November 21, 2022

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Ave. NW, Ste. CC-5610 (Annex B)
Washington, D.C. 20580

Submitted via https://www.regulations.gov

RE: Commercial Surveillance ANPR, R111004

AMERICAN CIVIL LIBERTIES UNION

National Office
125 Broad Street
18th Floor
New York, NY 10004
aclu.org

Deborah N. Archer
President

Anthony D. Romero
Executive Director

The American Civil Liberties Union ("ACLU") appreciates the opportunity to file this comment in response to the Federal Trade Commission's ("FTC" or "Commission") advanced notice of proposed rulemaking regarding commercial surveillance and data security (FTC-2022-0053-0001). The ACLU writes to highlight the numerous harms suffered by consumers due to lack of protection against abusive data collection, processing, and use practices by companies, and to urge the Commission to take strong, effective action through new trade regulation rules.

The ACLU is a nationwide, nonpartisan, nonprofit organization dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. In the digital age, our work seeks to ensure that emerging technologies enhance these principles rather than undermine them. Through litigation and policy advocacy, and in public education campaigns, the ACLU challenges practices that threaten our rights to privacy and freedom from discrimination, including abusive commercial surveillance practices and lax data security;[1] the nonconsensual collection and use of biometric identifiers;[2] and discrimination facilitated by automated systems and other modern technologies.[3]

---

[1] *See, e.g.*, Complaint, *ACLU v. Dep't. of Homeland Sec'y*, No. 1:20-CV-10083-PGG (S.D.N.Y. Dec. 3, 2020); Shreya Tewari & Fikayo Walter Johnson, *New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data*, ACLU (July 18, 2022), https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data; Request for Investigation & Complaint for Injunctive Relief, *In re AT&T Inc., Verizon Wireless, Sprint Nextel Corp., & T-Mobile USA, Inc.* (Apr. 16, 2013), https://www.aclu.org/legal-document/ftc-complaint-smartphone-security; Jay Stanley, *There's Nothing Inevitable About Apps That Track Your Every Move*, ACLU (Dec. 11, 2018), https://www.aclu.org/news/privacy-technology/theres-nothing-inevitable-about-apps-track-your-every-move.

[2] *See generally* ACLU, *The Fight to Stop Face Recognition Technology* (updated July 15, 2021), https://www.aclu.org/news/topic/stopping-face-recognition-surveillance; *see also, e.g.*, Joint Motion for Entry of Consent Order & Dismissal Ex. 2, *ACLU v. Clearview AI*, No. 2020 CH 04353 (Cook Cnty. Ill. Cir. Ct. May 9, 2022); Complaint, *Williams v. City of Detroit*, No. 2:21-CV-102827-GAD-APP (E.D. Mich. Apr. 13, 2021); Press Release, ACLU, ACLU Comment on Facial Recognition and Biometric Technology Moratorium Act (June 15, 2021), https://www.aclu.org/press-releases/aclu-comment-facial-recognition-and-biometric-technology-moratorium-act.

[3] *See, e.g.*, Galen Sherwin & Esha Bhandari, *Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform*, ACLU (Mar. 19, 2019), https://www.aclu.org/news/womens-rights/facebook-settles-civil-rights-cases-making-sweeping.

We are pleased to submit these comments, which reflect and synthesize the ACLU's experience furthering civil rights and liberties in the digital age.

EXECUTIVE SUMMARY

- Section I. FTC Rulemaking Should Address the Numerous Commercial Surveillance Practices that Disempower and Harm Consumers.
- Section II. Trade Regulation Rules Should Be Informed by, but not Exclusive to, Harms Arising from Commercial Surveillance Involving Biometric and Location Data.
- Section III. FTC Rulemaking Can and Should Address Algorithmic Discrimination and Other Prevalent Harms of Automated Decision-Making Systems.

I. FTC Rulemaking Should Address the Numerous Commercial Surveillance Practices that Disempower and Harm Consumers

Commercial surveillance practices are constantly evolving. Machine learning and other data-driven technologies create ever-growing demand for consumer data, and novel products and services open access to more and different types of personal information.

