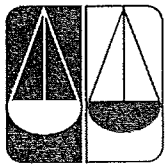

LAWYERS' COMMITTEE FOR
CIVIL RIGHTS
UNDER LAW

STATEMENT OF DAVID BRODY

MANAGING ATTORNEY OF THE DIGITAL JUSTICE INITIATIVE

LAWYERS' COMMITTEE FOR CIVIL RIGHTS UNDER LAW

U.S. HOUSE COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE

HEARING ON

PROTECTING AMERICA'S CONSUMERS: BIPARTISAN LEGISLATION TO STRENGTHEN DATA PRIVACY AND SECURITY

JUNE 14, 2022

I. Introduction

Chair Schakowsky, Ranking Member Bilirakis, and Members of the Committee, thank you for the opportunity to testify today on bipartisan, bicameral legislation that seeks to strengthen data privacy, security, and civil rights. My name is David Brody, and I am the Managing Attorney of the Digital Justice Initiative at the Lawyers' Committee for Civil Rights Under Law ("Lawyers' Committee").

The Lawyers' Committee uses legal advocacy to achieve racial justice, fighting inside and outside the courts to ensure that Black people and other people of color have voice, opportunity, and power to make the promises of our democracy real. Our Digital Justice Initiative works at the intersection of racial justice, technology, and privacy to address predatory commercial data practices, discriminatory algorithms, invasions of privacy, disinformation, and online harms that disproportionately affect Black people and other people of color, including people with intersectional identities, like immigrants, women of color, and LGBTQ people of color.

If a business posts a sign that says "Whites Only", it should not matter whether it is written in ink or pixels. The discrimination is the same. The harm is the same. And the legal consequences should be the same. We care about data privacy because it ensures that who we are cannot be used against us unfairly. Privacy rights are civil rights.

Every individual deserves the full measure of freedom in their engagement with an online and data-driven world—both freedom to and freedom from. Freedom to define yourself. Freedom to organize and advocate for what you believe. Freedom to learn. Freedom to play. Freedom to start a business or find new opportunities. Freedom to be let alone.

Achieving racial justice in a digital world also requires advancing freedom from discrimination and inequity. Everyone has a right to engage in the online economy free from algorithmic bias, digital redlining, and pervasive surveillance.

We are encouraged by the American Data Privacy and Protection Act, a bipartisan and bicameral effort to safeguard data privacy and civil rights online. Passing comprehensive privacy legislation would be a major advancement for the public good. The proposed bill includes a number of provisions that would protect the rights of all Americans, and some areas where we hope the legislation can be improved.

First, the bill would prohibit discriminatory uses of personal data and require companies to test their algorithms for bias. We know from years of reporting and research that algorithms used for advertising and eligibility decisions frequently produce discriminatory outcomes and restrict access to housing, employment, credit,

healthcare, education, and other businesses. This discrimination disproportionately impacts Black and Brown communities, as well as other marginalized and disenfranchised groups.[1]

Second, the bill would require companies to collect and use only as much personal data as is reasonably necessary to provide the services that consumers expect, and to safeguard that data. Reducing the amount of unnecessary personal data floating around online reduces the potential for that data to be abused. Identity theft and fraud disproportionately impact communities of color, and low-income consumers are less likely to have the resources to bounce back after being ripped off.[2]

Third, the bill would give individuals transparency into and control over how their data is used. Requiring disclosure of data practices—including revealing with whom a company shares your information—is essential to identifying and mitigating discriminatory practices. The bill also empowers individuals with the ability to access, correct, and delete their own information.

However, there are parts of the bill that need improvement. Most importantly, the narrow private right of action severely curtails the ability of individuals to obtain relief from a court when a company violates the Act. A right without a remedy is no right at all to people who have been wronged. The current proposal inserts several procedural hurdles that will not reduce litigation costs but will block injured individuals from being able to have their day in court—such as traps designed to trip up individuals who do not use magic words when asserting their rights. If we are to have rule of law, we must allow the law to rule. In addition, the bill gives many new responsibilities and authorities to the Federal Trade Commission, as it should. It is imperative for Congress to ensure that the FTC also receives all of the resources it needs to successfully execute this new mission.

