epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

January 23, 2020

Ms. Lisa Goldman, Mr. Alex Hoehn-Saric, Ms. Anna Yu,
Mr. Tim Kurth, and Mr. Bijan Koohmaraie
U.S. House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Ms. Goldman, Mr. Hoehn-Saric, Ms. Yu, Mr. Kurth, and Mr. Koohmaraie:

We write to you regarding your draft of a "comprehensive consumer privacy bill." While EPIC truly appreciates your attention to this issue and believes fundamentally in the need for comprehensive baseline privacy legislation, this draft unfortunately fails to protect American consumers from the unprecedented privacy and security threats they face today. EPIC recommends a new draft that gives individuals control over their personal information, requires businesses that collect personal information to use and maintain it responsibly, promotes innovation, and establishes robust enforcement provisions.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] EPIC recently released *Grading on a Curve: Privacy Legislation in the 116th Congress*.[2] EPIC's report set out the key elements of a privacy law and scored pending privacy legislation in Congress. As the Committee and Congress also considers comprehensive data privacy legislation, we urge you to review EPIC's report, attached to this statement.

Americans want privacy protection. In a November 2019 poll by Pew Research, three-quarters of Americans said there should be new regulations of what companies may do with personal data.[3] The same study found that "79% of adults assert they are very or somewhat concerned about how companies are using the data they collect about them," and 75% of respondents said they are "not too or not at all confident that companies will be held accountable by government if they misuse data."[4] Congress can and must change this.

We thank you for your bipartisan efforts to strengthen privacy protections in the United States. EPIC welcomes the opportunity to work with you on comprehensive baseline federal privacy legislation. We are attaching some of our concerns with your current draft and our report *Grading on*

[1] *About EPIC*, EPIC (2019), https://www.epic.org/epic/about.html.
[2] *See* https://epic.org/GradingOnACurve/.
[3] Pew Research Center, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information* (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.
[4] *Id.*

a Curve. We would like to discuss them in person and will reach out to schedule a meeting. It is critical to act now.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Mary Stone Ross*
Mary Stone Ross
EPIC Associate Director

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

The Right to Privacy is a fundamental right and Congress has a clear interest in protecting the privacy rights of all Americans. As the Committee considers comprehensive data privacy legislation, EPIC recommends a new draft that addresses the following issues:

Key definitions are either missing or weak

The scope of a privacy bill is largely determined by its definitions and EPIC is happy to provide language. Although all definitions are important, as you work to finalize language we urge you to pay especially careful consideration to the definitions of "covered entity," "covered information," "deidentified information," "personal information," "publicly available information," and "sell."

The definition of personal information is critical. It is important that personal information covers any information that relates to "a specific person." A good definition recognizes that personal data includes both data that is explicitly associated with an individual and also inferences made from that data about an individual.

Exceptions are loopholes; it is important to narrowly tailor them, including the definitions of deidentified and publicly available. For example, by definition, deidentified information is not personal information; it is therefore critical that it is narrowly tailored. Personal information also includes all information about an individual, including information that may be publicly available, such as zip code, age, gender, and race. Many information brokers sell publicly available and use publicly available information to create profiles. All personal data about an individual should be subject to privacy rules.

Enforcement is critical – Congress must establish an Independent Data Protection Agency

The United States urgently needs a Data Protection Agency. Virtually every other democratic government has recognized the need for an independent agency to address the challenges of the digital age. Given the enormity of the challenge, the United States should create a dedicated Data Protection Agency, based on a legal framework that requires compliance with baseline data protection obligations.[5] An independent agency could more effectively police the widespread exploitation of consumers' personal data and would be staffed with personnel who possess the requisite expertise to regulate the field of data security.[6]

Current law and regulatory oversight in the United States is woefully inadequate to meet the challenges and *creating a new Bureau of Privacy at the FTC will not solve this*. Even FTC Commissioner Joe Simons recently conceded in a Congressional hearing that the FTC does not have the authority to safeguard privacy, noting "on the privacy side, we have one hundred year old statute that was not in any way designed or anticipating the privacy issues that we face today."[7]

