



September 23, 2020

The Honorable Roger Wicker
Chairman
Committee on Commerce, Science and
Transportation
United States Senate
Washington DC, 20515

The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, and
Transportation
United States Senate
Washington DC, 20515

RE: Senate Commerce Committee Sept. 23rd hearing on “Revisiting the Need for Federal Data Privacy Legislation”

Dear Chairman Wicker, Ranking Member Cantwell, and Members of the Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write regarding the Committee’s hearing on “Revisiting the Need for Federal Data Privacy Legislation.” CCIA is an international, not-for profit association that represents companies of all sizes in the high technology products and services sectors, including in computer hardware and software, electronic commerce, telecommunications, and Internet products and services.¹

CCIA supports the Committee’s ongoing efforts to address the need for federal consumer privacy legislation. In recent years, increasing public attention to the subject of data protection, heightened risks of the emergence of an unworkable 50-state patchwork of inconsistent privacy regulations, and pressure from international data governance regimes have all underlined the need for strong and consistent rules of the road for the responsible treatment of consumer information throughout the economy. CCIA welcomes the opportunity to work with members of the Senate and offers the following comments for consideration as the Senate moves forward on this important subject.

Characteristics of a Successful Federal Privacy Framework

CCIA supports enacting a federal privacy framework that aligns with individuals’ expectations to protect people and communities and support the consumer trust that enables the digital economy.² Industry supports ongoing efforts to ensure that organizations are transparent about what data they are collecting, how they are using it, and under what conditions data may be transferred to third parties. Consumers should also have the right to object to data processing

¹ CCIA’s members employ more than 1.6 million workers and generate annual revenues in excess of \$870 billion. A full list of CCIA members is available at <https://www.cciagnet.org/members>.

² CCIA’s privacy principles framework for protecting data and promoting innovation is available at http://www.cciagnet.org/wp-content/uploads/2018/11/CCIA_Privacy_Principles.pdf

where feasible, and to reasonably access, correct, and request the deletion of their personal information. Robust enforcement of privacy rules should be carried out by the Federal Trade Commission and supplemented by State Attorneys General. Establishing these rights and obligations in a baseline consumer privacy framework will allow consumers to exercise greater choice and control in the digital economy, support competition on privacy within industry, while promoting American innovation and competitiveness.

CCIA would encourage any federal privacy legislation to retain the necessary flexibility to remain relevant and effective with the development of new technologies and business practices. Therefore, a comprehensive privacy law should be both technology-neutral, meaning it should not provide specific technology mandates, and sector-neutral, meaning it should apply to online and offline organizations. Furthermore, the development of prescriptive transparency and consent requirements could lead to longer and less intelligible notices, interrupt the user experience, fail to account for different experiences across technologies, and contribute to “click fatigue,” reducing the overall effectiveness of privacy efforts.³ In order to meaningfully inform and empower users, regulatory guidance and codes of conduct should support transparency mechanisms and user controls appropriate for differing products and services and tailored to situations where a use of data is unexpected in the context of a service or presents a significant impact to privacy.

Lessons Learned from the GDPR and CCPA

CCIA supports the Committee’s decision to consider the implementation of recently enacted privacy regimes in developing its approach to protecting consumer privacy. In Europe, there is emerging evidence that prescriptive requirements associated with the GDPR have disadvantaged small and medium sized enterprises relative to their larger, more technically savvy peers.⁴ Overly broad or prescriptive regulatory requirements can create significant overhead costs and record-keeping demands on small companies and raise the barriers to entry for new market players. Privacy legislation should, therefore, set baseline requirements, while providing industry with flexibility in meeting those requirements. Appropriate technical and organizational measures for the protection of personal information should be scalable based on context, such as organizations’ size and resources and the sensitivity and uses of the data at issue.

In California, ongoing efforts to comply with the California Consumer Privacy Act have underscored the importance of setting clear definitions, appropriately tailoring any grant of

³ See Centre for Information Policy Leadership, “Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR” (May 19, 2017), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf.

⁴ See e.g., Eline Chivot & Daniel Castro, “What the Evidence Shows About the Impact of the GDPR After One Year,” Center for Data Innovation (June 17, 2019), <https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/>.

rulemaking authority, and providing a sufficient on-ramp to effective dates.⁵ These procedural features are necessary for the overall effectiveness of a privacy law in order to ensure that organizations have predictability in implementing their compliance obligations and consumers can better understand and exercise their privacy rights.

Harmonization and Interoperability of Privacy Rules

CCIA supports harmonization and interoperability of privacy rules to aid the transfer of data across domestic and international borders to connect businesses to the global marketplace while supporting secure and effective data processing.⁶ The emergence of a patchwork of divergent privacy frameworks across the United States would raise compliance burdens for organizations and present challenges for consumers seeking to understand and exercise their privacy rights. Both organizations and individuals benefit from the ability for data controllers to maintain harmonized, interoperable compliance programs based on widely shared privacy values. Any new privacy protection regime should set consistent, baseline rules for the treatment of personal information within the United States and promote harmonization with emerging national and international concepts and practices in data protection. Taking steps to avoid unnecessarily encumbering organizations' ability to engage in international markets and process data within and beyond the United States will support the international flows of data that support trade relationships and the digital economy.

Conclusion

We look forward to working with you and other stakeholders on a strong and flexible modern privacy framework for the digital economy. Should you have additional questions, please feel free to reach out to Arthur Sidney, Vice President of Public Policy (asidney@ccianet.org) and Keir Lamont, Policy Counsel (klamont@ccianet.org). Thank you again for holding today's important hearing.

Sincerely,

Arthur Sidney
Vice President of Public Policy
Computer & Communications Industry Association

⁵ Keir Lamont, "Landmark CCPA Becomes Enforceable: Five Process Lessons for Policymakers," Disruptive Competition Project (June 30, 2020), <https://www.project-disco.org/privacy/063020-landmark-ccpa-becomes-enforceable-five-process-lessons-for-policymakers/>.

⁶ Joshua P. Meltzer, "The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment," Global Economy and Development at Brookings (Oct. 2014), <https://www.brookings.edu/wp-content/uploads/2016/06/internet-transatlantic-data-flows-version-2.pdf>