June 13, 2022

The Honorable Frank Pallone Jr.
Chair, House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Cathy McMorris Rodgers
Ranking Member, House Committee on Energy & Commerce
2322 Rayburn House Office Building
Washington, DC 20515

The Honorable Janice D. Schakowsky
Chair, Subcommittee on Consumer Protection and Commerce
House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Gus M. Bilirakis
Ranking Member, Subcommittee on Consumer Protection and Commerce
House Committee on Energy & Commerce
2322 Rayburn House Office Building
Washington, DC 20515

Re: Hearing on Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security

Dear Chair Pallone, Ranking Member McMorris-Rogers, Chair Schakowsky, and Ranking Member Bilirakis,

The Electronic Frontier Foundation (EFF) writes to thank the Committee for holding a hearing to examine the important topic of protecting the privacy and civil rights of all American consumers. New technologies are advancing our freedoms, but they are also enabling unparalleled invasions of privacy. National and international laws have yet to catch up with the evolving need for privacy that comes with new digital technologies.

EFF is a member-supported, non-profit civil liberties organization that works to protect freedom, justice, and innovation in the digital world. Founded in 1990, EFF has over 35,000 members. EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law to technology.

American consumers need a strong federal privacy law. EFF appreciates the Committee highlighting the national conversation over how the government should protect us from businesses that harvest and monetize our personal information, and address the racial and other bias that excludes consumers of color from opportunities. To achieve these goals, the discussion draft of the American Data Privacy and Protection Act needs to be strengthened in several areas.

No Preemption

Strong baseline federal privacy legislation would benefit consumers across the country, but any action that supplants stronger state laws would hurt consumers and prevent states from protecting their constituents. California's Consumer Privacy Act, Vermont's Data Broker

Act, and Illinois' Biometric Information Privacy Act are just a few of the state laws that already protect consumers, and other states are looking at similar proposals. These laws are working. Congress should not heed calls to strip Americans across the country of these state protections in the name of creating a single federal standard. While EFF supports federal legislation that actually protects consumer data privacy, we have long opposed doing so if the price is preemption of stronger state laws.[1]

Unfortunately, the American Data Privacy and Protection Act would preempt many state privacy laws. Specifically, section 404(b)(1) of the bill would create a general rule of preemption, and section 404(b)(2) would exempt from this general rule some but not all kinds of state privacy laws. This bill would preempt many existing kinds of state data privacy laws, apparently including:

- state constitutional guarantees of data privacy;
- state limits on when private entities may disclose their customers' data to the government;
- state protections of biometric and genetic privacy, except that two existing Illinois laws would not be preempted; and
- state mandates on online businesses to comply with device settings, like browser signals, that opt-out of data processing.

This bill also would stop state governments, the "laboratories of democracy," from protecting their residents from emergent threats posed by now-unforeseen technologies and business practices, unless state legislators can shoehorn such protections within the narrowly enumerated non-preempted categories.[2]

Thus, EFF urges Congress to remove all of section 404(b) in the current draft. Congress should substitute new language providing that the bill does not preempt any state laws, with the sole exception of state laws that conflict with the federal bill, and then only to the extent of the conflict. At the very least, Congress must dramatically expand the list of non-exempted categories of state laws. EFF hopes the drafters will put consumers first, and make the necessary changes to this language.

No Weakening Current Federal Privacy Laws

Existing federal statutes and regulations place privacy and other important limits on phone companies and other common carriers. These include the Communications Act of 1934. Creating new protections for the public should not require the dismantling of existing protections.

---

[1] Adam Schwartz, Lee Tien, Hayley Tsukayama, and Bennett Cyphers, *Consumer Data Privacy in California: 2019 Year in Review*, Electronic Frontier Foundation (December 31, 2019), available at https://www.eff.org/deeplinks/2019/12/year-review-consumer-data-privacy-california.

[2] See generally *New State Ice Co. v. Lieberman*, 285 U.S. 262 (1932) (Brandeis, J., dissenting).

Thus, EFF is concerned with section 404(b)(3) of the bill as drafted. It would provide that the Communications Act, and associated statutes and regulations, "shall not apply to any covered entity with respect to the collecting, processing, or transfer of covered data under this Act." A "covered entity" includes common carriers now subject to the Communications Act, and "covered data" includes any information that identifies or is reasonably linkable to a person or device.[3][4] This seems to mean that when common carriers process data in a manner subject to the Act, the bill exempts them from existing legal obligations under the Communications Act.

That would be a significant step backwards for regulations of common carriers, with ramifications extending far beyond data privacy. For example, it might even undermine future efforts by administrative agencies to reenact the "net neutrality" rules for common carriers. Thus, EFF recommends the deletion of this section, or at the very least, the addition of substantial new guardrails.