---

[5] EPIC, *The U.S. Urgently Needs a Data Protection Agency*, https://epic.org/dpa/.
[6] *See* Privacy and Digital Rights for All, *The Time is Now: A Framework for Comprehensive Privacy Protection and Digital Rights in the United States* (2019), https://www.citizen.org/sites/default/files/privacy-and-digital-rights-for-all-framework.pdf.
[7] *Online Platforms and Market Power, Part 4: Perspectives of the Antitrust Agencies*, 116th Cong. (2019), H. Comm. on the Judiciary, Subcomm. on Antitrust, Commercial, and Administrative Law, https://judiciary.house.gov/legislation/hearings/online-platforms-and-market-power-part-4-perspectives-

The FTC is ineffective and fails to use its current resources and authorities to safeguard consumers. Worse its failure to act imperils not only privacy but our very democracy. The agency ignores most complaints it receives, does not impose fines on companies that violate privacy, and is unwilling to impose meaningful penalties on repeat offenders.[8] Last year, our case EPIC v. FTC determined that there were over 26,000 complaints against Facebook pending with the Commission.[9] ***The FTC is simply ignoring thousands of consumer privacy complaints about Facebook's ongoing business practices.*** In documents obtained in September 2019 by EPIC, we uncovered 3,000 complaints new complaints filed with the FTC *since the Commission proposed the $5 billion settlement with Facebook two months prior.*[10] The FTC is not an effective data protection agency. Even when the FTC reaches a consent agreement with a company, the Commission fails to protect the interests of consumers.[11]

The FTC's problems are not lack of budget or staff. The FTC has not even filled the current post for a Chief Technologist. The FTC has simply failed to use its current resources and current authorities to safeguard consumers. ***Creating a new Bureau of Privacy at the FTC will not solve that issue.***

The Online Privacy Act, filed by Representatives Eshoo and Lofgren (H.R. 4978), creates an independent data protection agency with strong enforcement powers. The Online Privacy Act also sets out robust rights for internet users and clear obligations on data controllers, and promotes innovation. The Online Privacy Act is the strongest privacy bill in Congress to date and the Committee should schedule a hearing on this excellent bill and give it a favorable report without delay.

It is important to carefully consider what is "covered information"

Many businesses collect personal information from consumers using hundreds of tracking and collection devices[12] including passively through your Wi-Fi and blue tooth signals.[13] They not only know where you live and how many children you have, but also how fast you drive,[14] your

---

antitrust-agencies (testimony of Joseph Simons, Chairman, Fed. Trade Comm'n at 1:35:45: "on the privacy side, we have one hundred year old statute that was not in any way designed or anticipating the privacy issues that we face today.") (Nov. 13, 2019).

[8] Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.*, FTC File No. 1823109 at 17 (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

[9] EPIC, *EPIC FOIA - FTC Confirms More than 25,000 Facebook Complaints are Pending* (Mar. 27, 2019), https://epic.org/2019/03/epic-foia---ftc-confirms-more-.html.

[10] EPIC, *EPIC Uncovers 3,156 More Facebook Complaints at FTC—Over 29,000 Now Pending* (Sept. 22, 2019), https://epic.org/2019/09/epic-uncovers-3156-more-facebo.html.

[11] *See EPIC v. FTC*, No. 12-206 (D.C. Cir. Feb. 8, 2012).

[12] Oracle, 2019 Data Directory, http://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf

[13] *'Aisles Have Eyes' Warns That Brick-And-Mortar Stores Are Watching You*, NPR's Fresh Air (Feb. 13, 2017), https://www.npr.org/2017/02/13/514322899/aisles-have-eyes-warns-that-brick-and-mortar-stores-are-watching-you.

