Before the
National Telecommunications and Information Administration

	)
	)
Developing the Administration's	)
Approach to Consumer Privacy	)
	) Docket No. 180821780-8780-01
Request for Comments from the Public	)
	)
	)
	)

COMMENTS OF THE INTERNET COMMERCE COALITION

Jim Halpert
General Counsel to the Internet Commerce Coalition
DLA Piper US LLP
500 8th Street, NW
Washington, DC 20004

November 9, 2018

Internet Commerce Coalition

Comments of the Internet Commerce Coalition

The Internet Commerce Coalition ("ICC"), a coalition of leading Internet service providers and platforms, appreciates the opportunity to comment on NTIA's proposed framework for federal policy regarding consumer privacy.

The ICC's principal comment is that to achieve the important goals set forth in the RFC of enabling innovation with strong and meaningful privacy protections for consumers, the Administration should support and advocate for comprehensive federal privacy legislation that preempts state laws. We are now convinced that such legislation is essential to achieve legal clarity and to harmonize the regulatory landscape on privacy.

There are already numerous state laws on data privacy and data security and others coming, threatening a confusing and difficult thicket of regulatory requirements that does not serve either consumers or businesses.

States have begun adopting confusing and conflicting regulations and creating barriers to deployment of useful technologies. For example, the California Consumer Privacy Act (CCPA), although very well intended, was hastily drafted and contains confusing and sometimes conflicting text. As drafted, the law would preclude innovation and increase the cost of internal business operations because it contains inadequate exceptions for the use of de-identified data and for the use of data for research and development. Moreover, the law contains anomalies, such as an unprecedented definition of "personal information" that includes any information that could be associated with a household. The law's data access right, in combination with this broad definition, could allow one member of a household to obtain personal data of all other individuals listed as living in the same household – potentially including sensitive information such as social security numbers and financial account numbers. Although the law may be clarified before taking effect on January 1, 2020, these and other uncertainties in the CCPA demonstrate the importance of enacting and implementing preemptive federal legislation that adopts a comprehensive approach to privacy and provides certainty for consumers and industry.

Similarly, Illinois's well-intentioned, but misguided, biometric privacy law requires a "written release" for all biometric data collection and defines biometric data very broadly, with no exception for security purposes.[1] The law is enforceable through class action lawsuits for substantial statutory damages. Its result has been an abundance of litigation and a resulting decrease in the uses of beneficial authentication technologies, such as voiceprint and fingerprint data, that would otherwise be used to verify identities and prevent fraud.

In the wake of passage of the CCPA, we expect many other expansive privacy regulatory proposals that *differ from and conflicts with California's law*. If these proposals were to be enacted, the result will be an unworkable patchwork of requirements that confuses consumers and imposes significant cost and operational friction that falls particularly heavily on small-to-medium-sized enterprises. The only solution that will ensure consumers are both adequately

[1] 740 ILCS § 14/25.

protected *and* able to enjoy the benefits of innovative uses of data and technology is federal legislation that preempts state laws.

We therefore encourage NTIA to urge Congress to act to protect privacy nationwide through a uniform risk-based standard that is flexible enough to accommodate innovation. NTIA's proposal should follow a risk-based framework, as major privacy frameworks (FIPPs, OECD, APEC, FTC, GDPR) do. States could continue to play an important enforcement role with state Attorneys General having authority to enforce the federal framework vindicating the interests of consumers in their states, subject to the FTC's primary enforcement authority. In addition, recommended practices and self-regulatory frameworks should be used to complement the statutory framework.

This nationwide approach makes sense from a consumer perspective because in our mobile society, consumers frequently travel across states and do not expect their privacy rights to differ based upon where they are staying or moving. Providing consumers greater certainty over their privacy protections and rights will enhance consumer trust. A uniform federal framework will also enable companies to implement their practices uniformly nationwide, and simplify and enhance compliance.

Finally, a national privacy law would significantly strengthen the U.S. government's leadership position internationally and help it to advocate against cross-border data flow restrictions.

We thank you for considering our views and look forward to working in support of federal privacy legislation.

Respectfully submitted,

Jim Halpert, General Counsel