Chair Lina Khan
Commissioner Rohit Chopra
Commissioner Rebecca Slaughter
Commissioner Noah Phillips
Commissioner Christine Wilson

Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580

Chair Khan and Commissioners Chopra, Slaughter, Phillips, and Wilson:

We, the undersigned civil rights, civil liberties, and consumer protection organizations, write to bring your attention to the urgent need for the Federal Trade Commission to protect civil rights and privacy in data-driven commerce. The Internet is an irreplaceable venue for free expression, trade, employment and housing opportunities, banking, education, entertainment, and, of course, civic engagement. As courts have recognized for decades and recently reaffirmed, privacy rights are civil rights[1] and commercial data practices are inextricably intertwined with equal opportunity.[2]

We ask the FTC to (1) initiate rulemaking and take other appropriate actions to regulate unfair and deceptive commercial data practices such as those discussed below; (2) create an Office of Civil Rights; and (3) commit greater resources to aggressively enforce against unfair and deceptive practices. We urge the FTC to use all tools at its disposal.

Unfair and Deceptive Commercial Data Practices Cause Substantial Harm

As has been extensively documented by independent researchers, journalists, courts, companies, and this Commission, unfettered data practices employed single-mindedly for private gain cause significant harm to the public. Tech companies directly cause or contribute to many of these harms. Like the sprawling consequences of historic redlining, other harms arise as negative externalities (including downstream effects) from data-exploitative business models and the market incentives they create. Addressing direct harms and changing incentives will have positive effects for the Internet ecosystem as a whole.

---

[1] *See Am. for Prosperity Found. v. Bonta*, __ S.Ct. __, 2021 WL 2690268, *6 (July 1, 2021) (discussing *NAACP v. Alabama*, 357 U.S. 449 (1958)).

[2] *See Leaders of a Beautiful Struggle v. Baltimore Police Dept.*, __ F.4th __, 2021 WL 2584408, *14 (4th Cir. June 24, 2021) (en banc) (Gregory, C.J., concurring) (discussing how past redlining of Baltimore continues to affect resource distribution and public well-being, including "investment in construction; urban blight; real estate sales; household loans; small business lending; public school quality; access to transportation; access to banking; access to fresh food; life expectancy; asthma rates; lead paint exposure rates; diabetes rates; heart disease rates" and more.).

Harms to Civil Rights and Equal Opportunity

1) Automated decision-making systems produce and reproduce new and longstanding patterns of discrimination in recruiting, employment, finance, credit, housing, K-12 and higher education, policing, probation, healthcare, as well as the promotion of key services through digital advertising.

    a. Ex.: Facebook has been sued by advocates and the U.S. government for enabling discrimination by allowing advertisers to restrict ad viewership by race, religion, national origin, and other protected characteristics. Google and Twitter have similarly been investigated by HUD for housing discrimination.

2) Unscrupulous political operatives and foreign adversaries have used conventional advertising and targeting tools on social media platforms to interfere with U.S. elections and engage in voter suppression. Social media plays a key role in disinformation campaigns that spread conspiracy theories, threaten election integrity, and lead to violence such as the January 6 attack on the U.S. Capitol.

3) Disinformation campaigns in non-English languages are particularly rampant due to disregard by major platforms such as Facebook. The ability to target these types of campaigns depends on the privacy-invasive architecture of social media platforms.

4) Platform design choices routinely enable discrimination within important consumer services and workplaces.

    a. Ex: Airbnb enabled landlords to reject prospective guests with what were perceived to be distinctly Black names at higher rates than guests with what were perceived to be distinctly white names.

    b. Ex: Uber enabled drivers to discriminate against passengers with what were perceived to be distinctly Black names and provide more expensive services to women passengers. Uber likewise used biased consumer-reviews to make workplace decisions that may violate civil rights.

5) Social media firms' algorithmic design choices create pathways to white supremacy, which can lead to violence and deprivation of civil rights.

    a. Ex: An internal Facebook study obtained by the Wall Street Journal noted that "64% of extremist group joins are due to our recommendation tools...our recommendation systems grow the problem."

    b. Ex: YouTube video recommendations systemically recommend harmful and progressively more extreme content to viewers, creating pathways to radicalization.

6) Firms reify and advance existing social prejudices, particularly racism, throughout technology and online services, including through search engine and other predictive

text results, voice technologies, facial analysis, and other biometric and visual processing techniques.

7) Workers are increasingly monitored through digital surveillance programs in and beyond the place of employment, raising novel questions as to whether and how these applications enable exploitation and discrimination. Tech firms dehumanize workers through intrusive surveillance and intermediating working relationships with opaque, sometimes degrading workplace management software.

