July 18, 2022

**Re: ACLU Statement on American Data Privacy Protection Act, Ahead of Committee Markup**

Dear Chairman Pallone and Ranking Member McMorris Rodgers:

As you prepare for the full House Energy and Commerce Committee markup of the American Data Privacy and Protection Act (ADPPA), the American Civil Liberties Union provides this analysis of the provisions, which 1) highlights and explains important strengths of the legislation, 2) urges specific improvements to help some provisions better achieve their objectives, and 3) urges the deletion or substantial amendment of a few provisions that would undermine privacy, including those that preempt state-level laws that protect people today and into the future. We hope that the Committee uses the markup as an opportunity to send to the full House of Representatives a bill that strongly protects all Americans. The ACLU is not making a vote recommendation now on whether the Committee should report the ADPPA out of committee, but we may later make a scored floor vote recommendation, after review of the legislation as reported out of committee.

The ACLU appreciates your leadership, and the role of the Committee, in advancing the critical discussion on enacting federal legislation to protect our privacy and civil rights. Technology has become ever more sophisticated, but too often its benefits accrue only to those who develop it, while consumers are profiled, targeted, and algorithmically analyzed with no realistic way to exercise personal autonomy. Federal legislation that not only provides Americans with meaningful, enforceable rights but also establishes baseline obligations that prevent businesses from acting against consumers' interests is a critical element to addressing this issue. We are glad to see the Committee turning its attention to this issue in its consideration of the ADPPA.

In its current form, the ADPPA has many provisions that meaningfully advance the privacy and civil rights interests of all Americans. It would move beyond "notice and consent" and place meaningful limits on the uses of personal data, address discriminatory uses of data including biases in algorithmic decision-making, require privacy and security by design, and create mechanisms by which consumers could globally opt out of targeted advertising and data transfers. While these provisions may still require changes to maximize their impact, they all embody principles that are essential to protecting privacy and civil rights. Unfortunately, these advantages are accompanied by provisions that undermine their impact or otherwise fail to advance consumer privacy: a private right of action hamstrung by numerous deficits; obligations on the FTC to spend

ACLU
AMERICAN CIVIL LIBERTIES UNION

**National Political Advocacy Department**
915 15th Street, NW, 6th Floor
Washington, DC 20005-2112
aclu.org

**Kary Moss**
Acting National Political Director

**Anthony D. Romero**
Executive Director

**Deborah N. Archer**
President

scarce resources developing compliance materials for individual companies rather than engaging in robust rulemaking and enforcement; "pay-for-privacy" rules that allow companies to withhold services or charge additional fees to consumers who exercise their rights; problematic exceptions for government-affiliated entities and web scraping that undermine the ADPPA's broad scope; and preemption language that prevents states from enforcing existing protections and complementing federal lawmakers and regulators as they continue to address this complex and rapidly-changing topic into the future.

This letter explains the topics above, as well as other noteworthy aspects of the ADPPA, in greater detail. We urge you to address and resolve these concerns during committee markup and continue to develop a federal privacy bill that provides Americans with the much-overdue protections they expect and deserve.

## Provisions Furthering Privacy and Civil Rights

*Data Minimization*

One of the most notable advances of the ADPPA is its clear limitation on the permissible purposes for which personal data may be collected, processed, or transferred, codified in its provisions concerning data minimization.[1] We encourage the Committee to continue to tighten this provision to ensure that personal data is used exclusively for the benefit of the consumer, not to their detriment.

For too long, American privacy law has hewn to the deeply flawed notice-and-consent model. This approach has condoned exploitative data practices as long as consumers are put on "notice," via privacy policies that consumers lack both the expertise and the time to read, and give "consent" simply by using modern technology or, at best, failing to opt out of harmful practices. The ADPPA rightly rejects this approach, explicitly requiring data to be used only for defined purposes, generally related to the services or products that the consumer receives or their relationship with the company. It does not permit covered entities to simply disclose their intention to use data for an arbitrary purpose and then satisfy data minimization if their use is "reasonably necessary and proportionate" to that purpose.

This fundamental shift protects consumers from numerous practices that have undermined their privacy and safety for too long, from mobile apps surreptitiously collecting and selling location information[2] to online photo services repurposing consumer images to build a facial recognition engine.[3] Consumer data should be used for the consumer's benefit, not treated as corporate property. The ADPPA does well to enshrine this principle in law.

---

[1] Sec. 101.

[2] *E.g.* Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times, Dec. 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[3] Federal Trade Commission, *California Company Settles FTC Allegations It Deceived Consumers about use of Facial Recognition in Photo Storage App*, Jan. 11, 2021, https://www.ftc.gov/news-events/news/press-releases/2021/01/california-company-settles-ftc-allegations-it-deceived-consumers-about-use-facial-recognition-photo.

