



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

1615 H Street, NW
Washington, DC 20062

February 25, 2018

The Honorable Janice D. Schakowsky
Chair
Subcommittee on Consumer Protection
and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Cathy McMorris Rodgers
Ranking Member
Subcommittee on Consumer Protection
and Commerce
U.S. House of Representatives
Washington, DC 20515

Re: Hearings on Competition and Consumer Protection in the 21st Century (P181201)

Dear Chair Schakowsky and Ranking Member McMorris Rodgers:

The U.S. Chamber of Commerce respectfully submits this letter for the record for the hearing entitled “Protecting Consumer Privacy in the Era of Big Data,” and commends the Subcommittee for taking the lead in bringing together stakeholders to address this critically important issue.

The Chamber recognizes the importance of consumer privacy and, for this reason, we recently released model data privacy legislation,¹ which includes a nationwide privacy framework to protect privacy based upon risk to consumers, encourages transparency, and promotes innovation through collaboration between government and private stakeholders. We believe you should move forward with legislation that draws upon the principles as incorporated in the model legislation.

I. A National Privacy Framework is Necessary

The Chamber believes a new privacy 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”) as well as pending legislation in other states the Chamber urges Congress and the Administration to enact federal privacy legislation that offers consistent protections to Americans and promotes “harmonization and interoperability nationally and globally.”²

¹ See U.S. Chamber of Commerce Model Privacy Bill (February 13, 2019) available at https://www.uschamber.com/sites/default/files/uscc_dataprivacymodellegislation.pdf.

² 83 Fed. Reg. 48600.

Last year, California enacted the nation's first comprehensive privacy law. Among other things, the law requires companies to honor consumers' requests to stop selling personal information about them (also known as "opt-out" consent) and mandates that companies disclose to consumers the types of data about them that are sold.³ The law will not be enforced until six months after California's Attorney General publishes regulations, or July 1, 2020, whichever comes first.⁴

California is not alone in enacting privacy laws. Other states have enacted laws that affect individual sectors of the economy or practices not currently specifically addressed by a federal privacy law. For example, in May, the state of Vermont enacted a data privacy and security bill that covers data brokers.⁵ The Illinois' Biometric Information Privacy Act ("BIPA") prohibits the disclosure or use of biometric information without written consent.⁶ These often conflicting regimes, and the possibility that other states will also pass privacy laws, creates regulatory uncertainty which is harmful for businesses and confusing for consumers, who would have to understand and interact with many conflicting regimes.

Given the impact 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 also 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 numerous consumer benefits, economic growth, and trade.

In addition to creating regulatory certainty, a national federal privacy law would also be legally appropriate. Congress has long had the power to regulate both the instrumentalities and channels of interstate commerce as well as activities that substantially affect interstate commerce.⁷ In today's e-commerce environment, consumer data acquired during a purchase order may be transmitted from a computer in Virginia over an interstate broadband network to one of nearly 3 million data centers scattered across the country.⁸ This data can then be used to alert product fulfillment and shipping in yet another state like Tennessee.

³ SB 1121, the California Consumer Privacy Act (Signed into law September 23, 2018) available at https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

⁴ *Id.*

⁵ See Act 171 (Enacted into Law May 22, 2018) available at <https://legislature.vermont.gov/assets/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf>.

⁶ See 740 ILL. COMP. STAT. 14/15. Unfortunately, some plaintiffs have attempted to extend the reach of BIPA beyond Illinois itself. See Brief for the Chamber of Commerce of the United States of America as *Amicus Curiae* in Support of the Petitioner, *Patel v. Facebook, Inc.*, No. 3:15-cv-03747 (May 7, 2018) available at <http://www.chamberlitigation.com/sites/default/files/cases/files/18181818/U.S.%20Chamber%20Amicus%20Brief%20--%20Patel%20v.%20Facebook%2C%20Inc.%20%28Ninth%20Circuit%29.pdf> Some companies, as a result of BIPA have decided to stop offering some services in Illinois as well. Amy Korte, "Privacy Law Prevents Illinoisans from Using Google App's Selfie Art Feature," *Illinois Policy* (Jan. 23, 2018) available at <https://www.illinoispolicy.org/privacy-law-prevents-illinoisans-from-using-google-apps-selfie-art-feature/>.

⁷ *United States v. Lopez*, 514 U.S. 549 (1995).

⁸ See Chamber Technology Engagement Center, "Data Centers: Jobs and Opportunities in Communities Nationwide," at 4 (2017) available at https://www.uschamber.com/sites/default/files/ctec_datacenterrpt_lowres.pdf.

