epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

Developing the Administration's Approach to Consumer Privacy

Request for Comments

[Docket No. 180821780-8780-01]

November 9, 2018

---

The Electronic Privacy Information Center ("EPIC") submits these comments in response to the National Telecommunications and Information Administration's ("NTIA") request for comments seeking recommendations on the administration's approach to consumer privacy.[1]

EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues and is a leading advocate for consumer privacy.[2] In a recent commentary, EPIC said that the U.S. Department of Commerce ("Department") had failed to recognize the importance of privacy protection for the digital economy.[3] As EPIC President Marc Rotenberg wrote in the *Financial Times*, "Instead of criticizing the EU effort, the Commerce Department should help develop a comprehensive strategy to update US data protection laws."[4] The public supports regulation for data protection[5] and polls consistently show that Americans value their privacy.[6]

In these comments, EPIC begins by commending the NTIA for proposing a policy framework based on Fair Information Practices and not "notice and choice. The NTIA correctly states that notice and choice policies, "have resulted primarily in long, legal, regulator-focused privacy policies and check boxes, which only help a very small number of users who choose to read

---

[1] Nat'l Telecomms. & Info. Admin., U.S. Dep't. Commerce, *Developing the Administration's Approach to Consumer Privacy*, Request for Comments, Docket No. 180821780-8780-01 (Oct. 11, 2018), https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy [hereinafter RFC].

[2] EPIC is a non-partisan research and advocacy center in Washington, DC. EPIC's members include distinguished experts in law, technology, and public policy. EPIC, *About EPIC*, https://epic.org/epic/about.html.

[3] Marc Rotenberg, *Congress Can Follow the EU's Lead and Update US Privacy Laws*, FIN. TIMES, (May 31, 2018), https://www.ft.com/content/39044ec6-64dc-11e8-a39d-4df188287fff.

[4] *Id.*

[5] Kim Hart, *Exclusive: Public Wants Big Tech Regulated*, AXIOS (Feb. 28, 2018), https://www.axios.com/axios-surveymonkey-public-wants-big-tech-regulated-5f60af4b-4faa-4f45-bc45-018c5d2b360f.html

[6] EPIC, *Public Opinion on Privacy*, https://epic.org/privacy/survey/ (compilation of public opinion polls).

these policies and make binary choices." The NTIA further states that an "outcome-based approach emphasizes flexibility, consumer protection, and legal clarity can be achieved through mechanisms that focus on managing risk and minimizing harm to individuals arising from the collection, storage, use, and sharing of their information." The NTIA has identified seven critical Privacy Outcomes:

> 1. *Transparency.* Users should be able to easily understand how an organization collects, stores, uses, and shares their personal information. Transparency can be enabled through various means. Organizations should take into account how the average user interacts with a product or service, and maximize the intuitiveness of how it conveys information to users. In many cases, lengthy notices describing a company's privacy program at a consumer's initial point of interaction with a product or service does not lead to adequate understanding. Organizations should use approaches that move beyond this paradigm when appropriate.
>
> 2. *Control.* Users should be able to exercise reasonable control over the collection, use, storage, and disclosure of the personal information they provide to organizations. However, which controls to offer, when to offer them, and how they are offered should depend on context, taking into consideration factors such as a user's expectations and the sensitivity of the information. The controls available to users should be developed with intuitiveness of use, affordability, and accessibility in mind, and should be made available in ways that allow users to exercise informed decision-making. In addition, controls used to withdraw the consent of, or to limit activity previously permitted by, a consumer should be as readily accessible and usable as the controls used to permit the activity.
>
> 3. *Reasonable Minimization.* Data collection, storage length, use, and sharing by organizations should be minimized in a manner and to an extent that is reasonable and appropriate to the context and risk of privacy harm. Other means of reducing the risk of privacy harm (*e.g.*, additional security safeguards or privacy enhancing techniques) can help to reduce the need for such minimization.
>
> 4. *Security.* Organizations that collect, store, use, or share personal information should employ security safeguards to secure these data. Users should be able to expect that their data are protected from loss and unauthorized access, destruction, use, modification, and disclosure. Further, organizations should take reasonable security measures appropriate to the level of risk associated with the improper loss of, or improper access to, the collected personal data; they should meet or ideally exceed current consensus best practices, where available. Organizations should secure personal data at all stages, including collection, computation, storage, and transfer of raw and processed data.
>
> 5. *Access and Correction.* Users should have qualified access personal data that they have provided, and to rectify, complete, amend, or delete this data. This access and ability to correct should be reasonable, given the context of the data flow, appropriate to the risk of privacy harm, and should not interfere with an organization's legal obligations, or the ability of consumers and third parties to exercise other rights provided by the Constitution, and U.S. law, and regulation.