Strong Enforcement

Any strong federal data privacy legislation must contain the most important enforcement tool: the right for consumers to enforce their privacy rights in court. It is not enough for the government to pass laws that protect consumers from corporations that harvest and monetize their personal data. It is also necessary to ensure companies do not ignore them. The best way to do so is to empower ordinary consumers to bring their own lawsuits against the companies that violate their privacy rights. Strong "private rights of action" are among EFF's highest priorities in any data privacy legislation.[5]

Government agencies often lack the resources to enforce existing laws. A private right of action would ensure government agencies or consumers themselves can enforce any protections Congress designs.

Many privacy statutes contain a private right of action, including federal laws on wiretaps, stored electronic communications, video rentals, driver's licenses, credit reporting, and cable subscriptions. So do many other kinds of laws that protect the public, including federal laws on clean water, employment discrimination, and access to public records.[6]

Consumers must also have a real chance to use a private right of action. People often effectively give up such rights when they supposedly "agree" to waive them in terms of service and end user license agreements that they haven't read—and aren't expected to

[3] Section 2(2)
[4] Section 2(8)
[5] Adam Schwartz, *You Should Have the Right to Sue Companies That Violate Your Privacy*, Electronic Frontier Foundation (January 7, 2019), available at https://www.eff.org/deeplinks/2019/01/you-should-have-right-sue-companies-violate-your-privacy.
[6] *Id.*

read. Strong data privacy law should prohibit waivers and mandatory arbitration requirements, which allow companies to sidestep the users' rights.[7]

Unfortunately, while the American Data Privacy and Protection Act has a private right of action, as written, it would not provide the enforcement tools to ensure that bad actors follow the law. EFF has several suggestions on how to improve the enforcement of this bill.[8]

Narrow Exemptions

While statutes generally have at least some exceptions, they must be kept as narrow as reasonably possible, lest the exceptions swallow the rule.

EFF is concerned that many of the exceptions in this bill are too broad, and would undo much of the protection that the bill promises. For example, the bill's across-the-board list of exemptions includes:

- To detect or respond to a security incident;
- To detect against fraudulent or illegal activity; and
- To cooperate with an executive agency or a law enforcement official … concerning conduct or activity … [such agency or official] reasonably and in good faith believes may violate Federal, State, or local law, or pose a threat to public safety or national security.[9]

Also, while the bill grants data subjects rights to access, correct, and delete their data, people cannot exercise those rights if it would "interfere with law enforcement, judicial proceedings, investigations, or reasonable efforts to guard against, detect, or investigate malicious or unlawful activity, or enforce valid contracts."[10] These exemptions should be removed.

FTC Compliance Programs and Guidelines

The bill creates two opportunities for covered entities to compel the FTC to give them guidance on compliance with the law: "technical compliance programs" and "compliance guidelines".[11][12] FTC must respond to requests for either of these within 180 days.[13] As to

[7] Chao Jun Liu and Adam Schwartz, *Stop Forced Arbitration in Data Privacy Legislation,* Electronic Frontier Foundation (April 19, 2022), available at https://www.eff.org/deeplinks/2022/04/stop-forced-arbitration-data-privacy-legislation.
[8] Appendix 1, see below
[9] Section 209(a)(2), (4), and (9)
[10] Section 203(d)(3)(A)(vi).
[11] Section 303
[12] Section 304
[13] Sections 303(c)(2) and 304(a)(3)(A)(iii)

technical compliance programs, "any person" can seek such guidance, including trade associations, and a covered entity can sue the FTC for failing to meet the 180-day deadline, or for denying a request.[14][15]

EFF is concerned that both of these programs will force the FTC to invest its scarce resources in providing guidance on demand from covered entities and others. As a consequence, FTC will have far fewer resources for rulemaking, for investigating alleged violations, for bringing enforcement actions, and for guiding Congress on the need for further legislation. Thus, these sections should be greatly restricted, or even removed. Any inclusion of these sections in the final bill further demonstrates the need for strong private enforcement, and for removal of the impediments to such enforcement discussed above.

EFF also is concerned with the legal impact of this FTC guidance. If a covered entity satisfies a compliance guideline, it is deemed to satisfy the Act.[16] If a covered entity has a history of satisfying a technical compliance program, the FTC and state AGs must "consider" this before investigating or bringing an enforcement action, and a judge must "consider" this in a private enforcement suit.[17]

Further limits on these sections are necessary. It is not enough that compliance guidelines and technical compliance programs must meet or exceed the Act's requirements.[18] Most importantly, courts must be able to independently determine whether a covered entity has violated the Act, even when such violation purportedly falls within either of these two mechanisms.

No "Pay For Privacy" Schemes

Privacy is a fundamental human right. A federal privacy law must recognize this by including a non-retaliation rule that says companies cannot deny goods, charge different prices, or provide a different level of quality to those who exercise their privacy rights. Without this rule, pay-for-privacy systems will make privacy a luxury and exclude lower-income consumers from any intended protections.

The American Data Privacy and Protection Act begins well on this issue.[19] EFF recommends strengthening this section, by prohibiting a covered entity from responding to a person's exercise of their rights by providing them with a different quality of service (in addition to the current prohibitions on denying or terminating their service, or charging them a different price).