Almost sixty years ago, we decided as a nation that our polity is stronger when everyone has a fair chance. Congress passed the Civil Rights Act of 1964 to prohibit segregation in interstate commerce. The internet and other novel technologies create new challenges to the prevention and elimination of redlining and discrimination. It is time to build upon our civil rights infrastructure to ensure that everyone has equal

---

[1] *See* JANE CHUNG, RACISM IN, RACISM OUT: A PRIMER ON ALGORITHMIC RACISM, PUBLIC CITIZEN 10 (2022), https://www.citizen.org/article/algorithmic-racism/; YESHIMABEIT MILLNER AND AMY TRAUB, DATA CAPITALISM AND ALGORITHMIC RACISM, DATA FOR BLACK LIVES AND DEMOS (2021), https://www.demos.org/sites/default/files/2021-05/Demos_%20D4BL_Data_Capitalism_Algorithmic_Racism.pdf.

[2] FED. TRADE COMM'N, SERVING COMMUNITIES OF COLOR: A STAFF REPORT ON THE FEDERAL TRADE COMMISSION'S EFFORTS TO ADDRESS FRAUD AND CONSUMER ISSUES AFFECTING COMMUNITIES OF COLOR (2021), https://www.ftc.gov/system/files/documents/reports/serving-communities-color-staff-report-federal-trade-commissions-efforts-address-fraud-consumer/ftc-communities-color-report_oct_2021-508-v2.pdf.

opportunity on the internet and fair access to the information, goods, and services it enables.

II. Lack of Privacy and Online Civil Rights Protections Adversely Impacts Communities of Color

Privacy legislation is a civil rights issue because it can help ensure that people's identities and characteristics cannot be used against them unfairly. Strong legislation can secure for everyone the "inviolability of privacy" that is "indispensable to preservation of freedom of association."[3] Such protections can empower communities of color and open doors for marginalized populations. It can also provide clarity to businesses and level the playing field for entrepreneurs.

However, there is currently no comprehensive federal privacy law. Existing anti-discrimination laws have many gaps and limitations as well. Some exclude retail or have unresolved questions as to whether they apply to online businesses. Others apply to specific sectors, like housing and employment, but may not cover new types of online services used to match individuals to these opportunities. To give a few examples, under current federal law it would be legal for an online business to charge higher prices to women or to refuse to sell products to Christians.[4] A service provider could use discriminatory algorithms to look for workers to target for recruitment so long as the provider does not meet the definition of an "employment agency" under Title VII.[5] And it is wholly unclear whether existing laws will apply at all to discrimination in many new online-only economies related to online gaming, influencers, streamers, and other creators.

As a result of gaps in federal law, individuals currently have little recourse against discriminatory algorithms and AI models used in commercial data practices that reinforce the structural racism and systemic bias that pervade our society. Tech companies can misuse personal data, intentionally or unintentionally, to harm marginalized communities through deception, discrimination, exploitation, and perpetuation of redlining. Absent updated and robust anti-discrimination protections, online businesses can deny service on the basis of race or ethnicity, provide subpar products based on gender or sexual orientation, charge higher rates based on religion, or ignore the accessibility needs of persons with disabilities.

This dynamic is deeply contrary to cornerstone principles and promises of equal access and a level playing field for everyone. Without strong privacy and online civil rights protections, discrimination will continue to infect the digital marketplace. Not surprisingly, extensive documentation cited below demonstrates that consumers

---

[3] *NAACP v. Alabama*, 357 U.S. 449, 462 (1958).

[4] *See* 42 U.S.C. §§ 1981, 2000a; *Shaare Tefila Cong. v. Cobb*, 481 U.S. 615 (1987).

[5] Aaron Rieke and Miranda Bogen, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, UPTURN (2018), https://www.upturn.org/reports/2018/hiring-algorithms/.

of color continue to receive worse treatment and experience unequal access to goods and services due to discriminatory algorithms and exploitative data practices.

