



Tim Day
Senior Vice President
20062
U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC

January 15, 2019

VIA ELECTRONIC FILING

Katie McFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: Developing a Privacy Framework

Ms. McFarland:

The U.S. Chamber of Commerce (“Chamber”) respectfully submits these comments to the National Institute of Standards and Technology (“NIST”) in response to its request for comment about its development of a privacy framework.

The Chamber commends NIST for taking the lead in bringing together stakeholders to address this critically important issue and supports your efforts to develop a privacy framework. The Chamber encourages NIST to build upon its experience with developing its cybersecurity framework but also to consider the distinctions between privacy and security. NIST should continue to allow for public feedback and comment.

The Chamber recognizes the importance of consumer privacy and for this reason it recently adopted and released ten privacy principles for policymakers.¹ These principles address the need for a nationwide privacy framework that protects privacy based upon risk to consumers, encourages transparency, and promotes innovation through a collaborative relationship between government and private stakeholders. The Chamber encourages the policymakers to adopt an approach that draws upon these principles.

¹ See U.S. Chamber of Commerce Privacy Principles (September 6, 2018) *available at* https://www.uschamber.com/sites/default/files/9.6.18_us_chamber_-_ctec_privacy_principles.pdf.

I. A National Privacy Framework is Necessary

Although the Chamber previously advocated that self-regulation was the preferred mechanism to address consumer privacy,² the Chamber now believes a new approach is necessary. In light of high-profile incidents surrounding data, the implementation of the General Data Protection Regulation (“GDPR”) in Europe and passage of the California Consumer Privacy Act (“CCPA”), the Chamber recognizes the need for Congress and the Administration to pursue federal privacy legislation that offers consistent protections to Americans to promote “harmonization and interoperability nationally and globally.”³

Given the effect of data on interstate commerce and US economic prosperity, today’s current technological and state regulatory environment necessitates a federal privacy law that preempts state and local privacy laws. A national privacy framework will bolster continued U.S. leadership in trade internationally and facilitate interoperable cross-border data transfer frameworks.

Policies that promote the free flow of data across state and national borders will facilitate economic growth, trade, and numerous consumer benefits. NIST should keep in the mind the differences between the U.S. privacy regulatory regime and the regimes in other jurisdictions like the E.U. However, NIST’s framework should recognize that many companies who it may want to adopt the framework operate in multiple jurisdictions, so the privacy framework should be harmonious with internationally accepted standards where possible.

The value of the digital economy has a significant effect on the national economy and the welfare of individual Americans. For example, according to one study, digital advertising will overtake other forms of ads this year, topping over \$100 billion in value.⁴

Data-driven services are beneficial to consumers. For example, the vast majority of Americans prefer targeted advertising.⁵ Revenues obtained by providers from advertisers help reduce prices consumers must pay for products and services.⁶ And financial services companies are now using data to widen the pool of applicants that have access to credit.⁷

² Letter from Trade Associations to the Honorable John D. Rockefeller and the Honorable Kay Bailey Hutchison (June 29, 2011) *available at* https://www.uschamber.com/sites/default/files/documents/files/110629_MultiIndustry_PrivacyAndDataSecurity_Rockefeller_Hutchison.pdf.

³ 83 Fed. Reg. 48600.

⁴ Sean Fleming, “Digital now accounts for half of all US advertising,” World Economic Forum (Oct. 18, 2018) *available at* <https://www.weforum.org/agenda/2018/10/digital-now-accounts-for-half-of-all-us-advertising/>.

⁵ See IAB, “The Value of Targeted Advertising to Consumers,” (citing 2016 survey stating 71 percent of consumers prefer targeted advertising) *available at* <https://www.iab.com/wp-content/uploads/2016/05/Value-of-Targeted-Ads-to-Consumers2.pdf>.

⁶ Laurence Green, “Does advertising increase consumer prices?” Advertising Association, *available at* <https://www.adassoc.org.uk/advertisings-big-questions/does-advertising-increase-consumer-prices/>.

⁷ Ann Carnns, “New type of credit score aims to widen pool of borrowers,” *The Seattle Times* (Nov. 3, 2018) *available at* <https://www.seattletimes.com/business/new-type-of-credit-score-aims-to-widen-pool-of-borrowers/>.

In the future, autonomous vehicles, which will help reduce the 40,000 road fatalities each year of which 94 percent are caused by human error,⁸ will potentially use and transmit up to 4 terabytes of data per day.⁹

The 5G networks that will transfer the mass amounts of data necessary to power smart cities and the Internet of Things could produce over 3 million new jobs and \$500 billion in increased GDP over the next decade.¹⁰

Given the impact of data on interstate commerce, today's current technological and state regulatory environment necessitates a federal privacy law. Congress should adopt policies that promote the free flow of data across international borders for consumer benefit, economic growth, and trade. A national privacy framework will bolster continued U.S. leadership internationally and facilitate interoperable cross-border data transfer frameworks. When developing its framework, NIST should seek to harmonize its efforts with those of the FTC and the NTIA, in order to produce a consistent approach to privacy across the U.S. government.

II. NIST's Development of a New Federal Privacy Framework

The Chamber supports an approach to privacy that is risk-based, flexible and non-industry specific. Privacy protections should be considered in light of the benefits provided to consumers and the economy and the privacy risks presented by the data being used, and the way a business uses it. These protections should be based on the sensitivity of the data and informed by the purpose of its use and sharing. Likewise, consumer controls should match the risk associated with the data and be appropriate to the nature of the relationship between the consumer and the company.

