September 25, 2018

Re: ACLU Letter on Senate Commerce Committee hearing, "Examining Safeguards for Consumer Data Privacy"

Dear Senator,

On behalf of the American Civil Liberties Union ("ACLU"), we submit this letter for the record in connection with the Senate Commerce Committee hearing, "Examining Safeguards for Consumer Data Privacy," which will examine current data privacy laws and discuss possibly approached to further safeguarding consumers.

ACLU
AMERICAN CIVIL LIBERTIES UNION

Washington Legislative Office
915 15th Street, 6th floor
Washington DC 20005
(202) 544-1681
aclu.org

Susan Herman
President

Anthony Romero
Executive Director

Faiz Shakir
National Political Director

We are disappointed that the committee has chosen to move forward with this hearing without representation from any groups that represent consumer interests. We urge the committee to promptly hold additional hearings including representatives of consumer groups regarding what additional laws and regulations are needed to safeguard the public's privacy.

In the last year, we have seen countless data breaches, sharing of sensitive data without consent, and reports that companies have misled consumers regarding their data practices. These privacy violations have jeopardized the rights of millions of Americans and threatened our national security. It is past time for Congress to right the imbalance in our laws that has failed to protect consumers from industry practices that strip them over control of their data in the interest of profit. The central voice in this debate should be consumers. While it certainly fair to hear from industry regarding how regulations may impact their practices, they should not be the first or only voice to weigh in on how to safeguard consumer privacy. This is particularly important given that many industry proposals have been strongly opposed by consumer groups and would in fact weaken even existing privacy laws.

Many industry groups have pressed for federal legislation that preempts state law.[1] The ACLU strongly opposes such preemption. Preemption would come at an unacceptable cost for consumers. It could nullify existing laws, undermine existing enforcement and redress actions, and prevent states from taking steps to protect consumers from emerging privacy threats. This is particularly alarming because it has often been states – not the federal government – that have acted in a timely and important way to protect consumer interests.

States as diverse as Idaho, West Virginia, Illinois, and California currently have privacy legislation. For example, California was the first state to require

[1] *See* U.S. Chamber of Commerce, *U.S. Chamber Privacy Principles,* (Sept. 6, 2018), available at https://www.uschamber.com/issue-brief/us-chamber-privacy-principles; Internet Association, *Privacy Principles*, available at https://internetassociation.org/positions/privacy/

companies to notify consumers of a data breach.[2] While other states have since followed suit, the federal government has yet to enact a strong data breach law. California has also required that companies disclose through a conspicuous privacy policy the information they collect and share with third parties, benefitting consumers throughout the country.[3] Similarly, Illinois has set important limits on the commercial collection and storage of biometric information, which has impacted many companies' practices nationwide.[4] Idaho, West Virginia, Oklahoma, and many other states have other laws that protect student privacy.[5] Preemption could adversely impact many of these existing laws, and could foreclose future laws that protect consumers.

Rather than preempting state law, the ACLU urges Congress to enact federal legislation that serves as the floor – not the ceiling – for laws that protect consumers. Among other things**,** such legislation should include requirements that companies obtain informed consent to share, use, or retain information; provide data portability; ensure the consumers have clear and conspicuous information about data practices; and adopt appropriate cybersecurity practices. It should also address civil liberties and civil rights concerns associated with automated decision making practices and ad targeting, and limit so-called "pay for privacy schemes" or provisioning use of a service on consent to collect information unnecessary for the provision of such a service. Finally, any federal legislation must be accompanied by strong enforcement mechanisms and a private right of action for consumers who have their privacy violated.

Many of these proposals are not ones that have been put forward by industry, which further underscores the need to ensure that consumer voices are a central part of the debate over federal privacy legislation. If you would like to discuss these issues in more detail, please contact Senior Legislative Counsel, Neema Singh Guliani at nguliani@aclu.org.

Sincerely,

Faiz Shakir
National Political Director

Neema Singh Guliani
Senior Legislative Counsel

[2] *See* California Civil Code s.1798.25-1798.29
[3] *See* California Code, Business and Professions Code - BPC § 22575
[4] *See* Biometric Information Privacy Act, 740 ILCS 14/, http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57
[5] *See* Center for Democracy and Technology, *State Student Privacy Law Compendium* (October 2016), available at https://cdt.org/files/2016/10/CDT-Stu-Priv-Compendium-FNL.pdf