Are these offering greater value to consumers? If you ask consumers, the answer is clearly no. According to the Pew Research Center, as of 2019 *81% of consumers* believed that the potential risks of companies collecting data about them outweighed the benefits.[4] The same percentage agreed that they have very little or no control over the data companies collect.

Unfortunately, they are correct. Instead of responding to distrust by adapting their practices to protect consumers from harm, too many companies have instead sought to protect only their own interests, erecting obstacles to deter consumers from what little control they might exercise over their personal data or simply concealing the companies' practices from consumers outright.

The ACLU supports FTC rulemaking to rein in commercial surveillance, not by burdening users with the impossible task of managing their own data as it flows through the complex web of advertisers, data brokers, government agencies, and other parties who buy and sell it for their own benefit, but by changing the paradigm and demanding that companies collect and use consumer data in service of consumers. Strong rules that go beyond the "notice-and-choice" paradigm are the only way to address the serious harms that consumers experience under the current abusive system of commercial surveillance. The Commission can, consistent with the First Amendment, promulgate rules that constrain companies engaged in commercial surveillance of consumers.

A. Companies Use Various Commercial Surveillance Practices Designed to Disempower Consumers

Related Questions: *1. Which practices do companies use to surveil consumers?*

74. In which circumstance, if any, is consumer consent likely to be effective?

80. Have opt-out choices proved effective in protecting against

[4] Pew Research Ctr., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information* (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

commercial surveillance? If so, how and in what contexts?

Unfortunately, companies use every practice available to them, and work constantly to build new mechanisms of surveillance. In other words, for many companies, there is no such thing as too much data, too sensitive data, or data obtained under too questionable circumstances. Companies consider more data to collect, analyze, or sell to be a worthwhile end in itself.

As a result, companies have responded to persistent consumer opposition to data collection with ever-increasing commercial surveillance. Moreover, in their profit-seeking collection of personal data about consumers, they pursue tactics that undermine consumers' ability to control their personal information, and by extension their autonomy and their lives. "Opt-out" models are particularly susceptible to this manipulation. Opt-out mechanisms place the burden on consumers to identify and respond to privacy threats and incentivize companies to structure their systems to make opting out difficult. But even better models for discerning consumer choice (like opt-in consent) can be abused if not coupled with firm regulations outright prohibiting harmful practices.

1. Commercial Surveillance Is Designed to Circumvent Consumer Opposition to Data Collection

Consumers sometimes willingly share information, particularly where that information will be used for their personal benefit or a societal good. But when data is gathered for the benefit of corporate or governmental interests, consumers are understandably less likely to agree. The response to the recent change in iOS requiring affirmative consent to "track your activity across other companies' apps and websites" makes this clear: a strong majority of users decline consent to such tracking.[5] This is consistent with consumers' overall attitudes towards privacy.[6]

Under an effective privacy regime based on meaningful consent, companies handling consumer data would have two choices in this scenario. First, they could attempt to persuade consumers to share more data, presumably by convincing them that doing so is in the consumer's individual interests or to the benefit of society. Alternately, companies could adapt their practices to be consistent with consumer desires.

However, there is little evidence either of substantial efforts to win over consumers nor of any shift in public opinion in favor of the widespread collection of personal data.[7] Nor has there been a shift back to contextual advertising, a successful business model for decades with no requirement for commercial surveillance, or to non-advertising models that have existed even longer. Instead, companies have increasingly turned to commercial surveillance, paying lip service to "protecting privacy" while aggressively seeking to subvert informed consumer choice by concealing or rendering unavoidable data collection practices.