6. *Risk Management.* Users should expect organizations to take steps to manage and/or mitigate the risk of harmful uses or exposure of personal data. Risk management is the core of this Administration's approach, as it provides the flexibility to encourage innovation in business models and privacy tools, while focusing on potential consumer harm and maximizing privacy outcomes.

7. *Accountability.* Organizations should be accountable externally and within their own processes for the use of personal information collected, maintained, and used in their systems. As described below in the High-Level Goals for Federal Action section, external accountability should be structured to incentivize risk and outcome-based approaches within organizations that enable flexibility, encourage privacy-by-design, and focus on privacy outcomes. Organizations that control personal data should also take steps to ensure that their third-party vendors and servicers are accountable for their use, storage, processing, and sharing of that data.

1. *Transparency.* Users should be able to easily understand how an organization collects, stores, uses, and shares their personal information. Transparency can be enabled through various means. Organizations should take into account how the average user interacts with a product or service, and maximize the intuitiveness of how it conveys information to users. In many cases, lengthy notices describing a company's privacy program at a consumer's initial point of interaction with a product or service does not lead to adequate understanding. Organizations should use approaches that move beyond this paradigm when appropriate.

2. *Control.* Users should be able to exercise reasonable control over the collection, use, storage, and disclosure of the personal information they provide to organizations. However, which controls to offer, when to offer them, and how they are offered should depend on context, taking into consideration factors such as a user's expectations and the sensitivity of the information. The controls available to users should be developed with intuitiveness of use, affordability, and accessibility in mind, and should be made available in ways that allow users to exercise informed decision-making. In addition, controls used to withdraw the consent of, or to limit activity previously permitted by, a consumer should be as readily accessible and usable as the controls used to permit the activity.

3. *Reasonable Minimization.* Data collection, storage length, use, and sharing by organizations should be minimized in a manner and to an extent that is reasonable and appropriate to the context and risk of privacy harm. Other means of reducing the risk of privacy harm (*e.g.*, additional security safeguards or privacy enhancing techniques) can help to reduce the need for such minimization.

4. *Security.* Organizations that collect, store, use, or share personal information should employ security safeguards to secure these data. Users should be able to expect that their data are protected from loss and unauthorized access, destruction, use, modification, and disclosure. Further, organizations should take reasonable security measures appropriate to the level of risk associated with the improper loss of, or improper access to, the collected personal data; they should meet or ideally exceed current consensus best practices, where available.

Organizations should secure personal data at all stages, including collection, computation, storage, and transfer of raw and processed data.

5. *Access and Correction.* Users should have qualified access personal data that they have provided, and to rectify, complete, amend, or delete this data. This access and ability to correct should be reasonable, given the context of the data flow, appropriate to the risk of privacy harm, and should not interfere with an organization's legal obligations, or the ability of consumers and third parties to exercise other rights provided by the Constitution, and U.S. law, and regulation.

6. *Risk Management.* Users should expect organizations to take steps to manage and/or mitigate the risk of harmful uses or exposure of personal data. Risk management is the core of this Administration's approach, as it provides the flexibility to encourage innovation in business models and privacy tools, while focusing on potential consumer harm and maximizing privacy outcomes.

7. *Accountability.* Organizations should be accountable externally and within their own processes for the use of personal information collected, maintained, and used in their systems. As described below in the High-Level Goals for Federal Action section, external accountability should be structured to incentivize risk and outcome-based approaches within organizations that enable flexibility, encourage privacy-by-design, and focus on privacy outcomes. Organizations that control personal data should also take steps to ensure that their third-party vendors and servicers are accountable for their use, storage, processing, and sharing of that data.

EPIC also favors several of the "High-level Goals" in the RFC. However, it would be contrary to U.S. privacy law and principles of federalism to preempt state law. And the NTIA should support the creation of a federal privacy agency. The U.S. is one of the few developed countries in the world without a data protection agency. The practical consequence is that the U.S consumers experience the highest levels of data breach, financial fraud, and identity theft in the world. And U.S. businesses, with their vast collections of personal data, remain the target of cyber attack by criminals and foreign adversaries. The longer the U.S. continues on this course, the greater will be the threats to consumer privacy, democratic institutions, and national security. The U.S. needs a federal agency focused primarily on ensuring compliance with data protection obligation, and identifying emerging privacy challenges.

### A. High-Level Goals

**2. Are the descriptions clear? Beyond clarity, are there any issues raised by how the issues are described?**

The first high-level goal—"harmonize the regulatory landscape"—is contrary to U.S. privacy law and principles of federalism. Instead, the NTIA should promote federal baseline legislation. Federal baseline legislation ensures minimal protections while still preserving state and local innovation in response to new developments.