Nor does the ADPPA somehow restrain innovation or creativity in doing so. Most importantly, the ADPPA tethers data use to the services provided to or communications with the consumer without defining what those services or communications must be. It also permits a wide range of additional permitted purposes that reasonably protect the data holder's interests. What it does not do is allow companies to "innovate" by exploiting data shared for an entirely unrelated purpose, nor should it.

With that in mind, we encourage the committee to tighten the permitted purposes enumerated in Sec. 102(b) to ensure that, to the maximum extent possible, consumer data is only used in ways that align with the consumer's interests. For example, data holders should not be allowed to use consumer data "to conduct internal research or analytics" except to improve the actual services used by that consumer. Other uses should be strictly limited to prevent abuse, including provisions permitting the use of consumer data to combat fraud, promote security, or address legal claims. Finally, the Committee should clarify that no other provision of the ADPPA should be interpreted to imply any additional permitted purposes. Doing so will further the ADPPA's aim of ensuring that consumer data is used to further the consumer's interests, not the collecting party's.

*Civil Rights and Algorithms*

The ADPPA would also significantly strengthen anti-discrimination protections and require certain technology companies to carefully assess the real-world impact of algorithms, including their "disparate impact on the basis of individuals' race, color, religion, national origin, sex, or disability status."

These civil rights provisions would address serious problems that the ACLU has long highlighted. "There is ample evidence of the discriminatory harm that AI tools can cause to already marginalized groups … Bias is often baked into the outcomes the AI is asked to predict [and] the data used to train the AI … and can rear its head throughout the AI's design, development, implementation, and use."[4] "The impact on the daily lives of Americans is unprecedented. Banks and other lenders use AI systems to determine who is eligible for a mortgage or student loan. Housing providers use AI to screen potential tenants. AI decides who's helped and who's harmed with influential predictions about who should be jailed pretrial, admitted to college or hired."[5] "[T]he dangers of AI's algorithmic bias are invisible, complex and hard to describe,"[6] particularly because of the opaque, 'black box' nature of these technologies: often users do not know how these tools are making decisions – or whether or when they are even being used in the first place.[7]

---

[4] Olga Akselrod, *How Artificial Intelligence Can Deepen Racial and Economic Inequities*, ACLU (July 13, 2021), https://www.aclu.org/news/privacy-technology/how-artificial-intelligence-can-deepen-racial-and-economic-inequities.

[5] ReNika Moore, *Biden must act to get racism out of automated decision-making*, Washington Post (Aug. 9, 2021), https://www.washingtonpost.com/opinions/2021/08/09/biden-must-act-get-racism-out-automated-decision-making/.

[6] Moore, *supra*.

[7] *See generally* Comment Letter to National Institute of Standards and Technology, *A Proposal for Identifying and Managing Bias within Artificial Intelligence (Spec. Pub. 1270)* at 7 (Sept. 10, 2021), https://www.aclu.org/letter/aclu-comment-nists-proposal-managing-bias-ai.

The harms posed by algorithmic discrimination are under-appreciated and ongoing. "Thus far, federal agencies that regulate industries using AI have not taken the steps necessary to ensure that AI systems are accountable to the people they impact or that they comply with civil rights laws."[8] And the problems associated with AI and similar technologies show no signs of abating—even in the face of impact litigation by ACLU and other groups.[9]

Overall, the ADPPA addresses a number of these issues in meaningful ways. Namely, Section 207(a) broadly prohibits the collection, processing, or transfer of covered data by a covered entity "in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability." We note that the language "otherwise makes unavailable" has generally been construed by courts to provide a legal cause of action for "disparate impact" violations.[10]

Section 207(c) also requires that big technology companies (referred to as 'large data holders') using algorithms conduct annual impact assessments that include a description of key aspects of the algorithm such as its design, the data used to train it, and its inputs and outputs, an analysis of the "necessity and proportionality of the algorithm in relation its stated purpose," and an accounting of the steps taken to "mitigate potential harms," including harms related to disparate impact based on protected characteristics. The Act also requires all companies covered by the bill regardless of size to evaluate the design of new algorithms before deploying them, and to use an independent auditor for these evaluations and impact assessments when possible. Systematically assessing the potential bias and discriminatory effects of complex and often opaque technologies is highly valuable and distinct from what existing federal laws or regulations offer.

Additionally, the ADPPA advances other, overarching privacy protections that further civil rights goals, for example, by ensuring that data is only collected and used for proportional and necessary purposes.

