considered personal data, including information not associated with a particular individual.

While BSA supports open data initiatives broadly, in the specific context of COVID-19, collaboration between public and private entities has been instrumental. For instance, to help track the domestic spread of COVID-19, IBM and The Weather Channel have developed a mapping visualization that depicts state- and county-level data about confirmed cases and related deaths.[9] This new coronavirus tool launched on The Weather Channel mobile app and weather.com uses AI technology from IBM Watson to help users, families, and communities track COVID-19 at the county level, which is more localized than many resources currently available. In addition, Microsoft has partnered with the White House

[8] *See* Harvard T. H. Chan School of Public Health, *New 'How We Feel' App Aims to Improve COVID-19 Response*, April 3, 2020, *available at* https://www.hsph.harvard.edu/news/features/new-how-we-feel-app-aims-to-improve-covid-19-response.
[9] *See* Jonathan Vanian, *IBM and The Weather Channel Debut Coronavirus Map*, Fortune, March 25, 2020, *available at* https://fortune.com/2020/03/25/ibm-weather-channel-coronavirus-covid.

Office of Science and Technology Policy, the Allen Institute for AI, the Chan Zuckerberg Initiative, Georgetown University's Center for Security and Emerging Technology, Kaggle, and the National Library of Medicine to create a first-of-its-kind "open research dataset" of scientific literature related to COVID-19.[10] Intel has also pledged $50 million in funding for the COVID-19 related initiatives, including $40 million for "Response and Readiness" and "Online Learning" initiatives that will promote data collaboration by accelerating access to technology at the point of patient care, supporting scientific research, and ensuring access to online learning for students.[11]

As these examples demonstrate, the collective value of data is enhanced through responsible efforts to promote sharing. In 2018, Congress took an important step toward promoting data collaboration when it passed the OPEN Government Data Act, creating an expectation that federal agencies should make non-sensitive government data freely available to the public in machine readable formats. As this Committee examines how data can be brought to bear in the public response to COVID-19, we encourage it to pay particularly close attention to the continued implementation of the OPEN Government Data Act and to ensure that agencies have the funding they need to fully execute upon its vision. For instance, this Committee should explore potential opportunities for agencies to leverage privacy-enhancing technologies and governance frameworks — such as differential privacy, homomorphic encryption, and federated learning — to enable greater collaboration on data resources in ways that are consistent with the public's rightful expectations of privacy.

* * *

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these comments. We welcome an opportunity to further engage with the Committee on these important issues.

Sincerely,

Kate Goodloe
Director, Policy
BSA | The Software Alliance

[10] *See* Eric Horvitz, Open For Research: COVID-19 Literature Dataset, March 17, 2020, *available at* https://www.linkedin.com/pulse/open-research-covid-19-literature-dataset-eric-horvitz.
[11] *See Intel Commits $50 Million With Pandemic Response Technology Initiative to Combat Coronavirus, available at* https://newsroom.intel.com/news/intel-commits-technology-response-combat-coronavirus/#gs.3dwvl2.

Appendix

BSA Members Are Leading by Example in Using Data Responsibly to Fight COVID-19

BSA member companies are addressing COVID-19 in a number of ways, including providing free access to their services; helping to disseminate information about the spread of the virus; supporting medical research efforts; preventing the spread of malicious campaigns including email spam, malware, and ransomware; donating to emergency funds; and providing advice and help to companies transitioning to remote work. Many of those efforts are described on BSA's website,[12] which is continuously updated. They include:

- ***Lending Compute Power to Researchers.*** IBM, the White House Office of Science and Technology Policy, and the U.S. Department of Energy are spearheading the COVID-19 High Performance Computing Consortium, to bring more than 30 supercomputers into the fight against COVID-19. The public-private consortium also includes Microsoft and other government, industry, and academic leaders; the consortium offers free computing time and technical resources on world-class machines. To fight the virus, extensive research is needed in areas like bioinformatics, epidemiology, and molecular modeling — and that research demands a massive amount of computational capacity. The consortium aggregates computing capabilities of the world's most advanced and powerful computers to help researchers fight COVID-19.[13] Last week, consortium co-chairs Dario Gil, Director of IBM Research, and The Honorable Paul Dabbar, Undersecretary for Science at the U.S. Department of Energy, reported that the consortium received 35 proposals, matched 19 with a supercomputing partner, and that 11 proposals are "already up and running, just two weeks after we first had the idea for such a partnership." The consortium offers more than 400 petaflops of computing power.[14]