In advertising, for example, Facebook (now known as Meta) allowed discrimination in the targeting and delivery of ads for housing, credit services, and job openings based on race, sex, and age. The company was eventually forced to change its ad targeting system as part of a legal settlement,[6] but was still charged with engaging in race discrimination by the Department of Housing and Urban Development.[7] Similar practices have been the target of investigations, including at Twitter and Google.[8] In fact, Meta *literally* engages in redlining—it allows advertisers to select which zip codes to include or exclude from receiving an ad, and draws a red line on a map showing the excluded neighborhoods.[9] Academic research suggests that Facebook uses ad delivery algorithms that reproduce discrimination even when the advertiser did not intend to discriminate, including again in the housing, credit services, and employment contexts.[10]

In the job application and screening process, predictive artificial intelligence ("AI") tools can cement and reflect biases.[11] Amazon used a hiring algorithm for years that automatically penalized resumes for including the word "women's" and gave lower priority to applicants who had graduated from two all-women's colleges.[12]

Too often, a consumer's identify will determine which products they get offered. A Berkeley study found that biases in "algorithmic strategic pricing" have resulted in

---

[6] Barbara Ortutay, *Facebook to overhaul ad targeting to prevent discrimination*, ASSOCIATED PRESS, March 19, 2019, https://www.apnews.com/38c0dbd8acb14e3fbc7911ea18fafd58.

[7] Tracy Jan and Elizabeth Dwoskin, *HUD is reviewing Twitter's and Google's ad practices as part of housing discrimination probe*, WASH. POST, March 28, 2019, https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing-discrimination/.

[8] *Id.*

[9] "[Facebook] has provided a toggle button that enables advertisers to exclude men or women from seeing an ad, a search-box to exclude people who do not speak a specific language from seeing an ad, and a map tool to exclude people who live in a specified area from seeing an ad by drawing a red line around that area." Charge of Discrimination, *U.S. Dept. of Hous. and Urban Dev. v. Facebook, Inc.*, FHEO No. 01-18-0323-8 at 4 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf; Brief of *Amicus Curiae* Lawyers' Committee for Civil Rights Under Law in Support of Plaintiff's Opposition to Facebook's Demurrer to First Amended Complaint, *Liapes v. Facebook*, No. 30-CIV-01712, at 10 (Calif. Super. Ct. 2021), https://lawyerscommittee.org/wp-content/uploads/2021/03/Leave-and-Amicus-Combined.pdf.

[10] Louise Matsakis, *Facebook's Ad System Might be Hard-Coded for Discrimination*, WIRED, April 6, 2019, https://www.wired.com/story/facebooks-ad-system-discrimination/.

[11] Aaron Rieke and Miranda Bogen, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, UPTURN (2018), https://www.upturn.org/reports/2018/hiring-algorithms/.

[12] Jeffrey Dastin, *Amazon scraps secret AI recruiting tool that showed bias against women*, REUTERS, Oct. 9, 2018, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G.

Black and Latino borrowers paying higher interest rates on home purchase and refinance loans as compared to White and Asian borrowers. These pricing disparities are commonly driven by machine learning algorithms that target customers based on their personal data. The difference alone costs Black and Latino customers $250 million to $500 million every year.[13]

Retail websites have been found to charge different prices based on the demographics of the user.[14] For example, an online shopper's distance from a physical store, as well as distance from the store's competitors, has been used in algorithms setting online prices, resulting in price discrimination. Because of historical redlining and segregation, and the lack of retail options in many low-income neighborhoods, this resulted in low-income communities of color paying higher prices than wealthier, whiter neighborhoods when they shopped online.

Communities of color are targeted by predatory and low-quality for-profit online colleges.[15] Ashford University, a for-profit, mostly online University, deliberately sought to place their ads in front of Black, Latino, low-income students who are first in their family to attend college.[16] This targeting is as successful as it is predatory. Black and Latino students are overrepresented at Ashford as well as at other for-profit schools generally.[17] Once these students attend for-profit Universities online, they are trapped with higher levels of debt and loan defaults than students at public, non-profit schools. Roughly 70% of Black Americans who borrow money to attend Ashford or other for-profit colleges end up defaulting on that loan within ten years.[18]

Consumer financial discrimination is also common online. Google's search engine previously served ads for payday loans when a user ran searches for terms associated with financial distress such as, "I need money to pay my rent."[19]

---

[13] Laura Counts, *Minority homebuyers face widespread statistical lending discrimination, study finds*, HAAS SCHOOL OF BUSINESS AT THE UNIVERSITY OF CALIFORNIA, BERKELEY (Nov. 13, 2018). http://newsroom.haas.berkeley.edu/minority-homebuyers-face-widespread-statistical-lending-discrimination-study-finds/.

