April 19, 2019

The Honorable Roger Wicker
Chairman
Senate Committee on Commerce, Science, & Transportation

The Honorable Maria Cantwell
Ranking Member
Senate Committee on Commerce, Science, & Transportation

The Honorable Frank Pallone, Jr
Chairman
House Committee on Energy & Commerce

The Honorable Greg Walden
Ranking Member
House Committee on Energy & Commerce

Chairman Wicker, Chairman Pallone, Ranking Member Cantwell, Ranking Member Walden, and Members of the House and Senate Commerce Committees:

We, the undersigned members of the civil rights, civil liberties, and consumer protection communities, write to emphasize the importance of addressing data-driven discrimination and equal opportunity in comprehensive consumer privacy legislation. Fundamentally, the right to privacy exists to, among other things, protect against unfair and inappropriate uses of personal information. Any legislation addressing data practices must recognize and address how the exploitation of personal information can disproportionately harm marginalized communities, including by enabling discrimination—intentionally or unintentionally—against people of color, women, religious minorities, members of the LGBTQ+ community, persons with disabilities, persons living on low income, and immigrants.

Personal data are the raw materials that fuel discrimination. Commercial data practices that process massive quantities of personal data enable and facilitate discrimination on a systematic scale. Exploitation of personal information can cause myriad harms to marginalized communities, including:

- **Voter Suppression**: As shown by Russian 2016 election interference efforts that deliberately targeted African Americans, personal information can be weaponized to deceive and disenfranchise voters.[i]
- **Digital Redlining**: Using personal information to profile individuals enables discrimination and predatory marketing in employment,[ii] housing,[iii] credit,[iv] education,[v] and insurance[vi] opportunities.
- **Discriminatory Policing**: Commercial databases can be accessed by government surveillance programs and law enforcement agencies, often without a warrant or due process protections, and used in a discriminatory manner.[vii] These data are often used to target civil rights activists.[viii]
- **Retail Discrimination**: Companies can use a person's location and behavioral data to discriminate in the prices, terms, or discounts they offer in their online

stores, such as charging higher prices for low-income neighborhoods.[ix] Brick-and-mortar stores may also use facial recognition to surveil shoppers,[x] despite its well established racial and gender biases.[xi]

- **Exacerbation of Digital Inequity**: There is a gap between technology haves and have-nots. Companies widen this gap when they engage in data practices that exploit those who lack tech literacy or limit protections for those who can't afford to pay for privacy enhancements.[xii]
- **Amplification of White Supremacy**: The algorithms of social media companies use personal data to maximize user engagement at all costs, including by recommending extreme content such as fringe conspiracy theories and white supremacy.[xiii]
- **Identity Theft**: Low income families with fewer resources are more vulnerable to financial harms from identity theft. Even a small disruption to personal credit could be devastating to a family that is already struggling to make ends meet.[xiv]
- **Endangering Personal Safety**: Careless data practices by tech companies can expose vulnerable populations to threats to physical safety. They can non-consensually reveal someone's sexual orientation or gender identity,[xv] allow domestic abusers to track their victims,[xvi] and expose sensitive personal secrets.[xvii]

These harms occur primarily in three ways. Either a company who holds the personal information uses it to directly discriminate against marginalized communities; a company who holds the personal information makes it available to other actors who use it to discriminate against marginalized communities; or a company designs its data processing practices in a manner that unintentionally causes discriminatory results. But the bottom line is that if major tech companies and data brokers were not collecting, aggregating, and using vast quantities of personal information in privacy-invasive ways, many of these harms would not happen or would be far more difficult to perpetrate.

Comprehensive data practices legislation must prioritize and directly address the civil rights impacts from the exploitation of personal information. As Congress considers its legislative options, it should include provisions that:

1) Prohibit the use of personal data to discriminate in employment, housing, credit, education, or insurance—either directly or by disparate impact.
2) Prohibit the use of personal data to discriminate in public accommodations and extend such protections to businesses that offer goods or services online.
3) Prohibit the use of personal data to engage in deceptive voter suppression.
4) Require companies to audit their data processing practices for bias and privacy risks.
5) Require robust transparency at two tiers: easy-to-understand privacy notices for consumers, and comprehensive annual privacy reports for researchers and regulators. Companies must completely disclose how they collect and use personal data, including their algorithmic processing practices.

6) Enable researchers to independently test and audit platforms for discrimination.
7) Empower a federal agency with rulemaking authority, enforcement powers, and enough resources to address current and future discriminatory practices.
8) Provide individual rights to access, correct, and delete one's personal data and inferences made using that data.
9) Provide a private right of action. **Marginalized communities historically have not been able to rely upon the government to protect their interests, so individuals need to be able to vindicate their own rights.**
10) Establish baseline nationwide protections and allow states to enact stricter laws. **Under no circumstances should Congress enact any legislation that could preempt state civil rights laws, many of which are stronger than federal law.** For example, many states extend greater anti-discrimination protections to the LGBTQ+ community than federal law.

