

December 3, 2019

The Honorable Roger Wicker
Chairman
U.S. Senate Committee on Commerce,
Science, & Transportation

The Honorable Maria Cantwell
Ranking Member
U.S. Senate Committee on Commerce,
Science, & Transportation

Dear Senators Wicker and Cantwell:

The undersigned public interest groups have supported strong bipartisan privacy legislation for many years. As many of us stated a year ago, “unregulated data collection and use in the United States has eroded public trust in companies to safeguard and use data responsibly.”¹ That sentiment is just as true today as it was then. We are pleased to see the privacy debate move forward in Congress with the introduction of several new privacy bills, and write to provide reactions to three specific bills: the Consumer Online Privacy Rights Act (COPRA), the United States Consumer Data Privacy Act of 2019 (USCDPA), and the Balancing the Rights of Web Surfers Equally and Responsibly (BROWSER) Act. Of these three, COPRA provides the strongest privacy protections.

In November 2018, many of our groups argued that federal privacy legislation should incorporate and center on four principles: (1) privacy protections must be strong, meaningful, and comprehensive, with a focus on implementing Fair Information Practices (FIPs); (2) data practices must protect civil rights, prevent unlawful discrimination, and advance equal opportunity; (3) governments at all levels should play a role in protecting and enforcing privacy rights; and (4) legislation should provide redress for privacy violations beyond those causing financial harm, and should recognize and include intangible harms.

COPRA incorporates all four of these principles. The bill encompasses a framework similar to FIPs, which provides a good start toward needed protections such as data minimization, purpose specification, and access and correction rights. It would protect civil rights with strong antidiscrimination provisions covering protected classes in key contexts like housing and employment. It would give states and individuals the ability to enforce the law and would preempt state laws only where they directly conflict with federal provisions—allowing states the ability to innovate and provide additional privacy protections as technology evolves. Last, it would broadly define harms and “covered data,” allowing redress for intangible harms. COPRA is one of the strongest privacy bills introduced to date, and we encourage lawmakers from both sides of the aisle to review its benefits carefully.

By contrast, USCPDA fails to meaningfully fulfill the principles articulated above. The bill does not protect civil rights—it merely grants the Federal Trade Commission (FTC) a supporting role

¹ “Principles for Privacy Legislation.” Open Technology Institute, New America Foundation. 13 November 2018. <https://www.newamerica.org/oti/press-releases/principles-privacy-legislation/>.

to work with other agencies, which the FTC can already do, and requires the FTC to publish biennial reports on algorithmic bias. Given the growing mountain of evidence of data being used in a discriminatory fashion, such weak protections are unacceptable.² The enforcement provisions are also insufficient, particularly because individuals cannot vindicate their rights in court.

Additionally, USCPDA allows for so-called “approved certification programs” (also known as “safe harbors”), which may allow the largest companies to write their own compliance regimes, likely amounting to little more than ineffective self-regulation. Indeed, as repeatedly made evident in Senate hearings, such self-regulation has failed.³ The bill also includes an extremely broad preemption provision that would remove state legislatures completely from protecting privacy, including in specialized areas like employee and student privacy where the USCPDA offers no new protections. While the bill is a small improvement, it does not go far enough to adequately protect individual privacy.

The BROWSER Act is similarly insufficient. In that bill, the primary substantive protection provided is a requirement that online companies obtain opt-in approval from users for the use or disclosure of “sensitive” information, which is defined much more narrowly than in COPRA. The substantive protections are far from comprehensive, with no data minimization, data quality, or user rights included. It offers no protections for civil rights violations, nor does it allow states or individuals to enforce the law through a private right of action. Legislative proposals should not place the entire burden of protecting privacy on individuals by (perhaps) giving them more notice yet providing them with no additional protections, including a private right of action, against abuse and misuse of their data once collected.

We encourage the Senate to listen to its constituents when enacting privacy protections. Americans overwhelmingly want more privacy online,⁴ and Congress must provide these protections. We support strong bipartisan legislation that recognizes the privacy needs of Americans and places the onus of protecting privacy primarily on companies, not individuals. Of these three bills, only COPRA accomplishes these goals.

² Coalition letter to U.S. Senate Committee on Commerce, Science, and Transportation and U.S. House Committee on Energy and Commerce. 19 April 2019.
https://newamericadotorg.s3.amazonaws.com/documents/Letter_to_Congress_on_Civil_Rights_and_Privacy_4-19-19.pdf.

³ “Privacy Self-Regulation ‘Is Not Sufficient,’ Thune Says.” Wolters Kluwer TR Daily. 10 October 2018.
<https://rus.wolterskluwer.com/news/tr-daily/privacy-self-regulation-is-not-sufficient-thune-says/62748/>. For more information on problematic behavior from safe harbor programs, see <https://iapp.org/news/a/new-york-ag-settles-with-truste-over-coppa-safe-harbor-program/> and <https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its>.

⁴ “Most Americans want the government to do more to protect our data. Few think it will happen.” Brian Fung, CNN Business. 15 November 2019.
<https://www.cnn.com/2019/11/15/tech/data-privacy-pew-study/index.html>.

Signed,

Access Now

Campaign for Commercial-Free Childhood

Center for Digital Democracy

Center on Privacy and Technology, Georgetown Law

Common Cause

Consumer Action

Consumer Federation of America

Fight for the Future

Free Press Action

Media Alliance

MediaJustice

New America's Open Technology Institute

Oakland Privacy

Privacy Rights Clearinghouse

Public Citizen

Public Knowledge

U.S. Public Interest Research Group