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

1615 H Street, NW
Washington, DC

May 31, 2019

VIA ELECTRONIC FILING

Ms. April Tabor
Acting Secretary
Federal Trade Commission Office of the Secretary
Constitution Center 400 7th Street, SW
5th Floor, Suite 5610 (Annex A)
Washington, DC 20024

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

Ms. Tabor:

The U.S. Chamber of Commerce ("Chamber") respectfully submits these comments to the Federal Trade Commission ("FTC" or "Commission") in response to its request for comment in connection with its hearings on data privacy.

The Chamber commends the Commission for taking the lead in bringing together stakeholders to address this critically important issue during its hearing entitled, "The FTC's Approach to Consumer Privacy." The Chamber recognizes the importance of consumer privacy and for this reason in September 2018 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, affords consumers control over personal information, encourages transparency, and promotes innovation through a collaborative relationship between government and private stakeholders.

Furthermore, the Chamber released model privacy legislation on February 13, 2019[2] which would give consumers the ability to know how data about them is collected, used and shared, opt out of data sharing, and request data be deleted.

---

[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.
[2] *See* U.S. Chamber Model Privacy Legislation (February 13, 2019) *available at* https://www.uschamber.com/sites/default/files/uscc_dataprivacymodellegislation.pdf

I. A National Privacy Framework is Necessary

Although the Chamber previously advocated that self-regulation was the preferred mechanism to address consumer privacy,[3] 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."[4]

Among other things, the CCPA 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.[5] The law will not be enforced by the California Attorney General until the earliest of six months following when either California's Attorney General publishes regulations or July 1, 2020.[6]

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 2018, Vermont enacted a data privacy and security bill that covers data brokers.[7] The Illinois' Biometric Information Privacy Act ("BIPA") prohibits the disclosure or use of biometric information without written consent.[8] Other states during 2019 including Washington, Illinois, New York and Massachusetts have proposed comprehensive privacy legislation that either mirrors CCPA, GDPR, a hybrid of the two, or a fiduciary model for privacy enforcement.[9] These would create conflicting regimes, and the possibility that other

---

[3] 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.

[4] 83 Fed. Reg. 48600.

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

[6] *Id.*

[7] *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.

[8] *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/.

[9] *See e.g.* SB 5376 "Washington Privacy Act (WA 2019); HB 3358 "The Transparency and Privacy Act" (IL 2019); S 654 "New York Privacy Act" (NY 2019); S. 120 "An Act Relative to Consumer Privacy" (MA 2019).

states would 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 an 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 would also 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 would facilitate numerous consumer benefits, economic growth, and trade.

Both California and Europe have recognized the need for uniformity as opposed to fragmentation. The CCPA specifically states that its intent is to prevent a confusing patchwork of local laws. In fact Section 18 of CCPA states "[i]n order to prevent the confusion created by the enactment of *conflicting local laws regarding the collection and sale of personal information, it is necessary that this act take immediate effect."*[10]

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.[11] 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 U.S.[12] This data can then be used to alert product fulfillment and shipping in yet another state like Tennessee.

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.[13]

Recently, the Chamber's Technology Engagement Center released a report entitled *Unlocking the Digital Potential of Rural America* which found that increased access digital tools to rural small businesses such as broadband, cloud services, and digital training could lead to an increase of at least $47 billion annually to national GDP.[14] A conflicting patchwork of overly-

[10] SB 1121 § 18 (emphasis added).
[11] *United States v. Lopez*, 514 U.S. 549 (1995).
[12] *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.
[13] 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/.
[14] C_TEC *Unlocking the Digital Potential of Rural America* (Mar. 2019) *available at* https://americaninnovators.com/wp-content/uploads/2019/03/Unlocking-the-Digital-Potential-of-Rural-America.pdf.

burdensome data privacy regulations has the potential to stunt investment in digital tools which could connect all Americans especially those in those areas where easy access to and availability of products and services is limited.

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 would bolster continued U.S. leadership internationally and facilitate interoperable cross-border data transfer frameworks.

II. Creating and Enforcing a New Federal Privacy Framework

A. Notice and Choice Should Remain Part of a National Privacy Framework

The Chamber asserts that a national privacy approach should be risk-focused but still incorporate the Fair Information Practice Principle of Notice and Consent. The Chamber identified several requirements in its Model Privacy Legislation that companies should be required to fulfill in order to address consumer risks. The Commission should seek clear privacy protections that are flexible yet not overly broad and vague.

The Chamber asserts that clear rules of the road such as, giving consumers the ability to know how data about them is being collected, used, and shared, opting out of data sharing, and having data about them be deleted provide meaningful protections to consumers. At the same time the Commission should avoid promoting and using overly broad and vague standards that create confusion and are not rooted in tangible harm.

Generally, consumers should be able to opt out of having personal information about them shared with unaffiliated third parties. Some sensitive information may need to be subject to opt-in consent depending on its ability to harm consumers. 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 one contained in the CCPA, must allow for reasonable exceptions to such requests. Data deletion rights should not impede a company's ability to, among other things, 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. Rulemaking Authority

Successful commerce requires that both consumers and businesses have certainty. The Chamber concurs with Commission Chairman Joseph Simons when he testified before the House Consumer Protection Subcommittee on May 8, 2019 that the Commission should not be granted broad rulemaking authority.[15]

C. Time to Comply

In order to give stakeholders certainty and to eliminate confusion, any rules, guidance or enforcement of new theories under Section 5 authority should give stakeholders time to understand new rules and institute effective compliance programs. Many companies are scrambling to comply with California's new privacy law which will be enforced only the earlier of *six months* after the California Attorney General promulgates rules or July 1, 2020. As a result, companies may have very little time following issuances of the regulations before enforcement commences. This approach gives companies potentially only weeks to understand new rules. Compare this approach to the GDPR which gave companies at least two years lead time before full implementation. Any major change to the Commission's approach to privacy should give companies at least two years to implement compliance programs.[16]

III. 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, Congress, the Commission 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 privacy outcomes of such a law should be technological neutrality, a risked-based model, and should encourage privacy innovation.

---

[15] John Hendel, "FTC chairman tells congress: don't give me too much power," *Politico* (May 8, 2019) *available at* https://www.politico.com/story/2019/05/08/ftc-chairman-congress-rulemaking-authority-1418237.

[16] Sam Sabin, "Fresh Off GDPR, Companies Puzzle Over Complying With California's Privacy Law," *Morning Consult* (Dec. 18, 2018) *available at* https://morningconsult.com/2018/12/18/fresh-off-gdpr-companies-now-have-to-prepare-for-californias-privacy-law/.

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

Sincerely,

Tim Day
Senior Vice President