LAWYERS' COMMITTEE FOR CIVIL RIGHTS UNDER LAW

1500 K Street, NW
Suite 900
Washington, DC 20005

Tel: 202.662.8600
Fax: 202.783.0857
www.lawyerscommittee.org

April 7, 2025

The Honorable Brett Guthrie
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable John Joyce
Vice Chairman
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Guthrie and Vice Chairman Joyce:

The Lawyers' Committee for Civil Rights Under Law ("Lawyers' Committee") writes to provide the comments below in response to the House Committee on Energy & Commerce Privacy Working Group's Request for Information on the parameters of a federal comprehensive data privacy and security framework. The Lawyers' Committee is a national, nonprofit civil rights legal organization that was founded in 1963 at the request of President John F. Kennedy to mobilize the nation's leading lawyers as agents for change in the Civil Rights Movement. 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 the voice, opportunity, and power to make the promises of our democracy real. Our Digital Justice Initiative and Policy Project work 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.

Privacy legislation is fundamentally a civil rights issue, as privacy protections can help ensure that people's identities and characteristics cannot unfairly be used against them. Robust privacy legislation can secure for everyone the "inviolability of privacy" that is "indispensable to preservation of freedom of association."[1] Clear data privacy and security standards can help industry understand and meet expectations, ensuring that technological progress helps people and does not come at the expense of their rights.

The Lawyers' Committee appreciates the opportunity to comment on the appropriate parameters for a federal comprehensive data privacy and security framework. We believe that successful legislation should accomplish the following:

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

- Prohibit using personal data to discriminate on the basis of protected characteristics.
- Ensure that automated decision-making systems are tested for bias and other risks, especially in matters concerning housing, employment, education, credit, and public accommodations.
- Require companies to minimize the data they collect and give clarity on permissible and impermissible data uses.
- Create transparency mechanisms that are helpful to consumers and enable robust oversight, research, language accessibility, and accountability
- Provide consumers with the right to access, correct, and delete their personal data.
- Regulate the data broker industry.
- Empower enforcement by the Federal Trade Commission and state attorneys general and include a private right of action.
- Not preempt state laws, including those concerning privacy, cybersecurity, AI, consumer protection, and civil rights.

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

Robust privacy protections can empower communities of color and open doors for marginalized populations. It can also provide clarity for 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 how 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.[2] 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.[3] And it is wholly unclear how existing laws apply 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 services 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-

[2] *See* 42 U.S.C. §§ 1981, 2000a; *Shaare Tefila Cong. v. Cobb*, 481 U.S. 615 (1987).
[3] Aaron Rieke & Miranda Bogen, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, UPTURN (Dec. 10, 2018), https://www.upturn.org/reports/2018/hiring-algorithms/.

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. Consumers of color continue to suffer the consequences of unequal access to goods and services due to discriminatory algorithms and exploitative data practices.

In advertising, for example, Facebook (now known as Meta) allowed targeted ad delivery 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,[4] but was still charged with engaging in race discrimination by the Department of Housing and Urban Development.[5] Similar practices have been the target of investigations, including at Twitter and Google.[6]

In the job application and screening process, predictive AI tools have been found to make biased, adverse decisions in some cases.[7] 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.[8]

Too often, a consumer's identity will determine which products they get offered. A Berkeley study found that biases in "algorithmic strategic pricing" have resulted in Black and Latino borrowers paying higher interest rates on home purchase and refinance loans as compared to White and Asian borrowers.[9] 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.[10]

---

[4] Barbara Ortutay, *Facebook to overhaul ad targeting to prevent discrimination*, ASSOC. PRESS (Mar. 19, 2019), https://www.apnews.com/38c0dbd8acb14e3fbc7911ea18fafd58.
[5] Tracy Jan & Elizabeth Dwoskin, *HUD is reviewing Twitter's and Google's ad practices as part of housing discrimination probe*, WASH. POST (Mar. 28, 2019), https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing discrimination/.
[6] *Id.*
[7] Aaron Rieke & Miranda Bogen, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, UPTURN (Dec. 10, 2018), https://www.upturn.org/reports/2018/hiring-algorithms/.
[8] 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.
[9] Laura Counts, *Minority homebuyers face widespread statistical lending discrimination, study finds*, HAAS SCH. OF BUS., UNIV. OF CAL., BERKELEY (Nov. 13, 2018). https://newsroom.haas.berkeley.edu/minority-homebuyers-face-widespread-statistical-lending-discrimination-study-finds/.
[10] *Id.*