While NIST develops its own framework for privacy, legislators should enable consumers to have a say as to how personally identifiable information about them is shared. At the same time, companies using and sharing consumer data should be able to continue innovating and not be hindered by consumer consent outcomes and regulations that do not take into consideration the risks and benefits of data.

Consumers upon verified request should be given the qualified ability to request information about them be deleted. Any proposed right of deletion, like the CCPA, must allow for reasonable exceptions to such requests. Data deletion rights though should not impede a company's ability to among other things provide the goods or services for which a consumer and

⁸ See Chamber Technology Engagement Center Comments to Department to Transportation at 1-2, *In the Matter of Automated Vehicle Policy Summit* (Mar. 9, 2018) available at https://www.uschamber.com/sites/default/files/c_tec_av_3.0_comments_1.pdf.

⁹ Kathy Winter, "Meaning Behind One Big Number: 4 Terabytes," Intel Newsroom (Apr. 14, 2017) available at <https://newsroom.intel.com/editorials/self-driving-cars-big-meaning-behind-one-number-4-terabytes/>.

¹⁰ See Accenture Strategies, "Smart Cities: How 5G Can Help Municipalities Become Vibrant Smart Cities," at 1 (2017) available at https://www.accenture.com/t20170222T202102_w_us-en/acnmedia/PDF-43/Accenture-5G-Municipalities-Become-Smart-Cities.pdf.

business contract, maintain good data hygiene, conduct security-protected research, combat fraud and security threats, and comply with legal obligations.

While many companies are already transparent with their consumers, the Chamber supports a framework that would specifically encourage companies to be transparent with consumers about the collection, use, and sharing of information and provide this information to consumers in an easily-accessible format. Consumers should be able to obtain information regarding the ways in which personally identifiable information about them is collected, used, and disclosed. These transparency efforts should provide consumers meaningful information about information practices without hampering legitimate businesses practices and inundating individuals with information overload.

The private sector and federal regulators should also work in a collaborative and not adversarial manner and should develop partnerships to develop methods for achieving consumer privacy outcomes.

III. Encouraging Privacy Innovation

NIST should build on its experience developing the successful Cybersecurity Framework in creating a voluntary Privacy Framework, based on input from industry and other stakeholders. At the same time, a Privacy Framework must reflect a somewhat different approach from the Cybersecurity Framework, which focuses on cybersecurity risks and threats. A Privacy Framework should facilitate beneficial and innovative uses of data that present low risk of harm to individuals. It should recognize companies' flexibility to best determine and mitigate their own risks. The use of safeguards such as encryption and pseudonymization of data should be encouraged.

NIST should recognize the value that technology can play in working to protect the privacy of consumers. Any privacy approach should be neutral and not favor one technological solution over another in achieving desired outcomes. NIST should consider the role that technology plays in assessing risk to consumers regarding privacy and security. For example, several companies are working to use technology to assess security practices in order to protect information about consumers.¹¹ A privacy framework should not endorse any particular technological solution or approach, but it can – and should – facilitate innovative approaches to addressing consumer privacy.

¹¹ See, e.g., Andrew Ross, "Fico release free cyber security ratings service to companies worldwide," Information Age (June 19, 2018) available at <https://www.information-age.com/fico-cyber-security-rating-123473126/>; Brian Nordli, "How engineers at NSS labs put the 'security' in cybersecurity," Built in Austin (May 30, 2018) available at <https://www.builtinaustin.com/2018/05/30/NSS-Labs-Engineering-Spotlight>.

Technologies such as blockchain also hold the promise of securely transmitting information. Blockchain uses cryptographic methods to support secured transactions ranging from applications such as food security in supply chains¹² to real estate title transfer.¹³

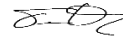
IV. Conclusion

Data is important to every business in the United States whether it be credit reporting companies enabling consumers to be able to access credit in a matter of minutes as opposed to days, marketers presenting tailored products and services to consumers, or automakers and technology firms contributing to the reduction of traffic deaths. Effective, innovative, and responsible use of data is improving the lives of Americans in significant ways. While large amounts of data are being used, analyzed, and shared to bring about these positive societal and economic changes, companies must also respect the privacy of individuals.

In order to achieve the right regulatory balance that strives to protect consumer privacy, foster regulatory certainty, and promote innovation, NIST's efforts should complement those of Congress and the Administration in developing a federal privacy framework that establishes a consistent national standard and avoids a patchwork of federal and state regulations.

The Chamber stands ready to work with the NIST to help develop a privacy framework that benefits all Americans.

Sincerely,



Tim Day
Senior Vice President

¹² Brigid McDermott, "Improving Confidence in Food Safety with IBM Blockchain," (Sept. 5, 2017) *available at* <https://www.ibm.com/blogs/blockchain/2017/09/improving-confidence-in-food-safety-with-ibm-blockchain/>.

¹³ Don Oparah, "3 Ways that Blockchain will Change the Real Estate Market," Tech Crunch (Feb. 6, 2016) *available at* <https://techcrunch.com/2016/02/06/3-ways-that-blockchain-will-change-the-real-estate-market/>.