Collectively, ADPPA would also expand federal civil rights protections by making it explicit that anti-discrimination protections apply far beyond the 'brick and mortar' context (such as physical stores, restaurants, and hotels) to new technologies and software services. The ADPPA also includes sex as a protected characteristic, which is otherwise not included in other federal laws governing discrimination in public accommodations. Finally, the ADPPA provides users with some ability to vindicate their rights through legal action in federal court, which has historically proven to be a critical venue for civil rights enforcement – although there are some real limitations discussed below.

We urge the Committee to amend the legislation to help ensure that the full scope of protections afforded by this provision are enforceable.

---

[8] Akselrod, *supra*.
[9] *See, e.g.*, Linda Morris and Olga Akselrod, *Holding Facebook Accountable for Digital Redlining* (Jan. 27, 2022), https://www.aclu.org/news/privacy-technology/holding-facebook-accountable-for-digital-redlining.
[10] *See, e.g.*, *Texas Dep't of Hous. & Cmty. Affs. v. Inclusive Communities Project, Inc.*, 576 U.S. 519, 545–46 (2015) ("disparate-impact claims are cognizable under the Fair Housing Act upon considering its results-oriented language, the Court's interpretation of similar language in Title VII and the ADEA, Congress' ratification of disparate-impact claims in 1988 against the backdrop of the unanimous view of nine Courts of Appeals, and the statutory purpose.")

First, some of the language in the civil rights section, 207(a), would benefit from being more explicit. The anti-discrimination provision currently prohibits the collection, processing, or transfer of covered data by a covered entity "in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability." Under controlling Supreme Court precedent, the language "on the basis . . . of sex" must include discrimination on the basis of sexual orientation or gender identity in light of the Supreme Court's 2020 ruling in *Bostock*.[11] However, to minimize any residual risk of incorrect statutory interpretations, we suggest 207(a) explicitly include discrimination "on the basis of . . ." "sexual orientation or gender identify." Likewise, we understand the language about "otherwise makes unavailable" to encompass a disparate impact claim, in parallel with similar language under Title VII and the ADEA.[12] But in light of the divided nature of past Supreme Court rulings on disparate impact, and to eliminate any risk of erroneous interpretations, we suggest explicitly referencing disparate impact violations in 207(a). The added language could be fairly simple, if need be (e.g., "otherwise makes unavailable the equal enjoyment of goods or services (*i.e., has a disparate impact*) on the basis of …").

Second, while the impact assessments and algorithm design evaluations required under the ADPPA are a critical step forward, the ADPPA solely requires that those be submitted to the FTC, which is insufficient to provide much needed transparency for the public. We encourage the Committee to amend the ADPPA to require that detailed summaries of the impact assessments and evaluations be published, whereas currently 207(c)(1)(B)(3)(C)(i)(III) leaves it up to companies to decide whether to publish a summary under ("*may* make a summary of such impact assessment and evaluation publicly available in a place that is easily accessible to individuals.") (emphasis added). Likewise, only the baseline non-discrimination provisions of the ADPPA civil rights section are designed to empower the general public to understand and protect their own rights in court (through a private right of action). The ADPPA's private right of action as currently drafted may not be used to enforce the requirements concerning algorithmic impact assessments or algorithmic design evaluations.[13] This means that there would be essentially no individual remedy for a user if a company failed to conduct any impact assessment whatsoever or materially diverged from its own assessment and mitigation plan (e.g., regarding disparate impact on race).

Third, the ADPPA's definition of "covered data" explicitly exempts "employee data" in fairly broad terms, particularly as it pertains to data regarding job applicants. That exemption is concerning because it would mean that individuals who encounter discriminatory hiring technology, for example through an employer's job application web site, do not have civil rights protections under the Act. Additionally, as currently drafted, it is unclear that software vendors that are providing technology related to job applications would have to conduct an impact assessment or algorithmic design evaluation at all—which could constitute a major gap in the enforcement landscape.

---

[11] *Bostock v. Clayton Cnty., Georgia*, 140 S. Ct. 1731, 1741 (2020) ("The statute's message for our cases is equally simple and momentous: An individual's homosexuality or transgender status is not relevant to employment decisions. That's because it is impossible to discriminate against a person for being homosexual or transgender without discriminating against that individual based on sex.").

[12] *See, e.g.*, *Inclusive Communities Project, Inc.*, 576 U.S. at 545–46.

[13] The private right of action provided in Section 403(e) is limited only to violations of the core anti-discrimination provision (Section 207(a)), but not for failure to properly conduct or reasonably adhere to an impact assessment (Section 207(c)).

Fourth, the protections for civil rights and algorithms should not apply exclusively to "covered data," which excludes information obtained from online content or visual observation (as well as other categories of data), and even express information or inferences therefrom about a consumer's race, color, religion, national origin, sex or disability. While First Amendment-related concerns may require limiting the application of other provisions to publicly available information, there is no reason it should be excluded from provisions regarding civil rights and algorithmic bias.