Retail websites have been found to charge different prices based on the demographics of the user.[11] 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.[12]

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."[13] Algorithms that set car insurance rates charge communities of color higher premiums than predominantly White neighborhoods with the same risk levels.[14] 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.

II. Civil Rights Provisions are Crucial to Safeguard Communities of Color Online.

To this end, any comprehensive privacy bill should include anti-discrimination language that prohibits using personal information 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.[15] Past federal privacy bills like the American Data Privacy and Protection Act ("ADPPA") have included an anti-discrimination section that would allow 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 ADPPA civil rights provision also preserves 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.

Testing algorithms is a key component of protecting civil rights online. Therefore, any privacy legislation should require algorithmic bias audits or impact assessments, in conjunction with state-level AI frameworks. We have seen algorithms reproduce patterns of discrimination in

---

[11] 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.
[12] *Id.*
[13] Aaron Rieke & Logan Koepke, *Led Astray: Online Lead Generation and Payday Loans*, UPTURN (Oct. 1, 2015), https://www.upturn.org/reports/2015/led-astray/.
[14] Julia Angwin et al., *Minority Neighborhoods Pay Higher Car Insurance Premiums Than White Areas With the Same Risk*, PROPUBLICA (Apr. 5, 2017), https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk; Sarah Jeong, *A.I. Is Changing Insurance*, N.Y. TIMES (Apr. 10, 2019), https://www.nytimes.com/2019/04/10/opinion/insurance-ai.html.
[15] Kashmir Hill, *Flawed Facial Recognition Leads To Arrest and Jail for New Jersey Man*, N.Y. TIMES (Dec. 29, 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition misidentify-jail.html.

employment recruiting, housing, education, finance, mortgage lending, credit scoring, healthcare, vacation rentals, ridesharing, and other services.[16] Any audits or assessments should test discrimination in these types of economic opportunities, as well as explicitly test for disparate impacts on the basis of protected characteristics. We expect that these assessments will help companies identify biases and problems in their algorithms before they are implemented and cause harm. For example, as applied to social media platforms, these protections should help increase fairness in recommendation algorithms that have been shown to disadvantage creators and influencers of color.[17]

III. Additional Consumer Protections are Needed to Protect Communities of Color Online.

Data minimization, transparency, and consumer rights are core consumer protections that are particularly important for communities of color.

a. Data Minimization

Pervasive access to people's 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 information 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 a person would not expect, or to which the person has not consented. 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.

Fraud and identity theft disproportionately harm Black and Brown communities. Data breaches are often especially problematic for people of color living on fixed or low incomes.[18] 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.[19] Data minimization reduces the amount of data that can fall into the wrong hands and be misused for fraud and identity theft.

---

[16] Civil Rights, Civil Liberties, and Consumer Protection Organizations Letter to the FTC (Aug. 4, 2021), https://www.lawyerscommittee.org/wp-content/uploads/2021/08/FTC-civil-rights-and-privacy-letter-Final-1.pdf.
[17] 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.
[18] Kori Hale, *T-Mobile's hack of 50 million users leaves black community at risk*, FORBES (Sept. 9, 2021), https://www.forbes.com/sites/korihale/2021/09/10/t-mobiles-hack-of-50-million-users-leaves-black-community-at-risk/.
[19] Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone,* VICE NEWS (Jan. 8, 2019), https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

Data brokers continually compile personal data and make it available for sale. This data is then used to conduct background checks for employment, housing, and other services, as well as for credit scoring. Inaccuracies in such data disproportionately harm people of color, as well as those who have a conviction or arrest record.[20] Moreover, data brokers often do little to prevent the misuse of the data sold.[21]