---

[5] Estimates vary, but all identified sources agree that a majority of consumers have and are expected to continue to decline tracking. *See, e.g.*, Filipe Espósito, *Number of Users Opting in to App Tracking on iOS Grows Significantly since Last Year*, 9 to 5 Mac (Apr. 14, 2022), https://9to5mac.com/2022/04/14/number-of-users-opting-in-to-app-tracking-on-ios-grows-significantly-since-last-year/ (estimating that 75% of users decline tracking); Thorin Klosowski, *Looking Back on a Year of Apple's Privacy Labels and Tracking* (Mar. 31, 2022), N.Y. Times, https://www.nytimes.com/wirecutter/blog/apple-privacy-labels-tracking/ (stating that ad-analytics company AppsFlyer estimated that 60% of users decline tracking).

[6] Pew Research Ctr., *supra* note 4.

[7] As the N.Y. Times pointed out, some efforts to persuade consumers to consent were particularly "cringeworthy," including claims that agreeing to tracking would "bring [an app] to more people in need" or "help [consumers] save money and live better through ads." Klosowski, *supra* note 5.

2. *Commercial Surveillance Practices Use Numerous Insidious Techniques to Disempower Consumers*

In an era of ever-increasing technological complexity, requiring consumers to manage their own privacy across myriad apps, devices, and web sites, and to discern between beneficial and harmful uses of their data, is impossible. Instead of restraining their data collection to practices that respect consumers' dignity and empower them to make meaningful decisions, companies have done the opposite: concealing or disguising data collection, eliminating functional notice, and discouraging or preventing the effective exercise of choice.

The following is an illustrative, but not comprehensive, survey of commercial surveillance practices, organized loosely by the way in which the practice disempowers consumers and invades unnecessarily into their private lives and decisions:

a. Commercial Surveillance Practices that Are Invisible to Consumers

While consumer awareness of privacy harms in general has increased, consumers are still poorly equipped to spot the "hidden cameras"—literal and figurative—that monitor their activities. The theoretical ability to limit data collection has no value if consumers have no indication that they are being surveilled in the first place. Unfortunately, that is all too common a reality:

- Many of the most popular web pages contain dozens or even hundreds of trackers that are invisible to the end user: pixel images, JavaScript code, and similar technologies that collect data on behalf of third parties.[8]

- Mobile applications similarly may incorporate numerous third-party "software development kits" (SDKs) designed specifically to collect data for third parties, hidden from the view of end users.[9]

- Privately-operated automated license plate readers (ALPR) silently collect information about vehicles and their occupants, compiling location data about millions of Americans without any meaningful notice.[10]

b. Commercial Surveillance Practices that Exploit Consumer Trust

Consumer trust in corporate data practices is justifiably low – but not every company is equally distrusted. While consumers evince profound mistrust towards entities widely known as poor data stewards, they are not as skeptical towards products that appear to legitimately have their best interests at heart.

Too often, however, such trust is misplaced; instead, examples abound of entities that appear to

---

[8] *See* Farhad Manjoo, *I Visited 47 Sites. Hundreds of Trackers Followed Me.*, N.Y. Times (Aug. 23, 2019), https://www.nytimes.com/interactive/2019/08/23/opinion/data-internet-privacy-tracking.html.

[9] *See* Sara Morrison, *The Hidden Trackers in Your Phone, Explained*, Vox (July 8, 2020), https://www.vox.com/recode/2020/7/8/21311533/sdks-tracking-data-location.

[10] *See* Angel Diaz & Rachel Levinson-Waldman, *Automated License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, Brennan Ctr. for Justice (Sept. 10, 2020), https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations.

serve consumers' best interests, but instead violate their trust:

- Mobile apps specifically geared towards Muslim communities collected precise geolocation data about users—useful to identify local prayer times—and sold this information to data brokers who resold it to various parties including the U.S. military.[11]

- Researchers at Mozilla gave 28 out of 32 mental health and prayer apps a "Privacy Not Included" warning label for routinely sharing data and engaging in other privacy-abusive practices.[12]

- Business "loyalty" or "rewards" programs often collect and profit from the personal data of members, contrary to most people's impression that the consumer is the one receiving benefits in appreciation of their loyalty.[13]

This issue extends even to products that are nominally billed as protecting user privacy or security:

- Data security mechanisms, such as two-factor authentication, have been marketed to consumers as safety features while actually using disclosed information for other purposes.[14]

- Products advertised as protecting consumer privacy, including VPN and ad-blocking apps, have harvested and sold data collected from their users' devices.[15]

More recently, COVID-19 has provided still more opportunities to push surveillance deeper into people's lives. In the early days of the pandemic, given the uncertainty about the transmission of the virus, many restaurants replaced physical menus with online menus, commonly accessed via QR codes. However, many of these QR codes served an ulterior purpose: instead of merely directing the customer

---

[11] Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, Vice (Nov. 16, 2020), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x; *see also* Alexandra S. Levine, *Suicide hotline Shares Data with For-Profit Spinoff, Raising Ethical Questions*, Politico (Jan. 28, 2022), https://www.politico.com/news/2022/01/28/suicide-hotline-silicon-valley-privacy-debates-00002617

[12] Mozilla, *Top Mental Health and Prayer Apps Fail Spectacularly at Privacy, Security* (May 2, 2022), https://foundation.mozilla.org/en/blog/top-mental-health-and-prayer-apps-fail-spectacularly-at-privacy-security/.

[13] *See* Press Release, Rob Bonta, Attorney Gen., State of Ca. Dep't of Just., On Data Privacy Day, Attorney General Bonta Puts Businesses Operating Loyalty Programs on Notice for Violations of California Consumer Privacy Act (Jan. 28, 2022), https://oag.ca.gov/news/press-releases/data-privacy-day-attorney-general-bonta-puts-businesses-operating-loyalty (highlighting California Attorney General's investigation into practice of exploiting data collected via loyalty programs contrary to the California Consumer Privacy Act).

[14] Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook. But that settlement, binding only on Facebook, has not necessarily curtailed the practice; while the Commission's research suggests that other parties have not engaged in "user-observable secondary uses" of such numbers, Min Hee Kim et al., *Secondary Education: Measuring Secondary Uses of 2FA Phone Numbers* (Aug. 2020), https://www.ftc.gov/system/files/attachments/office-technology-research-investigation/way2020-kim.pdf, there is no evidence that further hidden uses of such data have been curtailed.

[15] *See* Craig Silverman, *Popular VPN and Ad-Blocking Apps Are Secretly Harvesting User Data*, BuzzFeed News (Mar. 9, 2020), https://www.buzzfeednews.com/article/craigsilverman/vpn-and-ad-blocking-apps-sensor-tower

to a menu, they collected information in the process, surreptitiously adding to the customer's digital profile.[16]

c. Commercial Surveillance Practices Embedded in Essential or Unavoidable Services

Privacy-conscious consumers may do their best to avoid data-hungry online services. But doing without a credit card, a car, an Internet connection, or even an apartment is much more challenging. As more and more essential products become "smart," the potential for commercial surveillance has expanded into areas where consumers have little ability to simply opt out. Consumers are frequently in the dark about such practices. Even when consumers seek information about how their data is being collected and shared, companies only identify broad "categories" of shared information and recipients. Even savvy data journalists have been stymied in ferreting out the full details.[17]

- Credit card providers have access to "a vast amount of detail about our lives: how much we spend on travel, restaurants, political or religious donations, liquor stores, sex shops, and on and on. And of course, that kind of information is more powerful and revealing when combined with other data."[18]

- Connected cars "are capable of amassing data on nearly every aspect of a drive, from road conditions to whether or not you've gained weight since the last time you sat in the driver's seat."[19]

- Renters increasingly encounter "smart home" or "security" devices that demand access to personal data as a requirement of tenancy.[20]

- Internet service providers (ISPs) collect information about our browsing histories, television viewing habits, and other online activity, correlate activity across devices, and use that information for advertising purposes or for sale to other entities.[21]

---

[16] *See* Nicole Ozer & Jay Stanley, *Diners Beware: That Meal May Cost You Your Privacy and Security*, ACLU (July 21, 2021), https://www.aclu.org/news/privacy-technology/diners-beware-that-meal-may-cost-you-your-privacy-and-security.