For example, Vermont passed a law earlier this year requiring data brokers to disclose publicly whether consumers may opt-out of data collection, retention, or sale, and if so, how

consumers may do so.[7] Vermont law will provide U.S. consumers across the country, not just Vermonters, information on how to protect their information from data brokers that currently operate in the shadows of the economy. Therefore, preempting state laws will harm Americans beyond the residents of that particular state.

EPIC supports "Legal clarity while maintaining the flexibility to innovate" *(#2)* and sees no necessary trade-off between these goals. In fact, an outcomes-based approach to privacy protection should encourage innovation, consistent with the goals of a legal framework.

The NTIA proposes FTC enforcement (#7) because "[g]iven [the FTC's] history of effectiveness, the FTC is the appropriate federal agency to enforce consumer privacy."[8] The NTIA's assessment of the FTC's effectiveness is inaccurate. The Commission has repeatedly failed to enforce its own consent orders, and has allowed companies under consent order to continue privacy-harmful practices. In fact, the Commission only pursued a single enforcement action against either Google or Facebook. The action came more than seven years after the agency obtained consent orders against those companies, and only after the Commission was sued to compel enforcement.[9] The RFC also fails to mention two additional important enforcement mechanisms: state attorneys general and a private right of action.

**B. Next Steps**

**1. Are there any aspects of this approach that could be implemented or enhanced through Executive action, for example, through procurement? Are there any non-regulatory actions that could be undertaken? If so, what actions should the Executive branch take?**

It is important that any non-regulatory actions do not detract from the ultimate goal of enacting comprehensive data-protection legislation.

**3. What aspects of the Department's proposed approach to consumer privacy, if any, are best achieved via other means? Are there any recommended statutory changes?**

EPIC advises the Department to achieve its goals through promoting legislation. Twelve consumer privacy organizations—including EPIC—recently submitted a draft data protection framework to the U.S. Senate Committee on Commerce, Science and Transportation.[10] The framework outlines effective an effective data protection framework: (1) enact baseline federal data protection legislation, (2) limit government access to personal data, (3) establish algorithmic transparency and discriminatory profiling, (4) prohibit "take it or leave it" and other unfair terms, (5)

[7] VT. STAT. ANN. TIT. 9 § 62 (2018), https://legislature.vermont.gov/statutes/chapter/09/062.
[8] RFC, *supra* note 1 at 11.
[9] EPIC, *EPIC v. FTC (Enforcement of Google Consent Order)*, https://epic.org/privacy/ftc/google/consent-order.html.
[10] Letter from Consumer Privacy Organizations to Sen. John Thune, Chairman & Sen. Bill Nelson, Ranking Member, Senate Comm. on Commerce, Sci. & Transp. (Oct. 9, 2018), https://epic.org/testimony/congress/CPOs_to_SCC_US_Data_Protection_Framework_Oct2018.pdf.

ensure robust enforcement, (6) promote privacy innovation, and (7) establish a data protection agency.[11]

**E. One of the high-level end-state goals is for the FTC to continue as the Federal consumer privacy enforcement agency, outside of sectoral exceptions beyond the FTC's jurisdiction. In order to achieve the goals laid out in this RFC, would changes need to be made with regard to the FTC's resources, processes, and/or statutory authority?**

The Federal Trade Commission helps to safeguard consumers and to promote competition, but the FTC is not an effective data protection agency. The agency lacks authority to enforce basic data protection obligations and has failed to enforce the orders it has established. The FTC also lacks the ability, authority and expertise to engage the broad range of challenges we now confront—Internet of Things, Artificial Intelligence, connected vehicles, and more.

In 2011, the FTC entered into a Consent Order with Facebook, following an extensive investigation and complaint pursued by EPIC and several U.S. consumer privacy organizations. The Consent Order prohibited Facebook from transferring personal data to third parties without user consent.[12] As EPIC told Congress in April, the transfer of personal data on 87 million Facebook users to Cambridge Analytica could have been prevented had the FTC enforced its 2011 Consent Order against Facebook.[13] But the FTC failed to act.

Also In 2011, EPIC obtained a significant judgment at the FTC against Google after the disastrous roll-out of Google "Buzz."[14] In that case, the FTC obtained a consent order after Google tried to enroll Gmail users into a social-networking service without receiving meaningful consent from the users.[15] However, a new set of problems became apparent almost immediately after the judgment was entered: the FTC was unwilling to enforce its own consent orders. Almost immediately after the settlements, both Facebook and Google began to test the FTC's willingness to stand behind its judgments. Dramatic changes in the two companies' advertising models led to more invasive tracking of Internet users. Online and offline activities were increasingly becoming merged.