As Congress debates consumer privacy proposals, we look forward to continuing to work with you to ensure that legislation to rein in commercial data practices addresses the real-world harms caused by the misuse of personal information. For too long, corporations have ignored the digital pollution that their commercial data practices generate; they must be held accountable for the negative externalities of their business models. Comprehensive privacy reform is necessary to empower consumers, protect against discrimination, and promote equal opportunity for all in the modern public square and marketplace.

Sincerely,

Access Now
Center for Digital Democracy
Center for Media Justice
Center on Privacy & Technology at Georgetown Law
Color of Change
Common Cause
Consumer Action
Consumer Federation of America
Demand Progress Education Fund
Demos
Free Press Action
Human Rights Campaign
Impact Fund
Lawyers' Committee for Civil Rights Under Law
Maryland Consumer Rights Coalition
National Consumer Law Center, on behalf of its low-income clients
National Hispanic Media Coalition
National Urban League
New America's Open Technology Institute
Open MIC (Open Media and Information Companies Initiative)
Public Citizen
Public Justice Center
Public Knowledge
Southern Poverty Law Center
The Leadership Conference on Civil and Human Rights
United Church of Christ, OC Inc.

[i] Scott Shane & Sheera Frenkel, *Russian 2016 Influence Operation Targeted African-Americans on Social Media*, N.Y. Times (Dec. 17, 2018), https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html. *See also, e.g.,* Scott Detrow, *What Did Cambridge Analytica Do During The 2016 Election?*, NPR (March 20, 2018), https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election.

[ii] *See, e.g.*, Barbara Ortutay, *Facebook to overhaul ad targeting to prevent discrimination*, Associated Press (March 19, 2019), https://www.apnews.com/38c0dbd8acb14e3fbc7911ea18fafd58; 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/ (discussing new academic research showing that the platform's ad delivery algorithm engaged in discrimination even when an ad is neutrally targeted); 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; Upturn, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias* (Dec. 2018), https://www.upturn.org/reports/2018/hiring-algorithms/ ("Predictive hiring tools can reflect institutional and systemic biases, and removing sensitive characteristics is not a solution."); Drew Harwell, *Is your pregnancy app sharing your intimate data with your boss?*, Wash. Post (April 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think.

[iii] *See, e.g.*, 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/ (reporting that HUD filed a lawsuit against Facebook as well); A recent 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. This difference costs them $250 million to $500 million every year. 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/.

[iv] Google's search engine used to serve users ads for payday loans when they ran searches for terms associated with financial distress, such as "I need money to pay my rent." Upturn, *Led Astray: Online Lead Generation and Payday Loans*, (Oct. 2015), https://www.upturn.org/reports/2015/led-astray/.

[v] *See, e.g.*¸ Genevieve (Genzie) Bonadies et al, *For-Profit Schools' Predatory Practices and Students of Color: A Mission to Enroll Rather than Educate*, Harvard Law Review 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.

[vi] *See, e.g.*, Marshall Allen, *Health Insurers Are Vacuuming Up Details About You—And It Could Raise Your Rates*, ProPublica (July 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates ("God forbid you live on the wrong street these days," a health data vendor said. "You're going to get lumped in with a lot of bad things."); 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*, N.Y. Times (April 10, 2019), https://www.nytimes.com/2019/04/10/opinion/insurance-ai.html.

[vii] *See, e.g.*, Eli Rosenberg, *Motel 6 will pay $12 million to guests whose personal data was shared with ICE*, Wash. Post (April 6, 2019), https://www.washingtonpost.com/nation/2019/04/06/motel-leaked-personal-data-guests-ice-officials-say-now-it-owes-them-million/; Kristen V. Brown, *Major DNA Testing Company Sharing Genetic Data With the FBI*, Bloomberg News (Feb. 1, 2019),

https://www.bloomberg.com/news/articles/2019-02-01/major-dna-testing-company-is-sharing-genetic-data-with-the-fbi; Caroline Haskins, *Amazon's Home Security Company Is Turning Everyone Into Cops*, Motherboard (Feb. 7, 2019), https://motherboard.vice.com/en_us/article/qvyvzd/amazons-home-security-company-is-turning-everyone-into-cops ("neighborhood watch" app disproportionately reported people of color and its forums were rife with racism).