[17] *See* Kashmir Hill, *Amazon and Chase Will Not Give Me a Straight Answer About What They Do With My Credit Card Data*, Gizmodo (Jan. 23, 2019), https://gizmodo.com/neither-amazon-nor-chase-will-give-me-a-straight-answer-1831882327.

[18] *See* Jay Stanley, *Why Don't We Have More Privacy When We Use A Credit Card?*, ACLU (Aug. 13, 2019), https://www.aclu.org/news/privacy-technology/why-dont-we-have-more-privacy-when-we-use-credit-card.

[19] Alfred Ng, *What Your Car Knows About You*, Politico, Politico (Aug. 2, 2022), https://www.politico.com/newsletters/digital-future-daily/2022/08/02/car-knows-about-you-data-collection-privacy-00049309.

[20] *See, e.g.*, Sarina Trangle, *Privacy Concerns Mount Over Tech-Based Apartment Building Access*, AM N.Y. Metro (Sept. 22, 2019), https://www.amny.com/real-estate/apartment-access-privacy-concerns-1-29927187/; Hiawatha Bray, *In Smart Apartments, Is Tenants' Privacy For Rent?*, (Feb. 11, 2020), https://www.bostonglobe.com/2020/02/11/business/smart-apartments-is-tenants-privacy-rent/.

[21] *See* FTC, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers* (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.

- Mobile carriers, including AT&T, Sprint, and T-Mobile, have sold access to real-time location data to data brokers, who in turn resold it to government agencies, bail bondsmen and bounty hunters, among others.[22]

Other products or services that are tightly coupled with commercial surveillance may seem easier to decline—on an individual level. But with the increasing ubiquity of smart … well, everything, the "Internet of Things" presents a risk of surveillance built in to so many products that it's practically impossible to avoid:

- Products like Amazon Alexa or Google Nest raise obvious red flags for privacy-conscious consumers.[23] But an increasing number of consumer products—from televisions to toasters—are not merely capable of gathering and sharing data but do so by default.[24]

- These products are increasingly equipped with microphones and sensors, and thus able to record far more than just a consumer's interactions with that device.[25]

d. Commercial Surveillance Practices That Frustrate Consumers' Efforts to Protect Themselves

The previous examples primarily address situations where individual consumers are deprived of autonomy: either commercial surveillance is hidden or it is embedded in the ecosystem beyond their control. But even when consumers take steps to protect their privacy, obstacles too frequently remain.

As the Commission has observed, one of the most problematic categories of obstacles are "sophisticated design practices known as 'dark patterns' that can trick or manipulate consumers into … giving up their privacy."[26] Examples of dark patterns enabling commercial surveillance abound:

- Cookie opt-out mechanisms that require consumers to disable each type of cookie individually while streamlining the process of agreeing to all cookies, including third-party trackers.[27]

---

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

[23] *See* Jay Stanley & Josh Bell, *Does Your Shiny New Gadget Come with Privacy Pitfalls?*, ACLU (Dec. 20, 2018), https://www.aclu.org/news/privacy-technology/does-your-shiny-new-gadget-come-privacy-pitfalls.

[24] *See* Catherine Crump & Mathew Harwood, *Invasion of the Data Snatchers: Big Data and the Internet of Things Means the Surveillance of Everything*, (Mar. 25, 2014), https://www.aclu.org/news/speakeasy/invasion-data-snatchers-big-data-and-internet-things-means-surveillance-everything.

[25] *See* Kate O'Flaherty, *What Your Smart TV Knows About You – And How To Stop It Harvesting Data*, The Guardian (Jan. 29, 2022), https://www.theguardian.com/technology/2022/jan/29/what-your-smart-tv-knows-about-you-and-how-to-stop-it-harvesting-data.

[26] Press Release, Fed. Trade Comm'n, FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers (Sept. 15, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers.

