9 November 2018

"Developing the Administration's Approach To Consumer Privacy" (RIN 0660-XC043) (Docket # 180821780-8780-01)

Thank you for the opportunity to comment on "Developing the Administration's Approach To Consumer Privacy." In addition to our U.S. PIRG comments, we attach and associate ourselves with a set of "Public Interest Privacy Legislation Principles" endorsed this month by a wide set of privacy, community and civil rights organizations, including U.S. PIRG.

As you may know the U.S. Public Interest Research Group serves as the federation of state PIRGs. The state PIRGs are non-profit, non-partisan public interest advocacy organizations that take on powerful special interests on behalf of their members. U.S. PIRG and its members have long been active in protecting consumers on the matters discussed in this Request For Comment. For example, our federal and state advocacy efforts on improving Fair Credit Reporting Act (FCRA) compliance, including strengthening the rights of consumers to dispute the accuracy of their consumer credit reports, began in 1989.

Basing Your Proposal on the FIPPS Is Appropriate

We appreciate the NTIA's recognition of and deference to the longstanding Fair Information Practice Principles (FIPPS) first developed by a committee of the old Health, Education and Welfare Department (HEW) in an early-1970s report preceding passage of the 1974 Privacy Act governing the activities of government when it collects information. The FIPPS were subsequently adopted internationally and codified in 1980 by the Organization for Economic and Cooperative Development (OECD). However, we would also point out that only a robust application of the FIPPS protects privacy. FIPPS-lite proposals that talk the talk but don't walk the walk must be avoided. A FIPPS-lite regime would be designed to have the appearance of consumer control over allowable secondary uses of their information, but would not actually grant control.

However, Disparaging the States Is Not Appropriate

However, we believe that the RFC's denigration of the role of the several states in privacy innovation is misguided. Further, the use of the tired, pejorative term "patchwork" to mis-characterize state leadership on privacy suggests either a misunderstanding of the ways that the states have led efforts to protect consumer privacy or, worse, suggests a pre-determined bias toward preemption.

Preemption of Stronger State Laws Serves Only Special Interests

Where is the evidence, other than industry-backed non-scientific surveys, that the minimal cost of compliance with multiple but converging state laws, especially in an electronic age, outweighs the benefit of keeping the states active as first responders if new privacy threats emerge?

Congress Rarely Acts To Fully Protect Consumers So Preserving the Opportunity for State Action Is Appropriate

Congress rarely solves a problem completely, but getting Congress to consider a problem again when it fails is very difficult. Nevertheless, in 2003, when Congress enacted the Fair And Accurate Credit Transactions Act it wisely did not preempt state action on identity theft because it knew that the FACTA did very little to prevent or mitigate ID theft. Over the next several years, when left to flourish as laboratories of democracy, nearly every state enacted data breach notice and credit freeze laws to prevent identity theft.

Another problem occurs when Congress fails to grant consumers adequate protections due to pressure from special interests, as in Title V of the Gramm-Leach-Bliley Financial Modernization Act of 1999.

The House Energy and Commerce Committee, by bi-partisan acclamation, had included the Ed Markey-Joe Barton privacy amendment in its committee mark. That amendment granted a consumer the right to opt-out of information-sharing with both a bank's affiliates and its non-affiliates. Yet House leadership instead accepted the old House Banking Committee's mark as base floor text and then chose to deny Messrs. Markey and Barton a floor vote on their amendment, which, to be clear, had already passed a major committee. The final law included only special interest, industry-approved, weaker language creating an a "no-opt" regime for sharing with either affiliates or non-affiliates selling financial products. A no-opt regime means just that – no opt-in and no-opt-out. The company controls its use of your information regardless of your choice. In GLBA, consumers only gained a limited right to opt-out of information sharing with non-affiliated third parties selling non-financial products.

Even that limited "right" was further weakened by action of bank regulators when the OCC allowed continued sharing of customer account information with tawdry third-party marketing club companies, so banks could continue to earn lucrative commissions for products that couldn't be sold in a store, since no one would buy them.

However, this set of non-rights was accompanied by an extensive annual notice requirement primarily describing only a consumer's non-rights. Notice itself is not a right. That substitution of privacy notices for real privacy rights contributed to a situation, as you point out, where "such mandates result in long, legal, regulator-focused privacy policies and checkboxes." Had Gramm-Leach-Bliley fostered real privacy rights, its use notices would have been more useful.

