Before the
National Telecommunications and Information Administration
Washington, D.C.

In the Matter of	)	
	)	
Developing the Administration's Approach to Consumer Privacy	)	Docket No. 180821780-8780-01
	)	
	)	

COMMENTS
OF
THE AMERICAN CIVIL LIBERTIES UNION ("ACLU")

Submitted: November 9, 2018

Comments of the ACLU

Introduction

The ACLU supports protecting individual privacy through federal legislation that at a minimum protects consumers by creating clear and strong ground rules for the use of consumers' personal data, setting a floor rather than a ceiling for state-level protections, creating a private right of action against violators, and putting in place other strong enforcement mechanisms.

For nearly 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government and corporate abuse and overreach. With more than 1.5 million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for privacy, fairness, and the principle that every individual's rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

The ACLU broadly agrees with the views of our allied privacy, civil rights, and civil liberties public-interest organizations on the need for strong privacy protections for consumers based on the Fair Information Practice Principles (FIPPs), which are the basis for comprehensive privacy laws in most of the industrialized world as well as sector specific privacy laws in the United

States.[1] In these comments, we would like to emphasize several issues that are of particular interest and concern to our organization and its members.

Protections around the use and retention of information

The current state of privacy is unacceptable. As new technologies make ever-more-intimate levels of tracking feasible, companies are competing to exploit them as quickly as possible, with the only limits being what *can* be done, and inadequate examination of what *should* be done. As a result, American consumers are subject to a historically unprecedented level of monitoring, more extensive than many understand, and more intrusive than most are comfortable with.

This regime has been built around the concept of "notice and consent": As long as a company includes a description of what it is doing somewhere in a lengthy fine-print click-through "agreement," and the consumer "agrees" (which they must do to utilize a service) then the company is broadly regarded as having met its privacy obligations. And legally, a company is most vulnerable if it violates specific promises in those click-through agreements or other advertisements.

Our ecosystem of widespread privacy invasions has been allowed to fester based on the impossible legal fiction that consumers read and understand such agreements.[2] The reality is that many consumers can't possibly understand how their data is being used and abused, and they don't have meaningful control when forced to choose between agreeing to turn over their data or not using a particular service.

Worse, technologists and academics have found that advertising companies "innovate" in online tracking technologies to resist consumers' attempts to defeat that tracking. This is done by, for example, using multiple identifiers that replicate each other, virus-like, when users attempt to delete them. Advertisers, the experts conclude, "use new, relatively unknown technologies to track people, specifically because consumers have not heard of these techniques. Furthermore, these technologies obviate choice mechanisms that consumers exercise."[3]

In short, not only is there no meaningful mechanism in existence that allows consumers to control how and when they are monitored online, those companies are actively working to defeat consumer efforts to resist that monitoring. Currently, individuals who want privacy must attempt to win a technological arms race with the multi-billion dollar Internet-advertising industry.

American consumers are not content with this state of affairs. Numerous polls show that the current online ecosystem makes people profoundly uncomfortable.[4]

---

[1] For a brief history on the principles, see Robert Gellman, Fair Information Practices: A Basic History at http://bobgellman.com/rg-docs/rg-FIPShistory.pdf

[2] *See* Madrigal, Alex, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days,* The Atlantic (Mar 1. 2012) https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/

[3] Hoofnagle, et al, *Behavioral Advertising: The Offer You Cannot Refuse*, 6 Harvard Law & Policy Review (Aug. 2010), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2137601

[4] *See, e.g* Marc Fisher & Craig Timberg, *American Uneasy About Surveillance but Often Use Snooping Tools, Post Poll Finds*, WASH. POST, Dec. 21, 2013, https://www.washingtonpost.com/world/national-security/americans-

Privacy legislation should include a meaningful "opt-in" baseline rule for the collection of any information. By "meaningful," we mean among other things that care be taken not to allow it to degenerate back into the current "notice and consent" regime, where consumers are forced to "agree" to arcane lengthy, agreements that they cannot understand in order to participate fully in society. Crafting an effective rule to accomplish that goal will be a difficult task requiring great thought and study — but the goal should be clear. In working toward that aim, policymakers should learn from the experience of the European Union with its General Data Protection Regulation. They should also give statutory support to technological opt-in mechanisms such as a "do not track" flag in web browsers, by requiring that companies honor those flags. It is also important that protections be crafted in such a way that privacy is not turned into a "luxury good" for those with the disposable income to pay for it.