[27] Even when consumers opt out of tracking, many websites track them anyway. Thomas Germain, *I Said No to Online Cookies. Websites Tracked Me Anyway*, Consumer Reports (Sept. 29, 2022), https://www.consumerreports.org/electronics-computers/privacy/i-said-no-to-online-cookies-websites-tracked-me-anyway-a8480554809/.

- Sign-up flows that encourage consumers to share more information, such as their contact lists, with no visible way to decline.[28]

In other cases, commercial surveillance practitioners attempt to subvert consumers' attempts to act to protect their privacy via other mechanisms:

- According to research from 2020, a quarter of top websites engage in "browser fingerprinting," an identification technique developed explicitly to circumvent consumer efforts to prevent tracking.[29]

- Meta is currently facing a class action lawsuit alleging that it circumvented iOS restrictions on third-party tracking by opening web pages in Facebook's in-app browser, allowing it to continue to track users across third-party web sites.[30]

3. Consumer Surveillance Highlights Fatal Flaws in Consent-Based Privacy Protections

Many of the practices above arise out of companies' exploitation of so-called "notice-and-choice" privacy protections. The fundamental premise of these regimes, which is that it is possible for consumers to be adequately informed about what will happen to their personal information so that they can direct its flow and use, is questionable even in the abstract. But when information is delivered, and consent obtained, by a party that has both the incentive and the capacity to manipulate or outright subvert the consumer's intent, even highly motivated consumers are vulnerable to exploitation. Informed consent simply cannot be presumed to exist in an adversarial setting.

This problem is most evident around "opt-out consent." Opt-out mechanisms not only fail to recognize the power and information disparities between consumers and data collectors; they also provide an incentive for companies to deter consumers from making choices at all by manipulating the default settings to reflect the company's (and not the consumer's) preference.

But other consent-based approaches, including "opt-in" models and other expressions of choice that rely on some form of consumer actions, are also subject to manipulation as described above. These techniques may sometimes be appropriate as one part of a more comprehensive approach to data privacy, helping companies understand more precisely how an individual user wishes their data to be used. But because they are subject to manipulation and abuse by corporations with the opportunity and motivation to do just that, even these are not adequate as the primary elements of a data privacy regime.

B. Companies Have Not Voluntarily Utilized Effective Measures to Protect Consumer Data

Related Question: 2. Which measures do companies use to protect consumer data?

There are, to be sure, some companies that aggressively protect consumer privacy: explicitly refusing to collect, retain, process, or disclose information in ways that harm consumers or violate their

---

[28] *See* Brian Krebs (@briankrebs), Twitter (Aug. 13, 2022), https://twitter.com/briankrebs/status/1558441625197633537.

[29] Catalin Cimpanu, *A Quarter of the Alexa Top 10K Websites Are Using Browser Fingerprinting Scripts*, ZDNet (Aug. 26, 2020), https://www.zdnet.com/article/a-quarter-of-the-alexa-top-10k-websites-are-using-browser-fingerprinting-scripts/.

[30] Taylor Hatmaker, *Facebook Users Sue Meta, Accusing the Company of Tracking on iOS Through a Loophole*, TechCrunch (Sept. 2, 2022), https://techcrunch.com/2022/09/22/meta-lawsuit-ios-privacy/.

expectations, and deploying technical and procedural safeguards to protect consumer privacy. Yet, too many prominent actors and industry groups continue to limit their protections strictly to legal obligations (which they strenuously lobby to minimize), often construed narrowly.

For example, in response to the enactment of the California Consumer Privacy Act (CCPA), Facebook, Google and Amazon have reportedly implemented minimal changes to their data flows. Rather than change their overall approach to personal data to match the privacy-protective mandates of the law, Facebook and Google instead created separate interfaces exclusively for California residents to comply with the law, while simultaneously delegating to business partners many of the compliance responsibilities.[31] Facebook has also argued that its "pixel" tracker was outside the scope of the CCPA, apparently willing to test the limits of the law rather than ensure its practices were consistent.[32]