Nevertheless, consumer groups continued to support the mandated annual notices requiring disclosure of data collector information uses, even when most uses were not accompanied by a choice. Recall that the opt-out right under GLBA included only a limited opt-out right in limited circumstances. Why did we support it? Because, in the absence of privacy protections, the notice requirement at least forced firms to disclose their information collection and use practices to consumers every year; they were forced to explain what they could do with consumer financial DNA and other information in their customer profiles?

The banks then engaged in a relentless, long-term effort to get rid of the notices. They argued consumers were confused. The only reason consumers were confused is because they were smart; they knew Gramm-Leach-Bliley did not provide them any real rights, only notices. Over the last several years, the annual privacy notices have been eliminated by Congressional action, as part of a campaign by special interests to normalize their massive and disparate non-transparent secondary uses of consumer information.

Today, as industry groups seek passage of a GDPR-lite, they seek a law that will further normalize a set of even more unfair secondary uses of information that allow them to continue business as usual.

If The FTC Is To Remain Our Chief Privacy and Information Agency, It Must Gain Greater Authority to Enforce the Law

Other major industrialized countries have true data protection agencies. At the very least, the FTC must be modernized so it can better rein in abuses of privacy in the digital world. Today, under either its core Section 5 Unfair and Deceptive Practices Authority or its data security responsibilities under Gramm Leach Bliley, the FTC cannot impose civil penalties for a first offense. The administration needs to propose and back legislation to give the FTC full civil penalty authority, as unanimous bi-partisan FTC commissions have routinely asked Congress for over the years. The administration also needs to propose and back legislation giving the FTC full Administrative Procedures Act rulemaking authority. Its FTC Magnuson-Moss Act rulemaking procedures have been correctly described by a former chairman as “both draconian and medieval.”

The Administration Should Support Continued State Authority To Pass Stronger State Privacy and Data Security Laws and Continued Enforcement of Federal Privacy and Data Security Laws by State Attorneys General

States have always led on privacy, from do-not-call lists to data breach and credit freeze laws. States are now protecting consumers from much broader, real harms – including physical, emotional and biometric -- than any federal proposals, which tend to only begrudgingly admit that financial identity theft is a harm, but do not provide real monetary remedies. The states, however, are working to protect their citizens.

Now, California has jump-started a national conversation on privacy with passage of the imperfect but pioneering California Consumer Privacy Act. California should be allowed to perfect its law and other states should be allowed to experiment as well. No reason exists for Congress or the Commerce Department to deny the great privacy accomplishments of the states or, worse, to halt them.

Further, any action that the department or Congress takes should continue to allow state Attorneys-General to both enforce their own laws and enforce any federal privacy laws, without interference or unnecessary pre-approvals from Washington, D.C..

Respectfully,

Edmund Mierzwinski
Senior Director for Consumer Programs
U.S. PIRG
edm<AT>pirg.org
202-461-3821.

ATT: Public Interest Privacy Legislation Principles

Public Interest Privacy Legislation Principles

Unregulated data collection and use in the United States has eroded public trust in companies to safeguard and use data responsibly. Surveys show that, while individuals often try to remove or mask their digital footprints,[1] people think they lack control over their data,[2] want government to do more to protect them,[3] and distrust social media platforms.[4]

The current U.S. data privacy regime, premised largely upon voluntary industry self-regulation, is a failure. Irresponsible data practices lead to a broad range of harms, including discrimination in employment, health care, and advertising, data breaches, and loss of individuals' control over personal information. Existing enforcement mechanisms fail to hold data processors accountable and provide little-to-no relief for privacy violations.

The public needs and deserves strong and comprehensive federal legislation to protect their privacy and afford meaningful redress. Privacy legislation is essential to ensure basic fairness, prevent discrimination, advance equal opportunity, protect free expression, and facilitate trust between the public and companies that collect their personal data. Legislation should reflect at least the following ideas and principles:

1. Privacy protections must be strong, meaningful, and comprehensive

Privacy concerns cannot be fully addressed by protecting only certain classes of personal data held by some companies. Legislation should mandate fairness in all personal data processing, respect individuals' expectations for how data should be treated, provide for data portability, and include safeguards against misuse of data, including de-identified and aggregate data. Legislation should advance fundamental privacy rights and require all entities that collect, store, use, generate, share, or sell (collectively, "process") data both online and offline to comply with Fair Information Practices[5] (collection limitation, data