- ***Building Tools for Emergency Responders and Affected Businesses.*** On March 16, ServiceNow released four emergency response apps to both customers and non-customers. The apps help organizations manage emergency response workflows, including by helping government agencies in resourcing their crisis management teams to optimize staff and resources. The apps also help companies communicating with employees about safety updates relating to COVID-19. Despite the short development timeframe, the apps were built with privacy considerations from the outset and designed by default to not be intrusive and to not collect excessive amounts of data. Additionally, privacy flexibility is built into the apps, which enable companies or government entities using them to customize the questions they ask employees, depending on requirements of local privacy laws and the company personnel that receive the information collected. Ultimately, the apps give control to an organization to meet its legal obligations, including not only differing state and international privacy laws and regulations, but also the organization's internal privacy requirements. In just the first 10 days after the apps were released, they were leveraged by more than 1,000 different organizations,

[12] *See* BSA | The Software Alliance, BSA Member COVID-19 Resources, *available at* https://www.bsa.org/news-events/news/bsa-member-covid-19-resources.
[13] *See* The COVID-19 High Performance Computing Consortium, *available at* https://covid19-hpc-consortium.org/.
[14] *See* Dario Gil and Paul Dabbar, COVID-19 HPC Consortium, *The Science Behind the First Proposals to Fight COVID-19 With Supercomputers* (April 7, 2020), *available at* https://covid19-hpc-consortium.org/blog.

including hospitals and healthcare organizations, financial institutions, and local, state, and federal agencies.[15]

- ***Creating Data Dashboards to Improve Crisis Response*.** Splunk created a set of no-cost, interactive dashboards to help customers take a data-driven approach to tracking and responding to coronavirus. An individual or organization can download the Splunk COVID-19 Dashboard or Splunk Remote Work Insights solution, populate it with their own data, and use it to help get a better understanding of the data behind the pandemic. The dashboards will help leaders bring data to the crisis, provide context into how to keep business and mission success moving, and evaluate potential responses to best ensure public safety.[16]

- ***Helping Individuals Self-Assess Their Symptoms From Home, Based on CDC Protocols***. Microsoft partnered with the U.S. Centers for Disease Control and Prevention ("CDC") to develop a Coronavirus Self-Checker bot that can help individuals self-assess their symptoms using CDC's protocols. The bot was built on Microsoft's Healthcare Bot and is designed to assess symptoms and risk factors and suggest a next course of action, such as contacting a provider or managing the illness safely at home. The bot includes tools and controls that enable public health organizations to handle patient data appropriately and in compliance with applicable law. For example, the bot leverages a secure and compliant platform that is compliant with the Health Insurance Portability and Accountability Act ("HIPPA"), GDPR compliant, and ISO 27001, 27018, and CSA Gold certified; all data are also encrypted in transit and at rest; and the bot includes built-in compliance constructs.[17]

- ***AI- and Cloud-Based Tools for Doctors and Researchers Treating COVID-19*.** On April 3, IBM released a set of cloud- and AI-based tools and resources aimed at giving researchers, doctors, and scientists resources to accelerate COVID-19 drug discovery. These include an AI deep search tool that ingested the White House COVID-19 Open Research Dataset and several other licensed databases, an AI tool with 3,000 new, unique molecules containing COVID-related qualities, and a cloud-based, interactive data repository that allows microbiologists and bioinformaticians to study more than 300 million genomic sequences, including more than 500 public genome sequences for COVID-19, presented at the recent Stanford HAI conference.[18] These novel resources, made available for free to researchers, will help researchers gather insights, apply the latest virus genomic information to their findings, identify potential targets for treatments, and create new drug molecule candidates — all of which will help expedite research on finding a treatment for COVID-19.