In response to calls for greater protections, industry has long cautioned that strong limits on how companies can collect and use information could damage the online economy, but there is no reason that needs to be the case. An ad-supported ecosystem of services can flourish without collecting massive quantities of data about individuals in secret and without their consent. Broadcast television stations were an extremely lucrative business throughout the second half of the 20th century, yet their ads were never behaviorally targeted, and broadcasters were never privy to the intimate details of their audience members' individual viewing habits. Insofar as television ads were targetable at all, it was through contextual rather than behavioral targeting, in which ads are matched to the audiences that different shows attract. This is an effective means of targeting ads online, and one that is perfectly consistent with strong privacy protections. An advertiser that wants to reach golfers can place its ads on a site about golf or on pages returning the results for golf-related search terms.

We must place limits — telling companies, in essence, "that is enough, you may no longer compete in who can best intrude on consumers' privacy." Similar limits already exist in wiretapping statutes and telecommunications privacy laws—phone companies, for example, may not listen to the content of callsand target ads based on those calls. The industry does not complain about that limit because all companies are equally constrained. That is the model that should be followed for other privacy intrusions: set industry-wide limits that protect consumers from the competitive pressures faced by advertisers to invade privacy and protect advertisers from having to decide between ethically shady practices and failing to compete. At the outset, any such limits should approach the collection of consumer information that is not necessary for the provision of a service with trepidation. And the law should strictly limit so-called "pay-for-privacy" schemes.

Insofar as ad-based services have been built upon ethically problematic, non-consensual monitoring of individuals' private internet usage, it deserves to be rolled back, just as the

---

uneasy-about-surveillance-but-often-use-snooping-tools-post-poll-finds/2013/12/21/ca15e990-67f9-11e3-ae56-22de072140a2_story.html; Edward Baig, *Internet Users Say, Don't Track Me,* U.S.A. TODAY, Dec. 14, 2010, http://usatoday30.usatoday.com/money/advertising/2010-12-14-donottrackpoll14_ST_N.htm; JOSEPH TUROW ET. AL., CONTRARY TO WHAT MARKETERS SAY, AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT (2009), https://www.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf.

telemarketing industry was rolled back by the "do not call" registry. The rolling back of the telemarketing industry, just like the ban on listening to phone calls, has not stopped progress or innovation in healthier areas that benefit consumers more. If we protect our privacy and constrain behavioral advertising, ad budgets will not dry up, and ad-supported offerings will not wither away any more than television stations have. Nor will innovation in online and offline services cease, simply because the advertising industry has been proscribed from taking behavioral advertising to the next, even more intrusive, level.

Such rules are entirely compatible with a robust and flourishing economy, online and off, and in fact will establish predictability and stability of expectations that will enhance consumer confidence, prosperity, and innovation.

Permitting States to Put in Place More Stringent Standards

The ACLU believes that any federal privacy standards should be a floor — not a ceiling — for consumer protections. We are strongly opposed to legislation that would, as some industry groups have urged, preempt state action.[5] Such an approach would put existing consumer protections, many of which are state-led, on the chopping block and prevent additional consumer privacy protections from ever seeing the light of day. State regulators could lose the authority to sue or fine companies that violate their laws and consumers may be barred from taking companies to court.

Preemption would likely undermine rather than enhance consumer protections. There are countless examples of states leading the charge to pass laws to protect consumer privacy from new and emerging threats. For example, California was the first in the nation to require that companies notify consumers[6] of a data breach (all states have since followed suit[7]), the first to mandate that companies disclose through a conspicuous privacy policy the types of information they collect and share with third parties[8], and among the first to recognize data privacy rights for children[9]. Illinois set important limits on the commercial collection and storage of biometric information, such as fingerprints and face prints.[10] Idaho, West Virginia, Oklahoma and other states have passed laws to protect student privacy.[11] Nevada and Minnesota require internet service providers to keep certain information about their customers private and prevent

---

[5] *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/

[6] *See* California Civil Code s.1798.25-1798.29

[7] *See* National Conference of State Legislatures, *Security Breach Notification Laws,* (September 29, 2018), available at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[8] *See* California Code, Business and Professions Code - BPC § 22575

[9] See California Code, Business and Professions Code - BPC§ 22582

[10] *See* Biometric Information Privacy Act, 740 ILCS 14/, http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

[11] *See* Center for Democracy and Technology, *State Student Privacy Law Compendium* (Oct. 2016), available at https://cdt.org/files/2016/10/CDT-Stu-Priv-Compendium-FNL.pdf

disclosure of personally identifying information.[12] At least 34 states require private or governmental entities to conduct data minimization and/or disposal of personal information[13], and 22 have laws implementing data security measures[14]. Arkansas and Vermont have enacted legislation to prevent employers from requesting passwords to personal Internet accounts to get or keep a job.