Fifth, certain key provisions of the law (e.g., about impact assessments, 207(c)(1)(A); *see also* 301 (d)(1)) only apply to large data holders, which are defined rather restrictively.[14] This means that many large or medium-sized technology businesses that have massive amounts of user data, significant market impact, and the resources to comply with the Act would be exempt from key provisions. While all covered companies irrespective of size must conduct algorithmic design evaluations, those are inferior to the impact assessments that only large data holders must conduct, which are more stringent in their requirements and include post-deployment evaluation of harm.

Sixth, the Act largely excludes banks through the definition of "covered entity," since the Federal Trade Commission does not regulate, among other things, "banks, savings and loan institutions, and federal credit unions."[15] Practically speaking, that means that a large bank could continue to collect and use voluminous amounts of data through its web sites, apps, and other software services and – even if it used the same AI technology as other companies – it would be exempt from the Act, including its anti-discrimination and impact assessment requirements. The financial services and access that banks provide – or choose not to provide -- are obviously hugely consequential for individuals and communities of color.

*Privacy by Design and Data Security*

The ADPPA wisely codifies the FTC's long-standing efforts to require that companies implement privacy by design and data security, including reasonable efforts to mitigate privacy risks and protect against security breach, while also enhancing the FTC's ability to enforce these obligations. Not only does a legislative mandate reduce the risk of court decisions undermining the FTC's enforcement authority in this area, the ADPPA allows the FTC to impose monetary fines on even first-time violators of the privacy by design and data security provisions (as well as other provisions of the Act).[16] Moreover, the ADPPA does not preclude the FTC from pursuing an action under Section 5 of the FTC Act rather than under the ADPPA if it so chooses. Instead, the ADPPA more narrowly prohibits bringing actions for the same conduct under both the ADPPA and Section 5.

---

[14] *E.g.*, large data holders only include covered entities that in the last year (1) had over $250 million in gross revenues; and (2) collected, processed, or transferred the covered data of (a) more than 5,000,000 individuals or devices; and (b) the sensitive covered data of more 200,000 individuals or devices.

[15] *See* FTC, "Consumer Finance," https://www.ftc.gov/news-events/topics/consumer-finance ("The FTC's authority covers for-profit entities such as mortgage companies, mortgage brokers, creditors, and debt collectors – *but not banks, savings and loan institutions, and federal credit unions*.") (emphasis added). The Act partly exempts from data security requirements certain other financial institutions covered by Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), or the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.)).

[16] Sec. 401(c)(1).

If effectively enforced, the privacy by design and data security mandates would significantly benefit consumers. We do, however, have broader concerns about the FTC's ability to prioritize such enforcement given its numerous obligations under the ADPPA, discussed in more detail below.

**Provisions Needing Improvement to Accomplish Their Objectives**

*Private Right of Action*

When companies or other data collectors violate our privacy rights, we should personally be able to hold them accountable, period. A private right of action is essential to empower us to exercise our own rights and enforce the protections of the law, particularly where government agencies have limited resources—especially in our current economic environment—and thus lack the capacity (and perhaps incentive) to pursue every violation. A robust private right of action would ensure that the rights and obligations of the ADPPA are taken seriously, and violations are avoided rather than viewed as an acceptable cost of doing business. For this reason, Congress has ensured that federal privacy[17] and civil rights laws[18] are enforceable via a private right of action.

Although the ADPPA does contain a private right of action, with the possibility of pursuing monetary damages as well as injunctive relief, that right of action is otherwise deficient in a wide range of respects. These deficiencies are significant enough that the private right of action is unlikely to serve either as an effective vehicle for rights enforcement or as a motivator to comply with the law in order to avoid the risk of liability.

First, while allowing entities limited time to comply with a new law before facing liability may be appropriate, forcing consumers to wait four years for the ability to vindicate their own rights is neither reasonable nor typical. A delay of that length will leave people vulnerable to significant violations of their rights without recourse and increases the likelihood that the private right of action will be amended into oblivion by future congresses before it is ever in effect.

In addition, we see the following issues that lessen the impact of a private right of action in the ADPPA:

- **Limited application.** The PRA does not apply, most notably, to data minimization requirements (though it does apply to restricted practices, i.e. misuse of sensitive covered data). It also does not apply to privacy by design, or non-compliance with

[17] For example, the Stored Communications Act provides a private right of action, including a statutory minimum of $1,000 damages per infraction, for violations. 18 U.S.C. § 2707. The Communications Act also provides a private right of action for violations of the rules protecting the privacy of Customer Proprietary Network Information, or CPNI. 47 U.S.C. § 207.