[14] Andrea Peterson, *Some companies are tracking workers with smartphone apps. What could possibly go wrong?*, Wash. Post (May 14, 2015), https://www.washingtonpost.com/news/the-

personality[15], sleep habits, biometric and health information[16], financial information, and precise geographic location[17]—including if you visited a women's health clinic[18]. Comprehensive privacy legislation must cover the collection of all personal information whether it is collected online or offline.

Individual rights (right to access, control, delete) must be protected

Transparency is key and privacy legislation must give individuals meaningful control over their personal information held by others. This is accomplished by the creation of legal rights that individuals can exercise including the right to access and correct data, to limit its use, to ensure it is securely protected, and also that it is deleted when no longer needed.

Legislation must make clear the responsibility of companies to protect the personal data they choose to collect and the rights of individuals who entrust their personal information to other. The "notice and consent" framework has little to do with privacy protection. Federal privacy law must impose clear obligations on companies and establish meaningful protections for individuals.

Congress must impose strong obligations on data controllers

Organizations that choose to collect and use personal data necessarily take on obligations for the collection and use of the data. These obligations help ensure fairness, accountability, and transparency in decisions about individuals. Together with the rights of individuals describes above, they are often described as "Fair Information Practices." Many of these obligations are found today in U.S. sectoral laws, national laws, and international conventions. These obligations include:

- Transparency about business practices
- Data collection limitations
- Use/Disclosure limitations
- Data minimization and deletion

---

switch/wp/2015/05/14/some-companies-are-tracking-workers-with-smartphone-apps-what-could-possibly-go-wrong/

[15] Youyou, Kosinski, Stillwell, *Computer-based personality judgments are more accurate than those made by humans,* Proceedings of the National Academy of Sciences Jan 2015, 112 (4) 1036-1040; DOI: 10.1073/pnas.1418680112, https://www.pnas.org/content/112/4/1036 (from the abstract: *We show that (i) computer predictions based on a generic digital footprint (Facebook Likes) are more accurate (r = 0.56) than those made by the participants' Facebook friends using a personality questionnaire (r = 0.49); (ii) computer models show higher interjudge agreement; and (iii) computer personality judgments have higher external validity when predicting life outcomes such as substance use, political attitudes, and physical health; for some outcomes, they even outperform the self-rated personality scores.* This is the research that Cambridge Analytica used to manipulate voters during the 2016 election. The researcher subsequently showed (https://osf.io/zn79k/) that five low resolution images could determine sexual orientation to a significantly greater degree of accuracy than humans.)

[16] *Data Brokers — Is Consumers' Information Secure?,* S. Comm. on the Judiciary, Subcomm. on Privacy, Technology, and the Law (Testimony of Pam Dixon, Exec. Dir., World Privacy Forum) (Nov. 3, 2015), https://www.judiciary.senate.gov/imo/media/doc/11-3-15%20Dixon%20Testimony.pdf.

[17] Kaveh Waddell, *Why Bosses Can Track Their Employees* 24/7, The Atlantic (Jan. 6, 2017), https://www.theatlantic.com/technology/archive/2017/01/employer-gps-tracking/512294.

[18] Press Release, Attorney General Maura Healey, *AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities* (Apr. 4, 2017), https://www.mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts.

- Purpose specification
- Accountability
- Data accuracy
- Confidentiality/security

The current draft is lacking these important obligations on companies who collect personal data.

Require Algorithmic Transparency

As automated decision-making has become more widespread, there is growing concern about the fairness, accountability, and transparency of algorithms. All individuals should have the right to know the basis of an automated decision that concerns them. Modern day privacy legislation typically includes provisions for the transparency of algorithms to help promote auditing and accountability.

The Consumer Online Privacy Act, filed by Senators Maria Cantwell, Brian Schatz, Amy Klobuchar, and Edward Markey, has strong provisions requiring algorithmic decision-making impact assessments and prohibiting bias and discrimination in advertising.

Require Data Minimization and Privacy Innovation

Many U.S. privacy laws have provisions intended to minimize or eliminate the collection of personal data. Data minimization requirements reduce the risks to both consumers and businesses that could result from a data breach or cyber-attack.