Privacy issues are intertwined with countless facets of modern life, and states have been and will continue to be well-positioned to respond to these challenges.

Particularly in the area of consumer privacy, we should be wary of preemption that could lock in place federal standards that may soon be obsolete. New technology will likely require additional protections and experimenting with different solutions, and states have a vital role in fashioning those solutions.

It is also necessary for states to maintain a role in enforcing consumer privacy laws. Even a doubling of federal enforcement resourcing is likely to be inadequate to police the growing number of companies that handle consumer data. The Equifax breach provides a positive example of the roles that states can play. As a result of that breach, the data of over 140 million consumers was exposed due to what some members of Congress referred to as "malfeasance" on the part of the company.[15] One year later, the company is on track to post record profits, and consumers have not been compensated for the cost of credit freezes the breach made necessary. While the FTC has an ongoing investigation, it has yet to take action. In the meantime, the Massachusetts attorney general is currently suing Equifax seeking damages in an attempt to obtain compensation for individuals impacted by the breach. State attorneys general are essential privacy enforcers.

Preemption would not only be bad for consumers, it would represent a shift in the approach taken by many of our existing laws. For example, the Telecommunications Act explicitly allows states to enforce additional oversight and regulatory systems for telephone equipment provded they do not interfere federal law; it also permits states to regulate additional terms and conditions for mobile phone services. Title I of the Affordable Care Act permits states to put in place additional consumer protections related to coverage of health insurance plans, and HIPPA similarly allows states to enact more stringent protections for health information. The Federal Communications provides that it will supplant, rather than replace, existing state remedies.

---

[12] *See* National Conference of State Legislatures, *Privacy Legislation Related to Internet Service Providers-2018* (Oct. 15, 2018), available at http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers-2018.aspx

[13] *See* National Conference of State Legislatures, *Data Disposal Law*s, available at http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx

[14] *See* National Conference of State Legislatures, *Data Security Laws* (Oct. 15, 2018), available at http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx

[15] Liles, Kevin. *Hack Will Lead to Little, if Any, Punishment for Equifax*, New York Times (Sept. 20, 2017), available at https://www.nytimes.com/2017/09/20/business/equifax-hack-penalties.html

Further, all 50 states in some way regulate unfair or deceptive trade practices, an area also governed by section 5 the FTC Act.[16]

While the strength of these state laws varies, they are rarely deemed disharmonious with the FTC's mandate and rather are integral to manageable privacy regulation enforcement. Such coordination has historically allowed state to fill gaps that federal regulators simply do not have the resources or expertise to address.

Ensuring Strong Enforcement

The FTC has a long history of protecting consumer privacy in the United States. But in the electronic age, the agency requires more authority and resources to continue that effort. And state and local law-enforcement, including attorneys general, city attorneys, and district attorneys, can contribute to ensuring that privacy laws are complied with. Any federal privacy framework should both expand federal resources and provide authority for state and local authorities to investigate and enforce privacy laws.

In the last 20 years, the number of employees at the FTC has grown only slightly.[17] And the number of employees in the Division of Privacy and Identity Protection (DPIP), which is responsible for the agency's privacy and data security work, stands at approximately 50 people.[18] Both the agency as a whole and DPIP require additional resources and employees to address the outsize risks to privacy facing consumers. And for the agency's investigations and enforcement actions to have meaningful deterrent effect, the FTC should be given authority to levy civil penalties in consumer protection actions.[19]

Finally, state and local law enforcement should be given the authority to investigate and enforce federal privacy law to supplement federal and private enforcement efforts. The Fair Debt Collection Practices Act is enforceable by state attorneys general, and state enforcement provides another important source of protection for consumers targeted by unscrupulous debt collectors.[20]

Creating a Private Right of Action

Consumers should have the right to take companies who violate privacy standards to court. Such a private right of action is necessary to make consumers whole when their privacy is violated, and it also serves as a vital enforcement mechanism in addition to actions brought by regulators.

---

[16] Carter, Carolyn. *Consumer Protection in the States: A 0-State Report on Unfair and Deceptive Acts and Practices Statutes*, National Consumer Law Center, (Feb. 20019), available at https://www.nclc.org/images/pdf/udap/report_50_states.pdf

[17] FTC Fiscal Year 2019 Budget, p. 4, https://www.ftc.gov/system/files/documents/reports/fy-2019-congressional-budget-justification/ftc_congressional_budget_justification_fy_2019.pdf

[18] *Id.* at 41.