[14] Section 303(c)(1)
[15] Section 303(d)
[16] Section 304(c)
[17] Section 303(c)(1)
[18] Section 303(b) and 304(a)(3)(A)(ii)(I)
[19] Section 104

Privacy Safeguards

Consumer data privacy legislation should require companies to obtain consumers' opt-in consent before they collect, retain, use, or share consumers' personal information. If a consumer consents to collection of their information (such as location data to map a running route for a fitness tracker) for one purpose, companies must get additional consent before selling or using data for another purpose. Legislation must also require companies to:

- Minimize their processing of consumers' data, i.e., process it only as strictly needed to give consumers what they asked for;
- Tell consumers what personal information they have collected about them;
- Provide consumers a machine-readable copy of their data; provide consumers a right to correct and delete their data; and
- Act as information fiduciaries to the consumers whose information they have collected.

Congress should also enact a tailored ban on targeted ads based on our online behavior. Removing this incentive to collect and sell as much of our behavioral information as possible would reduce the temptation for bad actors to violate the privacy of American consumers.

Many of the bill's new privacy protections should be strengthened.[20]

* * *

Thank you again for your leadership highlighting this important topic that impacts the privacy and civil rights of all American consumers. The American Data Privacy and Protection Act might be a step in the right direction on many of these issues – assuming it is amended, as discussed above, to ensure strong private enforcement in court, and to not undo other privacy laws at the federal and state levels.

We look forward to working with you to improve this legislation and strengthen the necessary protections.

Sincerely,

India McKinney
Director of Federal Affairs
Electronic Frontier Foundation

[20] Appendix 2, see below

Appendix 1 - Improved Enforcement

EFF recommends the following changes to the draft language to create meaningful enforcement:

1. While the bill protects minors from pre-dispute arbitration agreements and class action waivers, it provides no such protection for adults.[21] While adults may proceed as a class in arbitration, this is woefully inadequate.[22] The protections given to minors should be extended to adults.
2. The bill bars all private enforcement for the first four years after the bill takes effect.[23] This should be removed. Enforcement should begin immediately.
3. The bill bars all private enforcement of key protections of the bill, including data minimization, privacy by design, algorithmic impact statements, and unified opt-out mechanisms.[24] The private right of action should be expanded to cover all of these rules, and others.
4. The bill does not provide the full arsenal of remedies.[25] Liquidated damages and punitive damages should be added.
5. The bill requires private enforcers, before filing suit, to give the FTC and their state attorney general (AG) a 60-day notice of their plans to sue.[26] This needless delay should be removed.
6. The bill bars private enforcers from demanding damages from an entity that violated the new law, before completion of the above 60-day notice period, or after the FTC or AG decides to sue.[27] This needless impediment to litigation should be removed.
7. The bill allows enforcement only in federal court.[28] This should be expanded to state courts. Among other reasons, some state courts have less strict standing rules than the federal courts.
8. The bill requires private enforcers, before filing suit, to give the entity that violated the new law a 45-day notice and opportunity to cure, if the action seeks an injunction, or is against a smaller entity.[29] This should be removed.

[21] Sections 403(b)(1) and (b)(2)(A)
[22] Section 403(b)(2)(B)
[23] Section 403(a)(1)
[24] Section 403(e)
[25] Section 403(a)(2)
[26] Section 403(a)(3)(A)
[27] Section 403(a)(3)(B)(i)
[28] Section 403(a)(2)
[29] Section 403(c)

Appendix 2 - Privacy Safeguards

EFF recommends the following changes to the draft language to create meaningful privacy safeguards:

1. The definition of "sensitive covered data" should be expanded.[30] This is important, because the bill requires opt-in consent to collect, process, or transfer such data.[31] This term should be expanded, for example, to also include employment history, familial and social relationships, and immigration status.
2. The current opt-out rule for data transfers and targeted ads should be changed to an opt-in rule.[32] Notably, the bill already extends opt-in protections to minors from these dangerous data practices.[33] Adults should enjoy these protections, too. Defaults matter, because most people do not change them.
3. The data minimization rule should be tightened to exclude targeted ads.[34] Also, processing should be "strictly" necessary, proportionate, and limited to an allowable purpose, and not just "reasonably" so.
4. The definition of "targeted advertising" should be amended to clarify that it includes data collected by a covered entity from its own customers and users.[35]
5. When a service provider completes a contract with a client, it should be required to delete their client's data, and should not be authorized to keep it so long as they de-identify it.[36] De-identified data is often easy to re-identify. Also, service providers should be banned from combining the data sets they obtain from different clients; rather, these data sets must be kept separate.
6. The rule against processing "nonconsensual intimate images" should be amended to add First Amendment safeguards.[37]
7. The rights to access, correct, and delete data need not be referred to as data "ownership."[38] Data privacy and autonomy are human rights and not property rights.

[30] Section 2(22)
[31] Section 204(a).
[32] Sections 204(c) and 204(d)
[33] Sections 205(a) and 205(b)
[34] Section 101(a)
[35] Section 2(26)
[36] Section 302(a)(3)
[37] Section 102(a)(5)
[38] Section 203