[18] According to the Supreme Court, there is "no doubt" that Congress authorized private rights of action to enforce both Title VI and Title IX. Cannon v. Univ. of Chicago, 441 U.S. 667, 703 (1979).

algorithmic impact assessment, privacy impact assessment, or various other requirements.[19]

- **Lack of statutory damages**. Actual damages accruing from privacy harms, at least those unassociated with identity theft or other financial crimes, are notoriously difficult to prove. Statutory damages are essential to provide appropriate remedies for harmed individuals and incentives for covered entities, which is why many privacy and consumer protection statutes include them. Punitive damages for particularly egregious behavior would also be appropriate.
- **Discretionary attorney's fees.** Particularly given the lack of statutory damages, the absence of mandatory attorney's fees means that only wealthy plaintiffs willing to fund their own case with limited prospect of recovery are likely to bring suit.
- **Government priority.** Private plaintiffs who suffer significant injuries, and thus present highly winnable cases, will be preempted from pursuing either litigation or a negotiated settlement if either the FTC or the AG steps in, further disincentivizing plaintiffs from investigating violations or pursuing complaints.
- **Mandatory arbitration.** While class action claims are expressly permitted, they may be limited to arbitration rather than judicial forums for adult plaintiffs. This is likely to seriously prejudice ordinary people's ability to obtain relief for violations of their rights under the law.
- **Right to cure.** While the right to cure is at least limited to cases seeking injunctive relief, it does limit the threat of litigation as an incentive to "do it right the first time," instead allowing covered entities to remedy infractions only after they face litigation.
- **Magic words.** Finally, any settlement offer or other "request [for] monetary payment" must include specific language specified in the ADPPA or "the person or joint class of persons shall forfeit their rights under this section." The contrast with the right to cure is particularly stark: while data holders that violate the ADPPA can remedy their actions, ordinary consumers may irrevocably forfeit their rights because of clerical errors and similarly insignificant mistakes.

Consumers need a practical mechanism to enforce their rights, not an obstacle course without even the likelihood of a meaningful remedy at the end. We recommend that the Committee ensure that the private right of action gives consumers a meaningful opportunity to enforce the ADPPA and protect their own privacy.

*Federal Trade Commission Authority and Obligations*

The FTC is given a central role in realizing the objectives of the ADPPA, made all the more critical by the deficits in the private right of action described above. The ADPPA, recognizing that centrality, grants the FTC considerable new authority and powers. Yet it also provides stark limits on its authority in other areas, while burdening it with various obligations on behalf of covered entities that threaten to consume its limited resources. The FTC's role should be streamlined to emphasize protecting consumers from predatory and

[19] In some cases, such as algorithmic impact assessments, private individuals lack even the knowledge of whether an impact assessment has been completed.

otherwise harmful data practices, not protecting companies from the risks of an enforcement action when they push the boundaries of the law.

The ADPPA does give the FTC one potent tool it lacks: violations of the Act are equivalent to violations of a rule defining an unfair or deceptive act or practice under the FTC Act, which allows the FTC to levy monetary penalties for first-time offenses.

The ADPPA also grants the FTC rulemaking authority, an essential tool to ensure that the ADPPA's protections endure against a backdrop of constantly changing technology and data practices. However, the FTC's authority to issue regulations too is narrow; in particular, the FTC's authority to increase the protections or obligations of the ADPPA in response to new threats or practices appear to be limited to establishing additional categories of sensitive personal information and technology-neutral data security processes.

Conversely, the ADPPA imposes multiple obligations on the FTC that appear to protect companies rather than consumers. The FTC is required to evaluate self-regulatory proposals, prepare non-binding guidance on a variety of topics, generate numerous reports and studies concerning the impact of the ADPPA, and even establish an "Office of Business Mentorship" tasked with guiding companies rather than protecting consumers.

While many of these latter provisions are not harmful per se, they threaten to siphon resources away from the FTC's enforcement activities. And while the ADPPA authorizes additional funding for the FTC, it does not commit to any specific amount. As such, barring an ironclad commitment to provide adequate funding to the FTC to robustly enforce the ADPPA while also fulfilling its new obligations, we encourage the Committee to amend the ADPPA to focus on the FTC's mission of protecting consumers by enforcing the privacy and civil rights protections in the ADPPA.

*Consumer Choice*

Opt-in consent is the most meaningful way to ascertain consumer preferences. Companies should be required to obtain permission *before* collecting and using consumers' data. In contrast, an opt-out requirement allows companies to use consumers' information without their consent and places enormous burden on consumers who wish to protect their data. An opt-out approach forces individuals to navigate complex systems to identify each and every entity that collects their data, determine the entity's opt-out procedure, and follow through with it. This approach disproportionately burdens those who often do not have sufficient time or knowledge—namely the elderly, the disabled, and those for whom English is not a first language.