[14] Jennifer Valentino-DeVries et al, *Websites Vary Prices, Deals Based on Users' Information*, WALL ST. J., Dec. 24, 2012, https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

[15] *See* Genevieve Bonadies et al, *For-Profit Schools' Predatory Practices and Students of Color: A Mission to Enroll Rather than Educate*, HARVARD L. REV. BLOG (July 30, 2018) https://blog.harvardlawreview.org/for-profit-schools-predatory-practices-and-students-of-color-a-mission-to-enroll-rather-than-educate/; Larry Abramson, *For-Profit Schools Under Fire For Targeting Veterans*, NPR, Apr. 9, 2012, https://www.npr.org/2012/04/09/150148966/for-profit-schools-under-fire-for-targeting-veterans.

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] Aaron Rieke and Logan Koepke, *Led Astray: Online Lead Generation and Payday Loans*, UPTURN (2015), https://www.upturn.org/reports/2015/led-astray/.

Algorithms that set car insurance rates charge communities of color higher premiums than predominantly White neighborhoods with the same risk levels.[20]

The common denominator in all of these examples is sloppy or abusive use of personal data. By prohibiting discriminatory data use and requiring companies to test their algorithms for bias, many of these harms can be prevented.

III. The American Data Privacy and Protection Act

The "American Data Privacy and Protection Act" would establish a national data privacy and data security framework. We are pleased to see that it prioritizes civil rights protections that address data-driven discrimination. The draft legislation is the first major comprehensive privacy proposal to gain bipartisan and bicameral support. We are encouraged by the progress of this legislation, and want to address this Committee on four important pieces of the legislation: the civil rights protections included, the importance of the bill's data minimization standards, how transparency empowers individuals, and the critical need for a more robust and effective private right of action.

A. Welcomed and Needed Civil Rights Protections

The time has come to enact a comprehensive consumer privacy law that safeguards civil rights online. We are encouraged by the strong civil rights section of the American Data Privacy and Protection Act especially the language that seeks to change the status quo for Americans harmed by discriminatory algorithms, advertising, and retail discrimination. Existing civil rights laws do not cover the entirety of the discriminatory harms people routinely experience online.

We welcome the civil rights provisions of the "American Data Privacy and Protection Act" that will prohibit many common forms of online discrimination. The bill prohibits using personal data to discriminate based on protected characteristics. This would prohibit targeting or delivering ads based on protected characteristics, such as race, sex, or religion. It would also apply to discriminatory algorithms and technologies that use them, such as commercial use of a biased facial recognition system.[21] The bill allows companies to process protected class data for the purpose of self-testing to root out discrimination, as well as to diversify a pool of applicants, candidates, or customers. The anti-discrimination provision would also preserve

---

[20] Julia Angwin et al, *Minority Neighborhoods Pay Higher Car Insurance Premiums Than White Areas With the Same Risk*, PROPUBLICA, April 5, 2017, https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk; Sarah Jeong, *A.I. Is Changing Insurance*, NEW YORK TIMES, April 10, 2019, https://www.nytimes.com/2019/04/10/opinion/insurance-ai.html.

[21] Kashmir Hill, *Flawed Facial Recognition Leads To Arrest and Jail for New Jersey Man*, NEW YORK TIMES, December 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

free speech; it does not apply to non-commercial activities or to private clubs or groups, which are the same exceptions in the Civil Rights Act of 1964.

In addition, the bill requires impact assessments for the algorithms employed by companies, as well as pre-deployment algorithmic design evaluations. We have seen algorithms reproduce patterns of discrimination in employment recruiting, housing, education, finance, mortgage lending, credit scoring, healthcare, vacation rentals, ridesharing, and other services.[22] The bill requires the assessments to test for discrimination in these types of economic opportunities, as well as to explicitly test for disparate impacts on the basis of protected characteristics. We hope that these assessments will help companies identify biases and problems in their algorithms before they are implemented and cause harm.

The civil rights provision in the bill will also apply to social media platforms. These protections should help increase fairness in recommendation algorithms that have been shown to disadvantage creators and influencers of color.[23] These provisions are critical in addressing civil rights online. We are encouraged by the digital access rights and transparency requirements that will help identify discriminatory practices, and we urge this Committee to include strong civil rights protections in legislation going forward.

B. Important Data Minimization Standards

Pervasive access to peoples' personal data, often obtained without the knowledge or consent of the individual, can lead to discriminatory, predatory and unsafe practices. Companies should not collect or use more personal info than is necessary to do what the individual expects them to do. Beyond basic cybersecurity and legal obligations, companies also should not use personal data for secondary purposes that an individual does not expect, or has not consented to. The reason is simple: personal data collected by companies can proliferate in a way that maximizes risk for the individual and for society at-large. Clear baseline protections for data collection, including both primary and secondary uses of data, should be enacted to help cage risk, and prevent harms.