[viii] *See, e.g.*, Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU of Northern California (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

[ix] *See, e.g.*, Jennifer Valentino-DeVries et al, *Websites Vary Prices, Deals Based on Users' Information*, WSJ (Dec. 24, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

[x] *See, e.g.*, Leticia Miranda, *Thousands of Stores Will Soon Use Facial Recognition, And They Won't Need Your Consent*, Buzzfeed News (Aug. 17, 2018), https://www.buzzfeednews.com/article/leticiamiranda/retail-companies-are-testing-out-facial-recognition-at; Annie Lin, *Facial recognition is tracking customers as they shop in stores, tech company says*, CNBC (Nov. 23, 2017), https://www.cnbc.com/2017/11/23/facial-recognition-is-tracking-customers-as-they-shop-in-stores-tech-company-says.html ("Facial recognition technology is used to identify a customer's gender, age and ethnicity"); Lara O'Reilly, *Walgreens Tests Digital Cooler Doors With Cameras to Target You With Ads*, WSJ (Jan. 11, 2019), https://www.wsj.com/articles/walgreens-tests-digital-cooler-doors-with-cameras-to-target-you-with-ads-11547206200.

[xi] Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. of Machine Learning Research 1 (2018), *available at* http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf (finding that facial recognition datasets are overwhelmingly populated by lighter skinned subjects, and that while facial recognition error rates are 0.8% for light-skinned males, they are up to 34.7% for dark-skinned females). *See also* Joy Buolamwini, *When the Robot Doesn't See Dark Skin*, N.Y. Times (June 21, 2018), https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html.

[xii] Amanda Hess, *How Privacy Became a Commodity for the Rich and Powerful*, N.Y. Times (May 9, 2017), https://www.nytimes.com/2017/05/09/magazine/how-privacy-became-a-commodity-for-the-rich-and-powerful.html. *See also* S. Derek Turner, *Digital Denied: The Impact of Systemic Racial Discrimination on Home-Internet Adoption*, Free Press (Dec. 2016), https://www.freepress.net/sites/default/files/legacy-policy/digital_denied_free_press_report_december_2016.pdf.

[xiii] *See, e.g.,* Rebecca Lewis, *Alternative Influence: Broadcasting the Reactionary Right on YouTube*, Data & Society (Sept. 18, 2018), https://datasociety.net/output/alternative-influence/ (discussing how YouTube and its recommendation engine incentivize and amplify white nationalist creators and influencers); Caroline O'Donovan et al, *We Followed YouTube's Recommendation Algorithm Down the Rabbit Hole*, Buzzfeed News (Jan. 24, 2019), https://www.buzzfeednews.com/article/carolineodonovan/down-youtubes-recommendation-rabbithole (discussing how regular news videos are often followed by recommendations for hate group, misogynist, or conspiracy theory videos).

[xiv] Sarah Dranoff, *Identity Theft: A Low-Income Issue*, Am. Bar Ass'n (Dec. 15, 2014), https://www.americanbar.org/groups/legal_services/publications/dialogue/volume/17/winter-2014/identity-theft--a-lowincome-issue/.

[xv] The popular LGBTQ+ dating app Grindr disclosed its users' HIV status, GPS location data, email addresses, and other profile information to third parties. Alison Bateman-House, *Why Grindr's Privacy Breach Matters to Everyone*, Forbes (Apr. 10, 2018), https://www.forbes.com/sites/alisonbatemanhouse/2018/04/10/why-grindrs-privacy-breach-matters-to-

everyone/#51ada44a67f4 ("In much of the world, public knowledge of an HIV diagnosis or LGBTQ+ identity can be highly stigmatizing and often leads to discrimination, or even violence."); Geoffrey A. Fowler, *When the Most Personal Secrets Get Outed on Facebook*, WSJ (Oct. 13, 2012), https://www.wsj.com/articles/SB10000872396390444165804578008740578200224 (discussing personal accounts of LGBTQ+ identities being involuntarily revealed to family members).

[xvi] Tracey Lindeman, *Connected Car Technology Can Enable Abusers to Track Their Victims*, Motherboard (Aug. 14, 2018), https://motherboard.vice.com/en_us/article/gy3kw7/internet-connected-car-technology-can-enable-abusers-to-track-victims; Aarti Shahani, *Smartphones Are Used to Stalk, Control Domestic Abuse Victims*, NPR (Sept. 15, 2014), https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims; Jason Koebler, *'I See You': A Domestic Violence Survivor Talks About Being Surveilled By Her Ex*, Motherboard (March 17, 2017), https://motherboard.vice.com/en_us/article/bmbpvv/i-see-you-a-domestic-violence-survivor-talks-about-being-surveilled-by-her-ex.

[xvii] After analyzing the purchases of a female high school student, Target sent an ad to her house for pregnancy-related products. This exposed the young woman's pregnancy to her father without her consent. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.