Not only does the current e-commerce environment make the handling of consumer data inherently an interstate issue, 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.⁹

Data-driven services are beneficial to consumers. For example, the vast majority of Americans prefer targeted advertising.¹⁰ Revenues obtained by providers from advertisers help reduce prices consumers must pay for products and services.¹¹ Financial services companies are now using data to widen the pool of applicants that have access to credit.¹²

In the future, autonomous vehicles, which have the potential to reduce the 40,000 road fatalities each year (of which 94 percent are caused by human error)¹³ will potentially use and transmit up to 4 terabytes of data per day.¹⁴

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.¹⁵

II. Creating and Enforcing a New Federal Privacy Framework

A. *What Outcomes Should Arise from a New Consumer Privacy Approach*

Policymakers should continue to focus on consumer data. The Chamber believes that a national privacy approach should be risk-focused. 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. Federal enforcement agencies should focus on cases in which consumers suffer actual harm, as opposed to mere speculative injuries or technical violations of the law. The Chamber's privacy legislation discussion draft draws upon these principles.

⁹ 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/>.

¹⁰ 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>.

¹¹ Laurence Green, "Does advertising increase consumer prices?" Advertising Association, available at <https://www.adassoc.org.uk/advertisings-big-questions/does-advertising-increase-consumer-prices/>.

¹² 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/>.

¹³ 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.

¹⁴ 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/>.

¹⁵ 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.

Consumers should have a say as to how personally identifiable information about them is shared. That is why the Chamber’s model legislation offers consumers the ability to opt out of data sharing with third parties. 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 to provide the goods or services for which a consumer and business contract, maintain good data hygiene, conduct security-protected research, combat fraud and security threats, and comply with legal obligations.

B. Accountability

1. Government Enforcement

The Chamber recognizes that robust privacy laws already apply to many sectors of the economy.¹⁶ Policymakers should work to harmonize sectoral privacy approaches unless there is a meaningful reason to keep an existing sectoral law. While the Chamber believes that some sectoral privacy laws dealing with sensitive personal information, such as the Health Insurance Portability and Accountability Act (“HIPAA”), should remain in place, policymakers and stakeholders should continue to engage industry about how legacy privacy laws interact with a new national privacy framework. Any new privacy framework should not impose dual enforcement of multiple federal agencies upon regulated entities.

With a few statutorily-established sectoral exceptions, the U.S. Chamber of Commerce recognizes that the Federal Trade Commission (“FTC” or “Commission”) generally is best positioned to enforce a new federal privacy framework. The FTC, pursuant to its Section 5 Unfair and Deceptive Trade practices authority in the FTC Act, has taken enforcement actions against various entities for privacy related issues. Additionally the FTC has “enforced statutes that protect certain health, credit, financial, and children’s information” and has “brought over 500 cases protecting the privacy and security of consumer information.”¹⁷ It is clear for those sectors within its established jurisdiction that the FTC has the expertise to enforce any new federal privacy framework. For this reason, the Chamber proposes that FTC be given the increased “unfair and deceptive trade practices” authority to enforce new consumer privacy rights such as opt-out, deletion, and transparency.

¹⁶ For example, sectoral federal privacy laws apply to entities in the healthcare, financial, insurance, and communications sectors. Other companies, like transportation companies, while not regulated specifically under a federal privacy law are under the jurisdiction of agencies like the Department of Transportation.

¹⁷ See Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission at 4, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (May 27, 2016) available at https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf.

2. Private-Sector Based Accountability

The private sector must also establish practices to promote accountability for businesses. While many companies are already transparent with their consumers, the Chamber supports requiring companies to be transparent with consumers about the collection, use, and sharing of information and to 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 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 establish partnerships to develop methods for achieving consumer privacy outcomes. For example, federal enforcers should not focus on taking enforcement actions against companies acting in good faith that have made technical violations of privacy statutes.

Any federal privacy law should provide safe harbor provisions that enable companies following agency-approved guidelines to be in compliance with federal law. For example, the Children’s Online Privacy Protection Act provides for such a program in which the FTC approves regulatory guidelines after notice and comment.¹⁸ The Chamber’s bill relies on the statutory language of COPPA’s Safe Harbor Program.

III. Encouraging Privacy Innovation

In addition to the establishment of policy outcomes that will be promoted by the private sector and enforced by appropriate government regulators, policymakers should also recognize the value that technology can play in working to protect the privacy of consumers. Any privacy approach should be technology-neutral and not favor one technological solution over another in achieving desired outcomes.

Congress 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.¹⁹ The Administration should not endorse any particular technological solution or approach, but it can – and should – facilitate innovative approaches to addressing consumer privacy.

Technologies such as blockchain also hold the promise of securely transmitting information. Blockchain uses cryptographic methods to support secured transactions ranging from applications such

¹⁸ See e.g. 15 U.S.C. § 6503.

¹⁹ 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>.

Tim Day, USCC

as food security in supply chains²⁰ to real estate title transfer.²¹ Congress and the Administration should encourage technologies like blockchain by fostering a regulatory environment that enables innovation to thrive.

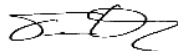
IV. Conclusion

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. Large amounts of data are being used, analyzed, and shared to bring about these positive societal and economic changes, and companies must 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, Congress, and the Administration must work to develop a federal privacy law that establishes a consistent national standard and avoids a patchwork of federal and state regulations.

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

Sincerely,



Tim Day
Senior Vice President

CC: The Honorable Frank Pallone, The Honorable Greg Walden

²⁰ 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/>.

²¹ 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/>.