Fraud and identity theft disproportionately harm Black and Brown communities. This Act reduces the amount of data that will fall into the wrong hands and be used illicitly for fraud and identity theft. Data breaches are often

---

[22] Civil Rights, Civil Liberties, and Consumer Protection Organizations Letter to the FTC, August 4, 2021, https://www.lawyerscommittee.org/wp-content/uploads/2021/08/FTC-civil-rights-and-privacy-letter-Final-1.pdf.

[23] Reed Albergotti, *Black Creators Sue YouTube, Alleging Racial Discrimination,* WASH. POST, June 18, 2020, https://www.washingtonpost.com/technology/2020/06/18/black-creators-sue-youtube-alleged-race-discrimination/; *Twitter finds racial bias in image-cropping AI,* BBC, May 20, 2021, https://www.bbc.com/news/technology-57192898.

especially problematic for people of color living on fixed or low incomes.[24] Companies track cell phone location data without consent and sell this data to debt collectors and other predatory actors, which disproportionately harms low income Black and Brown communities.[25] This bill's data minimization requirements will restrict data collection and use to purposes necessary for providing services expected by an individual and restricts secondary uses or data sharing without explicit opt-in consent.

Personal data are the fuel of online commerce. They can be used for good—to create new products, conduct beneficial research, mitigate disparities, or tailor experiences that consumers want. They can also be abused—to steal someone's identity, exclude someone from opportunities, target someone for harassment or abuse, engage in predatory practices and scams, or to reinforce the legacies of segregation and redlining.

Keeping data collection, use, and sharing limited to what is reasonably necessary and proportionate to provide expected services is essential to keeping consumers safe. Just like combustible fuel, an overflowing or leaking data ecosystem is a dangerous situation.

We are encouraged that the Act imposes a baseline duty on all covered entities to collect or use covered data only as needed and appropriate, and is not a "notice and consent" regime in which any practice is allowed so long as a consumer consents after being presented with lengthy and legalistic privacy notices. Such data minimization efforts can reduce risks of abuse and harm from data breaches. In contrast, notice and consent has repeatedly been shown to be a failure. Just as we do not expect consumers to understand how every aspect of their car engine works, we likewise should not expect them to understand how the online data ecosystem works. With a car, consumers expect that when we drive it off the lot it will be safe and function correctly, and that if it does not they will have recourse. Consumers should expect no less from digital products either.

C. *How Transparency Empowers Individuals*

Transparency about how companies collect and use data will ultimately shed light on discriminatory practices. Providing individuals with understandable, easy to read, privacy policies detailing data collection puts the individual in the driver's seat. This transparency, coupled with giving users the ability to access, correct, or

---

[24] Kori Hale, *T-Mobile's hack of 50 million users leaves black community at risk*, FORBES, September 9, 2021, https://www.forbes.com/sites/korihale/2021/09/10/t-mobiles-hack-of-50-million-users-leaves-black-community-at-risk/?sh=48fc391b7435.

[25] Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, VICE NEWS, January 8, 2019, https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

delete their data, lets individuals make empowered choices. They can choose to access and correct their data, opening pathways to self-sufficient fixes for inaccurate background check reports, which disproportionately harm Black and Brown Americans.[26] Giving individuals the power to delete their data empowers them to protect themselves. They can reduce their data footprint, or take away their data from insecure third parties, minimizing the risk of fraud, identify theft, and exploitation.

Currently, data brokers continually collect and amass data for sale. Some may not be accurate. This data is then used to conduct background checks for employment, housing, and other services, as well as for credit scoring. Inaccuracies disproportionately harm people of color, as well as those who have a conviction or arrest record. This bill rectifies that harm by creating a data broker registry, reporting requirements and a national opt-out registry. In addition, the bill requires businesses—including data brokers—to minimize the data they collect, restricts selling such data to third parties without consent, and provides individuals with a right to access, correct, or delete their data.

D. Need for a More Robust Private Right of Action

As encouraged as we are about some provisions of this Act, we know that data privacy legislation will only live up to its promise if it is able to be readily enforced. As currently written, the "American Data Privacy and Protection Act" has reasonably good enforcement mechanisms for the Federal Trade Commission and State attorneys general, but a narrow and limited private right of action for individuals. We have concerns that without a stronger private right of action, it will be difficult for individuals to vindicate their own rights and address the harms we have documented.