Good privacy legislation should also promote privacy innovation, encouraging companies to adopt practices that provide useful services and minimize privacy risk. Privacy Enhancing Techniques ("PETs") seek to minimize the collection and use of personal data.

EPIC appreciates the inclusion of data retention limitations in the draft, but this should not be left to rulemaking by the Federal Trade Commission.

Prohibit take-it-or-leave-it or pay-for-privacy terms

Privacy should not be a commodity that only the wealth can afford. Individuals should not be forced to trade basic privacy rights to obtain services. Such provisions undermine the purpose of privacy law: to ensure baseline protections for consumers.

EPIC appreciates the prohibition on pay-for-privacy provisions and take-it-or-leave-it terms of service in the draft bill. Those provisions should be retained.

Private Right of Action

Privacy laws in the U.S. typically make clear the consequences of violating a privacy law. Statutory damages, sometimes called "liquidated" or "stipulated" damages are a key element of US privacy law and should provide a direct benefit to those whose privacy rights are violated.

Without strong enforcement provisions, the law simply will not be complied with. We are already seeing this in the first month since the California Consumer Privacy Act took effect, where the lack of a private right of action coupled with a lack of funding for enforcement by the state

means companies are failing to comply.[19] A strong federal privacy law must include a private right of action.

Limit Government Access to Personal Data

Privacy legislation frequently includes specific provisions that limit government access to personal data held by companies. These provisions help ensure that the government collects only the data that is necessary and appropriate for a particular criminal investigation. Without these provisions, the government would be able to collect personal data in bulk from companies, a form of "mass surveillance" enabled by new technologies. The Supreme Court also recently said in the *Carpenter* case that personal data held by private companies, in some circumstances, is entitled to Constitutional protection.[20]

Congress Should Enact Privacy Law, not Delegate to an Agency Rulemaking Responsibility

Finally, EPIC is concerned that Congress has deferred to a federal agency the responsibility to draft and establish federal privacy law. This is the responsibility of Congress, Congress has done so in the past,[21] and should do so now. Leave it to the courts to determine how best to apply the mandates of Congress to new technologies.[22] Rulemaking is too slow and cumbersome to address the challenges ahead.

[19] Greg Bensigner, *So far, under California's new privacy law, firms are disclosing too little data — or far too much*, The Washington Post (Jan. 21, 2020), https://www.washingtonpost.com/technology/2020/01/21/ccpa-transparency/.

[20] *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

[21] Postal Service Act of 1792; Communications Act of 1934, 47 U.S.C. § 151 et seq; Privacy Act of 1974, 5 U.S.C. § 552; Family Educational Rights and Privacy Act (FERPA), 20 USC S. 1232g; Right to Financial Privacy Act of 1976, 12 U.S.C. §§ 3401-342; Privacy Protection Act of 1980, 42 U.S.C. § 2000aa et seq; Cable Communications Policy Act of 1984, 42 U.S.C. § 551; Electronic Communication Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848–1873 (codified as amended in scattered sections of 18, 28, 47, and 50 U.S.C.); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1988).

[22] *In re Vizio, Inc., Consumer Privacy Litigation*, 238 F. Supp. 3d 1204 (C.D. Cal. 2017) (applying VPPA and Wiretap Act to Smart TV data collection); *Yershov v. Gannet Satellite Info. Network*, 820 F.3d 482 (1st Cir. 2016) (applying VPPA to mobile video app); *Mollett v. Netflix*, 795 F.3d 1062 (9th Cir. 2015) (applying VPPA to streaming video service); *Joffe v. Google, Inc.*, 746 F.3d 920 (9th Cir. 2013) (applying Wiretap Act to Google's collection of private Wi-Fi data); *US v. Szymuszklewicz*, 622 F.3d 701 (7th Cir. 2010) (applying Wiretap Act to e-mail monitoring).