[19] *See* Testimony of FTC Chairman Joseph Simons Before the House Committee on Energy and Commerce, 6 ("Section 5 does not provide for civil penalties, reducing the Commission's deterrent capability"), available at https://www.ftc.gov/system/files/documents/public_statements/1394526/p180101_ftc_testimony_re_oversight_house_07182018.pdf.

[20] Letter from Attorneys General of Twenty-One States to House and Senate Leadership, April 19, 2018, https://ag.ny.gov/sites/default/files/hr_5082_multistate_letter.pdf.

Companies hold a staggering volume of data about consumers and that data frequently puts consumers at risk. Data about consumer behavior—when they read, shop, interact socially, play games, or pay their bills—is collected, stored, and analyzed.[21] And collection of data about consumers is no longer limited to their digital behavior — it is pushing further into the physical world as well, with consumers increasingly being identified and tracked by their license plates[22], their devices,[23] and even their faces.[24] This data collection is taking place at such a scale that consumers cannot practically understand and make informed decisions about their privacy.[25]

With data collection taking place on such a scale, the risks to consumers increase. California's data breach report identified almost 180 data breaches in 2015 that involved the personal information of California residents, including approximately 24 million records breached.[26] The scale and scope of potential harm associated with poor privacy practices is too extensive to be left to regulators.[27] A robust private right of action allows for consumers to enforce their privacy rights in court and aligns the incentives of companies with the consumers whose data they collect and maintain.

In order to be effective, however, a private right of action should have two key additional protections for consumers.

First, it should specify statutory damages for all violations of privacy rights, not just instances where a consumer has offered conclusive proof of actual damages. When conduct is potentially harmful, statutory damages offer a compelling solution. In copyright infringement, for example, statutory damages can range from $750 to $30,000 per work infringed.[28] Similarly, the Fair Debt Collection Practices Act provides for statutory damages of up to $1,000 per violation.[29] These statutory-damage provisions encourage rigorous compliance by establishing that violations carry a significant penalty. Privacy law should do the same.

---

[21] FEDERAL TRADE COMMISSION, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

[22] *See* You Are Being Tracked, How License Plate Readers Are Being Used to Record Americans' Movements, https://www.aclu.org/issues/privacy-technology/location-tracking/you-are-being-tracked.

[23] Cross Device Tracking, An FTC Staff Report, 3–4, https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf

[24] *Face Recognition Technology Set to Transform Retail*, FORBES, November 8, 2017, https://www.forbes.com/sites/sap/2017/11/08/face-recognition-technology-set-to-transform-retail/#5282b9c04877.

[25] Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC, March 1, 2012. https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/; Woodrow Hartzog, Privacy and the Dark Side of Control, IAI NEWS, September 4, 2017, https://iainews.iai.tv/articles/privacy-the-dark-side-of-control-auid-882.

[26] California Data Breach Report, February 2016, https://www.oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

[27] *See* Letter from California Attorney General Xavier Becerra to California Assembymember Ed Chau and Senator Robert Hertzberg, August 22, 2018 ("The lack of a private right of action, which would provide a critical adjunct to governmental enforcement, will substantially increase the [Attorney General's Office's] need for new enforcement resources. I urge you to provide consumers with a private right of action under the [California Consumer Privacy Act]."), available at https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2801&context=historical.

[28] 17 U.S.C. § 504(c)(2).

[29] 15 USC 1692k.

Second, consumers should be protected against mandatory arbitration clauses buried in terms of service that restrict their rights to have a court hear their claims and undermine the ability of class actions to collective redress for privacy violations.[30] One federal judge called these arbitration clauses "a totally coerced waiver of both the right to a jury and the right of access to the courts" that are "based on nothing but factual and legal fictions."[31] Privacy law should neither tolerate such waivers nor indulge the legal and factual fictions that underlie it.

As the agency develops its position on federal consumer privacy standards, we urge them to take these critical issues into account. If you have questions, please contact Senior Policy Analyst Jay Stanley (jstanley@aclu.org) or Senior Legislative Counsel Neema Singh Guliani (nguliani@aclu.org).

[30] Jessica Silver-Greenberg And Robert Gebeloff, *Arbitration Everywhere, Stacking the Deck of Justice*, N.Y.TIMES, October 31, 2015, https://www.nytimes.com/2015/11/01/business/dealbook/arbitration-everywhere-stacking-the-deck-of-justice.html.
[31] *Meyer v. Kalanick*, 291 F. Supp. 3d 526, 529 (S.D.N.Y. 2018).