While the ADPPA's unified opt-out provisions are better than requiring consumers to individually opt out for each site, the provisions still place the burden on consumers to make an unprompted choice. We encourage the Committee to require opt-in consent for all data—an approach that best protects consumers by requiring companies to explain and justify their need for personal information before they collect, use, and share that information.

If opt-in consent is not required, at a minimum, we encourage the Committee to ensure that universal opt-out requests are strengthened so that their reach is global as intended. As

currently drafted, third parties are exempted from consumer requests to opt out of the transfer of their personal data or to opt out of targeted advertising with respect to third party data,[20] and only those third parties that qualifies as third-party collecting entities are required to comply with "Do Not Collect" requests.[21] In addition, the ADPPA does not impose any obligation on third parties to comply with requests forwarded from the source of the data, the mechanism used to address this scenario in the CPRA.[22] As a result, once data is transferred to a third party, a consumer loses any right to control such data through the exercise of a unified opt-out mechanism,[23] and is left with the far inferior recourse of identifying each and every third party in possession of their personal data and submitting an individual request to delete to each. This undermines the purpose of the unified opt-out mechanism.

Finally, the current language of the ADPPA excludes "first-party marketing" from any consent provisions, including the universal opt-out provisions. If first-party marketing is not narrowly defined, it may be interpreted expansively by advertisers and others, causing the ADPPA to fail in its objective of providing consumers with an opportunity to exercise control. We encourage the Committee to eliminate, or at least narrowly define, provisions related to first-party data, marketing or advertising to avoid this outcome.

*Pretextual Consent & Individual Autonomy*

Deceptive design patterns, also known as "dark patterns," are design decisions that undermine an individual's autonomy, using a range of techniques to encourage individuals to "choose" an unintended or undesired option. This practice is unfortunately widespread, with hundreds of examples by major companies.[24] As such, it is essential that privacy and consumer protections directly address this practice.

The ADPPA does so through strong language prohibiting "pretextual consent" or preserving "individual autonomy," both of which proscribe consent obtained through either false or deceptive statements or designs "with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision making, or choice to provide such consent or any covered data."[25] This language provides the essential clear prohibition on deceptive design.

Unfortunately, the ADPPA imposes this prohibition sparingly. The provisions prohibiting deceptive design only apply to a limited number of interfaces and choices presented to consumers: the transfer of sensitive data or data about a minor, or any transfer by a service provider; the use of browsing or search history for advertising purposes, or to withdraw previously given affirmative express consent. It does not, however, apply to numerous other

---

[20] Sec. 302(d)(3).
[21] Sec. 206(b)(3)(C).
[22] The latest draft regulations of the CPRA would explicitly impose such a requirement on third parties. Draft CPRA Regulations § 7052(a), https://cppa.ca.gov/regulations/pdf/20220708_text_proposed_regs.pdf.
[23] If the third party is a third-party collecting entity, the consumer may be able to leverage the "Do Not Collect" mechanism to accomplish a simpler outcome—but that not only places an additional burden on the consumer, it assumes that mechanism is effective in all contexts, which may not be the case where consumers are identified in a manner that does not correspond to a Do Not Collect request.
[24] *See, e.g.,* Deceptive Design Hall of Shame, https://www.deceptive.design/hall-of-shame/all.
[25] Sec. 2(1)(D).

choices presented to consumers, including the use of deceptive practices to manipulate consumers into signing up for a service justifying data collection in the first place, providing specific information at the collector's behest, or any other decision that might impact the collection, processing or transfer of personal data.[26]

While these practices may well be subject to the FTC's traditional enforcement of unfair or deceptive trade practices,[27] there is no reason that such practices should not be subject to the enhanced enforcement powers of the ADPPA. The ADPPA should therefore prohibit deceptive design in any interaction with consumers, not merely a select subset.

*First Amendment Concerns*

The ADPPA includes the caveat that it shall not be construed "to limit or diminish First Amendment freedoms to gather and publish information guaranteed under the Constitution" under a heading titled "Journalism." It is important to clarify further what this instruction means, to ensure that important First Amendment-protected speech and activity is not unjustifiably prohibited by the Act.

First, some constitutionally-protected information gathering and publication is done by entities that are not media organizations, or that do not define themselves as engaged in journalism per se. Nonprofits doing advocacy work, for example, should also be recognized as often engaged in core protected speech activity that would otherwise be regulated by the ADPPA. At a minimum, the ADPPA should make clear that the limiting construction above applies to any covered entity, not just those engaged in journalism.

Second, the exceptions to the rights of access, correction and deletion should be broadened to avoid chilling constitutionally-protected speech. For example, as currently drafted, it is unclear whether an advocacy group focused on good government that collects information on individual law enforcement officers must honor access or deletion requests under the ADPPA, and whether its ability to do so turns on whether the covered entity holding the information is a media organization or not.