Keeping data collection, use, and sharing limited to what is reasonably necessary and proportionate to provide expected services is essential to keeping consumers safe. Therefore, any comprehensive privacy legislation should impose a baseline duty to collect or use covered data only as needed and appropriate, rather than a "notice and consent" regime in which any practice is allowed so long as a consumer consents after being presented with a lengthy and legalistic privacy notice. The "notice and consent" model has repeatedly been shown to be a failure, especially when it comes to the purchase and sale of information by data brokers. 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, a consumer expects that when they drive it off the lot, it will be safe and function correctly, and if it does not, they will have recourse. Consumers should expect no less from digital products.

b. Transparency and Consumer Rights

Transparency about how companies collect and use data will ultimately shed light on discriminatory practices. Providing individuals with understandable and 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 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.[22] Giving individuals the power to delete their data empowers them to protect

---

[20] *See* Kaveh Waddell, *How Tenant Screening Reports Make It Hard for People to Bounce Back From Tough Times*, CONSUMER REPS. (Mar. 11, 2021), https://www.consumerreports.org/algorithmic-bias/tenant-screening-reports-make-it-hard-to-bounce-back-from-tough-times-a2331058426/; Kristian Lum & William Isaac, *To predict and serve?*, 13 SIGNIFICANCE 14, 15–16 (2016), https://rss.onlinelibrary.wiley.com/doi/pdf/10.1111/j.1740-9713.2016.00960.x (discussing racial bias in predictive policing systems trained on arrest records).

[21] *See* First Amended Class Action Complaint at 9–11, *Brooks v. Thomson Reuters*, Corp., No. 3:21-cv-01418-EMC-KAW (N.D. Cal. Dec. 2, 2022), ECF No. 145; *See* Complaint for Damages, Declaratory, and Injunctive Relief at 4–7*, Ramirez v. LexisNexis Risk Sols.*, No. 2022CH07984 (Ill. Cir. Ct. Aug. 16, 2022), https://legalactionchicago.org/wp-content/uploads/2022/08/Castellanos-et-al.-v.-LexisNexis-Risk-Solutions-Complaint-For-Filing.pdf, *removed to federal court*, No. 1:22-cv-05384 (N.D. Ill. Sept. 30, 2022).

[22] Christina Stacy & Mychal Cohen, *Ban the Box and Racial Discrimination: A Review of the Evidence and Policy Recommendations*, URB. INST. 17 (Feb. 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).

themselves. They can reduce their data footprint, or delete their data from insecure companies, minimizing the risk of fraud, identity theft, and exploitation.

IV. We Need Strong Enforcement Mechanisms and to Ensure States Can Enact Even Stronger Privacy and Civil Rights Protections.

Any data privacy legislation can only live up to its promise if it is easily enforced. Therefore, it is crucial to have strong enforcement mechanisms for the Federal Trade Commission, which should operate at full capacity insulated from political whims, as well as state attorneys general. In addition, any privacy bill should include a private right of action to allow consumers 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 for the injury they suffer themselves, in a court of law. There should be no unnecessary procedural hurdles. Nor should there be a "right to cure" provision. Furthermore, both government enforcers and individuals should be able to seek a full range of remedies including injunctive and declaratory relief; attorneys' fees; and compensatory, punitive, and statutory damages.

Finally, states have led the way in protecting people, especially communities of color, on data privacy and security, and now on AI issues. We must enable states to continue to enact and enforce privacy, security, and AI laws in addition to traditional consumer protection and civil rights laws. Thus, any preemption language must be limited to floor preemption, where federal privacy legislation establishes baseline nationwide protections and allows states to provide further protections for their residents.

***

The Lawyers' Committee appreciates the opportunity to provide comments on this issue. We urge the Privacy Working Group to include robust civil rights protections in any comprehensive privacy legislation and ensure that arguments about technological progress are not used to diminish privacy and civil rights protections. If you or your staff have any questions or would like to discuss further, please contact Jina John at jjohn@lawyerscommittee.org.

Sincerely,

Jina John
Policy Counsel
Lawyers' Committee for Civil Rights Under Law