8) Delivery service drivers protested a nearly-invisible method of pay calculation that put customers' tips toward guaranteed minimum wages.

9) Platform companies use "psychological tricks" on workers, not dissimilar to the dark patterns used on consumers, to maximize company growth.

10) Facial recognition and other biometric surveillance technologies erode civil liberties, particularly for Black and Brown communities. The biases in these technologies and their use by law enforcement have led to traumatic violations of civil liberties, including a number of recent wrongful arrests of innocent Americans misidentified by faulty facial recognition software.

11) Ambient state and private surveillance in public spaces has a chilling effect on basic freedoms and disproportionately affects Black and Brown communities.

Harms to Consumer Protection and Invasions of Privacy

1) Digital firms employ "dark pattern" techniques to confuse and exploit consumers, including intentionally complicating the process of opting-out of data collections.

2) Digital firms use similar designs to trick consumers into sharing personal data or buying services they may not want.

3) Digital firms use similar designs to obscure pricing and fee structures for services up front.

4) Digital firms use similar designs and practices to make it difficult for consumers to change privacy settings, delete accounts, or cancel services.

5) Amazon has labeled as "Amazon's Choice" or sold from its warehouses products that are deceptively labeled, or have been declared unsafe or banned by federal regulators.

6) E-commerce sites like Amazon and Google have continued to sell items they promised to ban, such as pill presses that have been used to manufacture counterfeit prescription drugs or firearm accessories.

7) Millions of businesses listings on mapping sites are fraudulent with analysts cited by the WSJ estimating up to 11 million listings on Google maps may be false listings.

8) Negligence and lax safety standards enable bad actors to commit elaborate frauds on digital platforms.

    a. Ex: Various Airbnb scams.

    b. Ex: Applications on smartphone app stores with billions of downloads have been found to be committing ad fraud.

9) Research conducted by Consumer Reports found that nearly half of consumers struggle to distinguish between a paid ad and an objective search result.

10) Large online advertising platforms are combining data with real-world purchasing and customer information to track them across the web and in the physical world.

11) Navigation applications optimize routes for speed regardless of the negative impact on public safety and traffic. Multiple people have been killed by so-called "self-driving" or auto-pilot enabled cars on public roads. Some evidence suggests the entry of a ride-sharing application into a city increases the number of fatal accidents by 3%.

12) Platform transportation companies erode the hard-won public safety protections put in place over decades around seatbelts, child safety seats, distracted driving, helmet-wearing, and more.

13) E-commerce and platform companies whose delivery drivers kill or maim pedestrians refuse to take responsibility for those injuries, despite incentivizing dangerous driving behavior.

    a. Ex: Amazon incentivized drivers to rush through holiday delivery. Upon being sued by the family of a pedestrian who was killed, they claimed: "The damages, if any, were caused, in whole or in part, by third parties not under the direction or control of Amazon.com."

14) Firms' amplification and enabling of public health misinformation at scale has eroded public trust in vaccines and public health officials. Too many American families and their loved ones have been severely harmed by their belief in misinformation, particularly during the COVID-19 pandemic, and vaccine hesitancy remains an issue.

15) Large online advertising platforms like Google have placed ads on sites promoting COVID-19 conspiracy theories in contrast to the commitments they made to combat COVID-19 misinformation.

16) Platform design choices that algorithmically amplify false information and propaganda in order to increase engagement on social media can grossly warp public discourse and understanding around public events, complicating the media landscape for consumers.

17) Firms track Americans in gross detail, relying on contrived interpretations of consumer consent or without explicit consent.

    a. Ex. Mobile phone trackers collect precise location over 14,000 times per day.

18) Firms collect consumer data that they do not need without consent.

19) Firms accept and purchase user data collected by other firms without their consent.

    a. Ex: Facebook received ovulation data from a third party without user consent.

20) Firms collect consumer data under the pretense of consent, perpetuating the fallacy that consumers are in a position to read, understand, or give informed consent (often consumers *must* use services and lack other options or the ability not to consent).

21) Firms use deceptive disclosures and settings to trick consumers into allowing data sharing with third parties.

22) Firms use personal consumer data—including private emails, conversations, and photographs—to develop algorithmic products without full consumer knowledge, consent, or reciprocity.

23) Firms fail to secure or delete obsolete user data, resulting in significant individual and collective costs. While firms may prefer to paint themselves as victims, a more apt metaphor might be oil companies who fail to prevent oil spills.

    a. Ex: Experian's API weakness likely exposed "most Americans'" credit scores, creating a feeding frenzy for identity thieves.

    b. Ex: Popular genetic testing services have insufficient security leading to significant potential for exploitation of genomic and health information.