While the exceptions for public figures, for example, are welcome, they do not cover all situations in which important speech is at stake. In the above example, individual law enforcement officers may not be regarded as public figures and any complaints about them, particularly if about off-duty behavior, may not fall within the exceptions.

The exceptions to the rights of access, correction and deletion should be expanded, to ensure that covered entities can conduct such investigations or hold information about allegations of wrongdoing by individuals (or confidential discussions about them) without having to reveal that information to those subjects.

---

[26] In addition, the current draft is unclear as to the form of consent required upon material changes to a privacy policy or practice: while the relevant section is titled "Affirmative Express Consent," the text describes only an opportunity to opt out. Sec. 202(e)(1).

[27] *FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads*, https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

In some scenarios, such access to information by a subject could reveal the sources of the information even if the covered entity received the information in confidence. Such right of access could potentially lead to the subject of allegations of wrongdoing demanding the deletion of the data incriminating them—thereby preventing any intended publication, or any intended non-public sharing of such information.

*De-Identification*

De-identification, used properly, is an important tool to protect privacy, allowing uses of data that protect individuals by ensuring that the two cannot be linked. However, it is also ripe for abusive interpretations, particularly those that allow companies to evade obligations under the law by classifying information as "de-identified" while retaining the ability to re-identify such data in the future. We encourage the Committee to address this by clarifying that covered entities may not classify information as de-identified if they retain the ability to re-identify it, regardless of any "administrative" or "physical" obstacles they have imposed (and thus retain the ability to remove).[28]

**Provisions that Should Be Eliminated or Substantially Altered**

*State Law Preemption and Alterations to Federal Privacy Provisions*

If the objective of the ADPPA is to protect the privacy of Americans, it should start by preserving the numerous protections already enshrined in law to the maximum extent possible. Congress has historically given states room to enact stronger privacy[29] and civil rights[30] protections than those embodied in federal law. States, the venerable "laboratories of democracy," serve a particularly critical function in a space as rapidly evolving as data privacy. The ADPPA should serve as a floor providing minimum protections for all Americans, not a ceiling. Preemption should be reserved to address situations where compliance with multiple legal regimes is simply not practicable—particularly where there is no evidence that the current state laws are incompatible or that companies are unable to find innovative methods of meeting their requirements. And neither language limiting preemption to provisions "covered by" (rather than merely "related to") the ADPPA nor the limited set of exemptions to preemption adequately preserve that necessary space.

Barring continuing Congressional attention to the issue of data privacy, preemption would freeze the current regime in place and preclude states from enacting stronger protections that are already in the works. States such as Massachusetts, New York and Washington would be barred from passing already-introduced comprehensive data privacy laws that include more robust duties of loyalty than those found in the ADPPA. Counties and municipalities would be unable to bar the deployment of many forms of surveillance technologies in their communities. And states would be left to rely on Congress (given the

[28] Such protections remain important in the context of de-identified data transferred to a service provider or third party, however.

[29] For example, the Graham-Leach-Bliley Act preempts state laws only where they fail to provide greater protection than that Act. 15 U.S.C. § 6807(b).

[30] *See* 42 U.S.C. § 2000h-4 (("[n]othing contained in any title [of the Civil Rights Act of 1964] shall be construed as indicating an intent on the part of Congress to occupy the field in which any such title operates to the exclusion of State laws on the same subject matter.")

FTC's limited rulemaking authority) to adapt to new threats and challenges as technology continues to evolve. Even were a robust form of the ADPPA enacted, it would not guarantee that more Congressional action will follow in the near future.

Preemption would also reverse stronger protections based upon laws *already* enacted. Examples of such preemption, weakening rather than strengthening consumer privacy, include but are not limited to:

- **Sensitive data.** State-level consumer privacy laws provide heightened protection for categories of information not deemed "sensitive" by the ADPPA, such as CPRA's inclusion of "racial or ethnic origin, religious or philosophical beliefs, or union membership." State-level laws also provide greater protection for sensitive data than the ADPPA: both the Colorado Privacy Act (CPA) and the Virginia Consumer Data Protection Act (VCDPA) require affirmative consent to process sensitive data at all.
- **Broadband and telecommunications customer data.** The Communications Act subjects Customer Proprietary Network Information and cable and satellite customer data to strict limitations on disclosure with robust enforcement mechanisms. In addition, after the repeal of the FCC's Broadband Privacy Rule, Maine, Minnesota and Nevada passed broadband privacy laws specifically targeting broadband ISPs.
- **Data security.** Several states, including Massachusetts, have enacted laws and regulations specifically governing data security that have different criteria for assessing reasonable security practices, additional mandatory practices, penalties or enforcement mechanisms, or other obligations or consequences above and beyond ADPPA's data security provisions.[31]
- **State constitutions.** States including Washington and California have constitutional rights to privacy that apply even against private parties, providing a critical tool for courts to protect against abuses as technology and corporate practices evolve.
- **State agencies.** State-level agencies have considerable rulemaking authority, which allows them the flexibility to adapt to meet the needs of the moment. The California Privacy Protection Agency, for example, is authorized to promulgate regulations allowing for cybersecurity and privacy audits.[32]
- **Mandatory floor.** State ballot initiatives, such as the CPRA, can create an effective floor to privacy protections, allowing legislators to improve but not weaken protections in the future. Congress lacks any such mechanism short of a constitutional amendment.