---

[15] *See* ServiceNow Blog, Nearly 1,000 Organizations Worldwide Implement ServiceNow's Free Emergency Response Apps (March 25, 2020), available at https://blogs.servicenow.com/2020/update-on-emergency-response-program.html.

[16] *See* Splunk, COVID-19 Dashboards, *available at* https://covid-19.splunkforgood.com/dashboard_hub.

[17] *See* Microsoft Official Blog, Delivering Information and Eliminating Bottlenecks with CDC's COVID-19 Assessment Bot (March 20, 2020), available at https://blogs.microsoft.com/blog/2020/03/20/delivering-information-and-eliminating-bottlenecks-with-cdcs-covid-19-assessment-bot.

[18] *See* IBM Research Blog, *IBM Releases Novel AI-Powered Technologies to Help Health and Research Community Accelerate the Discovery of Medical Insights and Treatments for COVID-19* (April 3, 2020), *available at* https://www.ibm.com/blogs/research/2020/04/ai-powered-technologies-accelerate-discovery-covid-19.

- ***Supporting Emergency Responders and Care Providers***. Salesforce is among the companies providing no-cost technology solutions to emergency response teams, care management teams, health systems, and other healthcare and life sciences organizations affected by the COVID-19 pandemic. The company's technology solution lets organizations worldwide stay engaged with patients, employees, and partners, including use of its pre-configured health cloud that helps entities manage health-related requests via phone and chat, and a learning program that quickly distributes the latest safety and testing protocols. The solution uses encryption, audit trails, and monitoring to help ensure the privacy and security of data, and to meet internal and external compliance requirements including HIPAA.[19]

Several initiatives by BSA members highlight the impact of open data efforts, including:

- ***Leveraging Open Government Data to Track the Spread of COVID-19.*** To help track the domestic spread of COVID-19, IBM and The Weather Channel have developed a mapping visualization that depicts state- and county-level data about confirmed cases and related deaths. To develop the platform, IBM relied on data from the World Health Organization, the CDC, and reporting from states and counties across the country. Because the project incorporates data from so many sources, IBM utilized AI-enabled tools to transform the data and make it interoperable. In some instances, the state- and county-level data was made available in non-machine-readable formats, and thus required the use of "computer-vision technology to analyze the documents and obtain the relevant information."[20]

- ***Enhancing Industry Sharing to Enable Research Collaboration.*** Microsoft has partnered with the White House Office of Science and Technology Policy, the Allen Institute for AI, the Chan Zuckerberg Initiative, Georgetown University's Center for Security and Emerging Technology, Kaggle, and the National Library of Medicine to create a first-of-its-kind "open research dataset" of scientific literature related to COVID-19.[21] The "CORD-19" dataset includes over 29,000 machine-readable scholarly articles on the coronavirus family and will enable researchers around the globe to leverage AI in the quest to identify a potential vaccine.

- ***Accelerating Access to Technology at the Point of Care and Speeding Scientific Research Through Data Sharing.*** Intel's $50 million pledge to support COVID-19 relief work includes funding for a variety of projects that will accelerate scientific research and enhance access to technology and data at the point of care. For instance, Intel is working with India's Council of Scientific and Industrial Research and International Institute of Information Technology, Hyderabad, to use Intel technologies to improve the effectiveness of COVID-19 testing and to help develop genome sequencing to understand epidemiology and AI-based risk stratification for patients with comorbidities. The success of these initiatives will depend on the ability of stakeholders to share data.

---

[19] *See* Salesforce Care for Health: No Cost COVID-19 Care Response Solution, March 16, 2020, available at https://www.salesforce.com/blog/2020/03/covid-19-care-response-solution-healthcare.html.
[20] *See* Jonathan Vanian, *IBM and The Weather Channel Debut Coronavirus Map*, Fortune, March 25, 2020, *available at* https://fortune.com/2020/03/25/ibm-weather-channel-coronavirus-covid.
[21] *See* Eric Horvitz, Open For Research: COVID-19 Literature Dataset, March 17, 2020, *available at* https://www.linkedin.com/pulse/open-research-covid-19-literature-dataset-eric-horvitz.