24) Poor data protection can result in both exploitative and exclusionary conduct.

25) Privacy harms are especially acute in combination with competitive harms: experts have shown that firms that achieve market dominance and successfully suppress competitive threats are able to lower privacy protections to pursue and extract greater data gains from consumers.

    a. Ex: Facebook pivoted away from privacy-protection toward privacy exploitation upon achieving significant market power.

26) Digital firms use unprecedented data collection and targeting tools to exploit behavioral shortcomings and biases amongst consumers in real-time.

27) Digital firms employ a bevy of dynamic pricing strategies, which nearly three-quarters of Americans think is a problem.

FTC Should Regulate and Stop Unfair and Deceptive Commercial Data Practices

The following practices relating to the use of consumers' personal data are unfair or deceptive. They cause many of the harms discussed above, either directly or by causing downstream negative externalities. The FTC should take immediate action to address them using all tools at its disposal, including but not limited to rulemaking.

Civil Rights and Equal Opportunity

1) Using criteria that have the purpose or effect of resulting in adverse eligibility determinations or to target or deliver advertisements for housing, employment, credit, insurance, or educational opportunities on the basis of protected characteristics. This does not include using protected characteristics (a) for legitimate self-testing for the purpose of preventing unlawful discrimination, complying with legal requirements, or assessing diversity, equity, and inclusion programs; or (b) for the bona fide and primary purpose of expanding an applicant, candidate, participant, or customer pool by increasing diversity and inclusion.
2) Using personal data to violate rights protected by federal law, where such rights are capable of being violated by a private actor. This includes using personal data to deprive or defraud someone of the right to vote in violation of federal law.
3) Disclosing non-public information related to an individual's sexual life without specific opt-in consent, such as their sexual activity, relationships, orientation, gender identity or expression, preferences, communications, or behavior. This does not include automated linking to, republishing of, or indexing such information if it was already disclosed by others—such as routine search engine operations.
4) Offering online services that are not accessible to persons with disabilities.
5) Failing to provide disclosures and policies in all languages in which the company routinely provides service.
6) Using machine learning or artificial intelligence technology to process personal data or aggregate data about a population without ensuring, prior to deployment and through regular assessment, that such processing does not directly or indirectly result in adverse eligibility decisions or exclusion from commercial opportunities on the basis of protected characteristics.
7) Using machine learning or artificial intelligence technology in a manner that does not comport with what the technology is marketed or represented to do, if such use causes harm to consumers.
8) Claiming that a product using machine learning or artificial intelligence technology can predict future outcomes with a degree of certainty or accuracy, or predict human behavior at all, if the claimant does not possess reliable evidence that such technology has any such capability greater than a simple linear regression analysis or random chance.

9) Representing that a product using machine learning or artificial intelligence technology has a source, sponsorship, approval, certification, accessories, characteristics, components, uses, or benefits that it does not have, or that such product is of a certain standard, quality, grade, style, or model when it is not.

10) Designing, modifying, or manipulating a user interface of a service, directed at children under the age of 13, with the purpose or substantial effect of cultivating compulsive usage.

11) Using personal data to target or deliver personalized advertisements to children under the age of 13. This does not include contextual advertising.

12) Using personal data to conduct psychological experiments on users without opt-in consent and compliance with best practices for such research, if it is reasonably foreseeable that such experiments may result in harm physical or mental health.

Data Protection

1) Failing to minimize data collection and retention. Collected data should be limited to what is necessary to provide the service requested by the consumer; should not be used for secondary purposes; and should not be retained for longer than is necessary to satisfy the purpose for which it was collected. Secondary uses should not be allowed without additional and specific opt-in consent.

2) Using facial recognition technology on persons in traditional public forums or places of public accommodation without opt-in consent.

3) Collecting, sharing, or otherwise using an individual's biometric data, including but not limited to facial recognition technology, without specific opt-in consent and without a valid business necessity.

4) Disclosing, without authorization or in excess of authorization, the content of a communication to anyone who is not a party to the communication or who does not have authorization to access it, including both state actors and private parties.

5) Collecting sensor recordings of environmental data from a consumer device, in conjunction with personal data, without opt-in consent. This includes data collected by a microphone, camera, or other sensors capable of measuring chemicals, light, radiation, air pressure, speed, weight or mass, positional or physical orientation, magnetic fields, temperature, or sound. This does not include processing by an entity that did not directly collect the data.