---

[1] *The State of Privacy in Post-Snowden America*, Pew (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america.
[2] Bree Fowler, *Americans Want More Say in the Privacy of Personal Data*, Consumer Reports (May 18, 2017), https://www.consumerreports.org/privacy/americans-want-more-say-in-privacy-of-personal-data.
[3] Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, Pew (Mar. 27, 2018), http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns.
[4] *Id.*
[5] Fair Information Practices are similar to those adopted by the OECD. *See* OECD Privacy Framework, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

quality, purpose specification, use limitation, security safeguards, openness, access and correction rights, and accountability) across the complete life cycle of the data. Legislation should require all data processing to be clearly and accurately explained, justified, and authorized by the individual. People should have the right to know when their data has been compromised or otherwise breached. Additionally, legislation should require entities processing data to adopt technical and organizational measures to meet these obligations, including risk assessments of high-risk data processing.

2. Data practices must protect civil rights, prevent unlawful discrimination, and advance equal opportunity

Legislation should ensure fundamental fairness of and transparency regarding automated decision-making. Automated decision-making, including in areas such as housing, employment, health, education, and lending, must be judged by its possible and actual impact on real people, must operate fairly for all communities, and must protect the interests of the disadvantaged and classes protected under anti-discrimination laws. Legislation must ensure that regulators are empowered to prevent or stop harmful action, require appropriate algorithmic accountability, and create avenues for individuals to access information necessary to prove claims of discrimination. Legislation must further prevent processing of data to discriminate unfairly against marginalized populations (including women, people of color, the formerly incarcerated, immigrants, religious minorities, the LGBTQIA/+ communities, the elderly, people with disabilities, low-income individuals, and young people) or to target marginalized populations for such activities as manipulative or predatory marketing practices. Anti-discrimination provisions, however, must allow actors to further equal opportunity in housing, education, and employment by targeting underrepresented populations where consistent with civil rights laws. Moreover, decades of civil rights law have promoted equal opportunity in brick-and-mortar commerce; legislation must protect equal opportunity in online commerce as well.

3. Governments at all levels should play a role in protecting and enforcing privacy rights

The public consistently call for government to do more, not less, to protect them from misuse of their data. Legislation should reflect that expectation by providing for robust agency oversight, including enhanced rulemaking authority, commensurate staff and resources, and improved enforcement tools. Moreover, no single agency should be expected to police all data processors; therefore, legislation should empower state attorneys general and private citizens to pursue legal remedies, should prohibit forced arbitration, and importantly, should not preempt states or localities from passing laws that establish stronger protections that do not disadvantage marginalized communities.

4. Legislation should provide redress for privacy violations

Individuals are harmed when their private data is used or shared in unknown, unexpected, and impermissible ways. Privacy violations can lead to clear and provable financial injury, but even when they do not, they may, for example, cause emotional or reputational harm; limit awareness of and access to opportunities; increase the risk of suffering future harms; exacerbate informational disparities and lead to unfair price discrimination; or contribute to the erosion of trust and freedom of expression in society. In recognition of the many ways in which privacy violations are and can be harmful, legislation should avoid requiring a showing of a monetary loss or other tangible harm and should make clear that the invasion of privacy itself is a concrete and individualized injury. Further, it should require companies to notify users in a timely fashion of data breaches and should make whole people whose data is compromised or breached.

Signed,

Access Humboldt
Access Now
Berkeley Media Studies Group
Campaign for a Commercial-Free Childhood
Center for Democracy & Technology
Center for Digital Democracy
Center for Media Justice
Center on Privacy & Technology at Georgetown Law
Color of Change
Common Cause
Common Sense Kids Action
Consumer Action
Consumer Federation of America
Consumers Union
Customer Commons
Demand Progress
Free Press Action Fund
Human Rights Watch
Lawyers' Committee for Civil Rights Under Law
Media Alliance
Media Mobilizing Project
National Association of Consumer Advocates
National Consumer Law Center
National Consumers League
National Digital Inclusion Alliance
National Hispanic Media Coalition
New America's Open Technology Institute
Oakland Privacy
Open MIC (Open Media and Information Companies Initiative)
Privacy Rights Clearinghouse
Public Citizen
Public Knowledge
U.S. PIRG
United Church of Christ, OC Inc.