It is worth noting that much of the debate over the American Data Privacy Protection Act in Congress has focused on the issue of state preemption, with industry voices insisting that the burden of complying with "inconsistent" state laws would undermine innovation to the detriment of both the online economy and individual consumers. But as the ACLU has pointed out, there is no reason to expect that state laws are or would be *incompatible* with each other such that a company could not extend the protections required by any given state to everyone.[33] Rather, companies could implement privacy practices that protected all consumers equally and satisfied—or, better yet, exceeded—the combined requirements of every state law. In any event, strong nationwide regulations promulgated and enforced by the Commission would create an essential backstop, ensuring that residents of states without enforceable privacy laws are not left unprotected.

Because so many companies have so aggressively sought to avoid meaningful changes to their practices to protect privacy, rather than focus on measures companies *have* adopted, it is likely more informative to examine the privacy-protective measures that major players in the data ecosystem *could* adopt—but that they have not yet done so.

1. Policies That Would Protect Consumer Data Privacy

The ACLU, including its affiliates, have supported numerous federal and state consumer privacy efforts over the past several years, several of which have been enacted into law,[34] and weighed in on

---

[31] *See* Allison Schiff, *Here's How Facebook, Google And Amazon Are Tackling CCPA Compliance* AdExchanger (July 9, 2020), https://www.adexchanger.com/privacy/heres-how-facebook-google-and-amazon-are-tackling-ccpa-compliance/.

[32] Sara Morrison, *Facebook Is Gearing Up for a Battle with California's New Data Privacy Law*, Vox (Dec. 17, 2019), https://www.vox.com/recode/2019/12/17/21024366/facebook-ccpa-pixel-web-tracker.

[33] *See* Letter from Christopher E. Anders, on behalf of the ACLU, to Chairman Pallone and Ranking Member McMorris Rodgers re: ACLU Statement on American Data Privacy Protection Act, Ahead of Committee Markup (July 18, 2022), https://www.aclu.org/letter/aclu-statement-american-data-privacy-protection-act-ahead-committee-markup.(hereinafter "ACLU Statement on American Data Privacy Protection Act").

[34] *See, e.g.*, ACLU of New York, *New York Deserves Digital Fairness* (Jan. 27, 2022), https://www.nyclu.org/en/publications/new-york-deserves-digital-fairness; ACLU of Massachusetts, *ACLU Supports New Massachusetts Bill to Advance Online Privacy and Equity* (Oct. 3, 2021), https://www.aclum.org/en/news/aclu-supports-new-massachusetts-bill-advance-online-privacy-and-equity; ACLU of Washington, *Introducing the People's Privacy Act: Real Privacy Protections for Everyone* (Jan. 28, 2021), https://www.aclu-wa.org/story/introducing-people%E2%80%99s-privacy-act-real-privacy-protections-everyone; ACLU of Maine, *LD 946; An Act To Protect the Privacy of Online Customer Information* (last visited Nov. 16, 2022), https://www.aclumaine.org/en/legislation/ld-946-act-protect-privacy-online-customer-information; ACLU of

other proposals concerning consumer privacy.[35] We have also compiled numerous case studies and other materials documenting the ways that companies succeed or fail in protecting consumer privacy.[36] These efforts repeatedly emphasize the same set of core practices that companies can and should follow—even without a legal obligation to do so—to protect consumer data:

- Ensure, first and foremost, that **harmful data uses are not permitted**. Audit data uses to identify and address algorithmic bias or other negative outcomes.
- **Implement purpose limitations and data minimization practices** by collecting, retaining, processing, and disclosing only the data needed to operate and provide services to consumers.
- Communicate clearly with users and **obtain informed, opt-in consent** to confirm that data practices match consumer expectations. Leverage global signals and other tools to better understand and respond to consumer choice. But make clear that opt-in consent does not excuse companies from complying with purpose limitations and data minimization requirements.
- **Protect data from misuse** by mindfully designing and continuously evaluating and improving privacy and security practices.
- **Maintain transparency** by allowing users full visibility into privacy and, insofar as possible, security practices.