---

[11] *Id.*

[12] Fed. Trade Comm'n., *In re Facebook*, Decision and Order, FTC File No. 092 3184 (Jul. 27, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

[13] *See*, EPIC Statement to S. Comm. on the Judiciary and S. Comm. on Commerce, Sci. & Transp. (Apr. 9, 2018), https://epic.org/testimony/congress/EPIC-SJC-Facebook-Apr2018.pdf.

[14] *In the Matter of Google, Inc.*, EPIC Complaint, Request for Investigation, Injunction, and Other Relief, before the Federal Trade Commission, Washington, D.C. (filed Feb. 16, 2010), https://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf.

[15] Press Release, Fed. Trade Comm'n., FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network: Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data (Mar. 30, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles- rollout-its-buzz.

In March 2018, the FTC finally announced that it would investigate Facebook.[16] It is critical that the FTC conclude the Facebook matter, issue a significant fine, and ensure that the company uphold its privacy commitments to users. In July, the UK Information Commissioner's Office fined Facebook the maximum allowable fine under UK law as the result of the Cambridge Analytica breach, charging the company with "failing to safeguard people's information [and] failing to be transparent about how people's data was harvested by others and why they might be targeted by a political party or campaign. Over seven months have passed since the new Commission announced it was reopening its investigation of Facebook, but still there is no judgment."[17] It is vital that the FTC not lag behind other countries in enforcement.

This problem will not be solved by granting the FTC more authority, because the agency has failed to use the authority it already has. The United States is one of the few advanced economies in the world that does not have a federal data protection agency, even though the original proposal for such an institution emerged from the United States in the 1970s.[18]

As the data breach epidemic reaches unprecedented levels, the need for an effective, independent data protection agency has never been greater. An independent agency can more effectively utilize its resources to police the current widespread exploitation of consumers' personal information and would be staffed with personnel who possess the requisite expertise to regulate the field of data security.

**C. Are there other ways to achieve U.S. leadership that are not included in this RFC, or any outcomes or high-level goals in this document that would be detrimental to achieving the goal of achieving U.S. leadership?**

EPIC urges the NTIA to pursue U.S. ratification of Convention 108 ("Privacy Convention" or "Convention"). The Privacy Convention is the first binding international legal instrument on data protection, and is open to any country, including non-members of the Council of Europe.[19] The Council of Europe established the Convention in 1981 to strengthen the legal protection of individuals with regard to automatic processing of personal information.[20] The Convention was amended in 2018 to reflect changes in new technology.[21] The Convention now requires prompt data breach notification, establishes national supervisory authorities to ensure compliance, permits

---

[16] Fed. Trade Comm'n., Press Release, Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns About Facebook Privacy Practices (Mar. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection.

[17] INFO. COMM'R'S OFFICE, INVESTIGATION INTO THE USE OF DATA ANALYTICS IN POLITICAL CAMPAIGNS, (2018), https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf.

[18] *See* EPIC, *The Privacy Act of 1974*, https://epic.org/privacy/1974act/#history.

[19] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, ETS No. 108. art. 23 https://rm.coe.int/1680078b37 [hereinafter Privacy Convention]

[20] Privacy Convention, *supra* note 32.

[21] Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), May 18, 2018, CM(2018)2, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e.

transfers abroad only when personal data is sufficiently protected, and provides new user rights including algorithmic transparency.[22]

EPIC has long campaigned for the United States to ratify the Privacy Convention.[23] Privacy is a fundamental human right. In the 21st century, it may become one of the most critical human rights of all. Civil society organizations around the world have recently asked that countries which have not yet ratified the Council of European Convention 108 and the Protocol of 2001 do so as expeditiously as possible.[24]

**Conclusion**

EPIC supports the NTIA's proposed Privacy Outcomes and several of the High-Level Goals. But the RFC is lacking key elements for effective data protection in the United States. The NTIA should support federal baseline legislation, the creation of a dedicated privacy agency, and the ratification of the International Privacy Convention.

These are not policy preferences or partisan perspectives. These are the steps that modern societies must take to safeguard the personal data of their citizens.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Christine Bannan*
Christine Bannan
EPIC Consumer Protection Counsel

**Attachment**

*Draft Framework for Data Protection in the United States from Consumer and Privacy Organizations* (Fall 2018)

[22] EPIC, *Council of Europe Modernizes International Privacy Convention* (May 18, 2018), https://epic.org/2018/05/council-of-europe-modernizes-i.html.
[23] EPIC, *Council of Europe Privacy Convention*, https://epic.org/privacy/intl/coeconvention/.
[24] EPIC Statement to Sen. Bob Corker, Chairman & Sen. Bob Menendez, Ranking Member, Senate Comm/ on Foreign Relations (Apr. 13, 2018), https://www.epic.org/EPIC-SFR-Pompeo-April2018.pdf.