6) Collecting personal data as a third party about users of an online service, where such data is not publicly available, without opt-in consent from affected individuals. This includes, for example, cursor movements and clicks, heat maps, in-app activity, location information, third party tracking beacons and cookies, and other third-party methods of tracking user activity.

Due Process

1) Requiring consumers to consent to pre-dispute binding arbitration clauses or class action waivers.
2) Requiring consumers to waive privacy or other rights to obtain service or requiring that consumers who do not waive their rights pay a higher fee. This does not include customer loyalty programs, such as grocery store discount cards.
3) Denying consumers the ability to access, correct, delete, or port their personal data in response to a reasonable request.
4) Failing to provide an effective and prompt appeal when requests to access, correct, delete, or port data are denied.
5) Using dark patterns and other misleading user interfaces to unfairly or deceptively induce consent or other adverse actions from a consumer.

Transparency

1) Failing to affirmatively disclose, in a clear and conspicuous manner, how a data processor collects, uses, shares, and retains personal data, including failing to explain a consumer's ability to control the use of their data.
2) Failing to affirmatively disclose when and how a company uses machine learning or other artificial intelligence technology to process personal data, when such processing affects commercial goods, services, or opportunities that a consumer may receive. This includes failure to disclose non-sensitive information from risk assessments.
3) Failing to conspicuously provide all relevant privacy policies and controls in one place, such as scattering privacy policies, updates, or controls across multiple parts of a website or app. This practice is particularly deceptive when a consumer's intent to change a privacy control in one area can be undermined by failure to change other controls in other areas, and such discrepancy is not conspicuous.
4) Refusing to tell a consumer to whom the company disclosed their personal data, or with whom the company contracts to share such data, in response to a reasonable request.
5) Failing to notify a consumer when the company discloses their personal data to a state actor unless the company is legally required not to disclose.
6) Misstating or mischaracterizing the subject matter, methods, frequency, or results of any of one's own internal or external assessments.

Security

1) Failing to secure personal data, to protect the integrity of personal data, or to prevent unauthorized access or processing of personal data.

2) Failing to promptly notify affected parties following a data breach.

3) Failing to comply with state data breach laws and regulations when such failure affects interstate commerce and is not inconsistent with federal law.

4) Disclosing non-public personal data to a service provider or third party without contractually requiring the service provider or third party to meet the same privacy standards as the company, or without engaging in reasonable oversight to ensure compliance with such requirements.

Accountability

1) Retaliating against whistleblowers who attempt to report unfair or deceptive practices.

2) Knowingly aiding and abetting another person engaging in an unfair or deceptive practice.

3) Failing to report to the Commission if a company has knowledge that a service provider, affiliate, or customer has engaged in an unfair or deceptive practice involving the company's goods or services. This does not include content immunized by 47 U.S.C. 230.

4) Failing to provide an annual sworn certification from a C-suite officer or equivalent senior officer that a company (other than a small business) is fully compliant with the FTC's data privacy rules.

Office of Civil Rights

The FTC should create an Office of Civil Rights. There are more than 30 civil rights offices within federal agencies. The harms and unfair or deceptive practices discussed in this letter are part of a large, interconnected data ecosystem. Expanding the Commission's expertise on discrimination and equal opportunity will help it holistically assess the equities of modern digital trade. Such an Office will create a focal point for Agency expertise and stakeholder engagement on these important issues. The Office could also advise on actions the Commission may take, and coordinate with other agencies, to help respond to commercial data practices that may result in unjust disparate treatment or impact on the basis of race, ethnicity, religion, national origin, immigration status, disability, sex, gender identity or expression, sexual orientation, age, or familial status.

As the FTC looks to chart a new course for oversight of unfair and deceptive practices arising from commercial data practices and big tech, we look forward to working with you to protect civil rights, promote algorithmic fairness, advance equal opportunity, and preserve privacy and free expression.

For more information, please contact David Brody and Sara Collins.

Sincerely,

Access Now

Accountable Tech

Asian Americans Advancing Justice | AAJC American

Association for Justice

ADL

Center for American Progress

Center for Digital Democracy

Center for Democracy and Technology

Center on Privacy & Technology at Georgetown Law

Common Cause

Common Sense Media

Consumer Action

Consumer Federation of America

Electronic Privacy Information Center

HTTP

Lawyers' Committee for Civil Rights Under the Law

Media Alliance

National Council of Asian Pacific Americans National

Fair Housing Alliance

National LGBT Task Force

OCA – Asian Pacific American Advocates

Public Citizen

Public Knowledge

Ranking Digital Rights

The Greenlining Institute