The federal and state governments both have important roles to play in protecting consumer privacy. The ADPPA can best advance that goal by addressing actual conflicts between regimes and otherwise serving as a baseline, not a ceiling, for privacy rights.

*Entities Acting on Behalf of Government Agencies*

[31] MA. GL 93H & 20 CMR 17.
[32] Ca. Civ. Code 1798.185(a)(15) & (a)(18).

The current draft of the ADPPA excludes from the definition of covered entity not only government entities themselves but "a person or an entity that is collecting, processing, or transferring covered data on behalf of [any] government entity."[33] This exception is deeply problematic and misguided, allowing commercial entities to obtain data nominally covered by the protections of the ADPPA and then turn around and leverage their blanket exemption to use it in ways outside of the ADPPA's permitted purposes and often outright harmful to the data subject's interests. It would countenance companies like Clearview AI compiling a faceprint database from any source, whether "publicly available" or not, and profiting from the sale of that information.

Excluding "government service providers" who exclusively process information provided by government entities would be a far more sensible approach. But the ADPPA should not give private entities carte blanche to flout its requirements simply because their (possibly not even exclusive) customer is a government agency.

*Pay for Privacy*

The ADPPA includes a section entitled "Loyalty to Individuals with Respect to Pricing." Unfortunately, this provision permits, rather than prohibits, "pay-for-privacy" regimes that allow data holders to charge higher prices or offer reduced services to consumers who exercise their rights.

Pay for privacy transforms privacy from a fundamental right to a luxury good. This is particularly problematic because lower-income communities are particularly vulnerable to predatory data practices. Provisions like this increase marginalization and exacerbate the digital divide. The Committee should instead ensure that ADPPA provides robust private protections, including the basic right to control one's own data, to every consumer.

*Sensitive Covered Data*

Rather than a uniform opt-in regime, ADPPA pursues a two-tier approach, with tighter minimization requirements on the collection and use of, and opt-in consent for the transfer of, "sensitive" data. While we understand the desire to calibrate the degree of protection to the sensitivity of the data, this distinction is ultimately unworkable in an age of machine learning, where it is typically impossible to know what information a model has "derived" or "inferred" from its inputs.

In addition, so-called non-sensitive information can be leveraged for purposes that are quite sensitive. For example, if Cambridge Analytica is to be believed, "non-sensitive" information such as social media likes can be used for highly sensitive activities such as influencing how individuals vote.

"Sensitive" data also serves a second purpose: it determines the protection afforded to inferences based on publicly available information. Here, however, the difference between sensitive and non-sensitive data is even more dramatic: while inferring sensitive information is subject to heightened protections under the ADPPA, inferences that do not include sensitive information are exempt from the law entirely. Again, given the opaque

[33] Sec. 2(9)(B)(ii).

nature of "inferences" in the machine learning setting, this distinction is likely impracticable.

We believe that the best approach to protecting consumer privacy is to impose strong basic requirements for all data, coupled with context-specific decisions about privacy and security safeguards that consider the potential ways that the data at issue could be used to harm the consumer.

Failing that, we recommend that "sensitive covered data" include any information related to protected characteristics, including race, ethnicity, religion, national origin, immigration status, disability, sex, gender identity and sexual orientation—the last under all circumstances, not merely when the data holder determines whether its use would be "consistent with the individual's reasonable expectation of privacy" as currently drafted. Consumers, not data holders, should have the final say as to whether such information should be shared with any third party, and should know that its collection and processing is subject to scrutiny.

---

The ACLU greatly appreciates the work and commitment to privacy and nondiscrimination reflected in the ADPPA, but at the same time, we also have serious concerns about the likely effect of several provisions. Importantly, all of the problems can be fixed. The ACLU strongly urges the Committee to address and resolve these concerns during markup and send to the House floor a bill that will finally and fully provide the privacy and nondiscrimination protections that all Americans have long deserved. If you have any questions about this legislation, please contact Chris Anders at canders@aclu.org. Thank you again for your work on this matter.

Sincerely,

Christopher E. Anders
Federal Policy Director