The best way for an individual to safeguard their rights is to be able to seek a remedy to the injury they suffer themselves, in a court of law. As currently written, the private right of action in the Act is weak and difficult to enforce. The private right of action will not come into force until four years after the Act becomes effective. Despite the real and pervasive harms rampant on the internet, real people will be asked to wait years to have wrongs against them addressed, while faceless and anonymous entities causing harm can continue to flourish. Once a private individual is allowed to bring suit, they are still limited in the remedies they can seek. Under the current language of the Act, remedies are limited to compensatory

---

[26] Christina Stacy & Mychal Cohen, Urban Inst., *Ban the Box and Racial Discrimination: A Review of the Evidence and Policy Recommendations*, 17 (2017), https://www.urban.org/sites/default/files/publication/88366/ban_the_box_and_racial_discrimination_4.pdf (finding that inaccuracies in criminal record data especially harm people of color, because they represent a disproportionate share of U.S. arrests and are thus more likely to have missing information regarding the outcome of a case).

damages, injunctive and declaratory relief, and attorney's fees and costs. There is no provision for punitive or statutory damages, which have served as an effective deterrent for especially harmful actors under other legal regimes—not even nominal damages are allowed.

In addition, there are numerous procedural pitfalls designed to trip up individuals on their way to the courthouse, some of which may be unconstitutional violations of free speech or due process. First, the bill bars *anyone* from making *any* request for money to a covered entity until certain narrow conditions are met—and those conditions may never occur.[27] Besides being an unconstitutional prior restraint on speech, this would cause huge unintended consequences—consumers could not request refunds and businesses would be unable to invoice each other. It would effectively shut down interstate commerce if a court loyally applied the plain meaning of the text. It would also severely jeopardize the ability to recover compensatory damages. Moreover, it would impede the ability of businesses to settle disputes without having to engage in more costly litigation. If the goal of this provision is to deter the trial bar, that will also fail as smart attorneys can easily circumvent it.

Second, the bill includes an onerous "right to cure" that does nothing that is not already accomplished by existing civil procedure and standing rules—other than impose new hurdles to get to court.[28] It ostensibly gives covered entities a window to cure an injury before an individual could bring a case seeking injunctive relief. However, Article III standing and equitable relief jurisprudence *already* provide this offramp: a defendant can always cease an ongoing harmful practice and if there is no risk of recurrence, then claims for injunctive relief are moot and get dismissed. All this new provision does is risk creating new substantive hurdles to otherwise meritorious cases—it will increase litigation costs while providing no benefit.

Third, the bill plays "gotcha" games designed to trick everyday consumers into forfeiting their rights. A "demand letter" provision requires that an individual must use a specific sentence—magic words—in their *first* communication to a covered entity asserting a violation of their rights.[29] If the individual fails to do so, they forfeit their rights. What average consumer is going to know to do this when contacting customer support to dispute an issue and try to assert their rights? Consumers may forfeit their rights without ever knowing, and the covered entity will be free to continue its unlawful practices. In addition, this provision appears to be a substantive due process violation: the provision says that one individual's failure can cause an entire class of individuals to forfeit their rights.

---

[27] *See* Sec. 403(a)(3)(B) of the bill, titled "Bad Faith."
[28] *See* Sec. 403(c) of the bill.
[29] *See* Sec. 403(d) of the bill.

Finally, the private right of action does not apply to the data minimization section of the bill, which is the core protection for consumers. This means individuals will not be able to sue when a company fails to comply with their most basic requirement to only process personal data in a manner that is necessary and proportionate.

We support removing the barriers in the private right of action as the clearest way to ensure that the promises made elsewhere in this bill materialize for all who access the digital world.

IV. Conclusion

The "American Data Privacy and Protection Act" is a promising piece of legislation aimed at solving long lingering critical problems. We appreciate this Committee's attention to the issue and the opportunity to testify on how to strengthen privacy protections for individuals and curb data-driven discrimination. The Lawyers' Committee looks forward to working on a bipartisan bias to advance this legislation over the finish line, ultimately securing long overdue data privacy and online civil rights protections for all Americans, particularly people of color who are most often targeted for harm in the digital world.