2. Policies that Fail to Protect Consumer Data Privacy

In contrast, some policies are clearly inadequate to protect consumer privacy:

- **Opt-out "consent**," which as discussed elsewhere not only disregards the infeasibility of burdening consumers with identifying and managing their own privacy but also incentivizes companies to "innovate" by concocting new schemes to deter consumers from exercising this right.
- **De-identification or pseudonymization**, which far too frequently provide inadequate protections against many privacy harms due to the well-documented ability to re-identify information[37] and are irrelevant to the dignitary and community-oriented harms that may surface even from truly anonymous data. While there are privacy-protective computing techniques that legitimately address these concerns, "de-identification" serves primarily to protect data collectors from legal consequences while leaving consumers at risk.
- **Inadequate implementation** of measures to mitigate known privacy harms. After an

Illinois, *Biometric Information Privacy Act* (last visited Nov. 16, 2022), https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa.

[35] *See* ACLU Statement on American Data Privacy Protection Act, *supra* note 33; ACLU Comments to the Nat'l Telecomm. re: Developing The Administration's' Approach to Consumer Privacy (Nov. 9, 2018), https://www.aclu.org/letter/aclu-comments-developing-administrations-approach-consumer-privacy.

[36] *See, e.g.*, Jacob Snow, *What Companies Can Do to Protect Privacy and Free Speech: The ACLU Guide*, ACLU (Oct. 25, 2018), https://www.aclu.org/news/privacy-technology/what-companies-can-do-protect-privacy-and-free-speech-aclu.

[37] *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2009).

investigation by the ACLU of Northern California revealed that Facebook and Twitter provided access to "social media monitoring" services that generated "threat scores" of activists and viewed Black Lives Matter protesters as potential criminals,[38] both social media platforms asserted that their policies prohibited such use.[39]

C. Commercial Surveillance Harms Consumers in Numerous Ways

Related Question: *4. How, if at all, do these commercial surveillance practices harm consumers or increase the risk of harm to consumers?*

Commercial surveillance harms consumers in numerous ways; some practices harm everyone, others impact particular communities, and still others harm individual consumers. Many of these harms derive from the most basic: commercial surveillance is inherently harmful because it violates the fundamental right to privacy and control over personal information that is essential to individual autonomy and full participation in society.

1. Commercial Surveillance Effectuates Privacy Harms

Commercial surveillance—the collection, processing, and disclosure of consumer data without consent—can effectuate privacy harms that violate fundamental human rights. Even where such harms cannot be quantified, they should be considered in any analysis of harms from commercial surveillance.

Commercial surveillance threatens the "right to be left alone," as the right to privacy was famously described by Samuel Warren and Louis Brandeis.[40] The right to privacy is fundamental in and of itself, allowing individuals the space to consider new ideas and directions, including those that society might not embrace, without immediate risk of censure or criticism. It is also an essential safeguard to many other fundamental rights, ensuring that individuals may practice their religion, discuss politics, seek information or support for a mental health issue, or decide to have an abortion or seek other medical care without worrying about social or government censure.

This fundamental right is protected in a wide range of contexts. Laws prohibit the interception of letters or telephone calls. Librarians owe a duty of confidence to readers, doctors to patients, lawyers to clients, banks to customers, et cetera. "Intrusion upon seclusion" has long been recognized as tortious behavior. And the right to privacy is recognized in numerous state constitutions and under the Universal Declaration of Human Rights.

Violating a consumer's privacy by engaging in commercial surveillance that subverts their ability to bestow or withdraw consent should thus be viewed as harmful in and of itself, not merely as an action that may create the potential for harm. As courts have recognized, the nonconsensual loss of control over our personal information is itself a cognizable harm, whether or not an individual can

---

[38] *See* Matt Cagle, *This Surveillance Software is Probably Spying on #BlackLivesMatter,* ACLU of Northern California (Dec. 5, 2019), https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter.

[39] Chris Moody, *Developer Policies to Protect People's Voices on Twitter*, Twitter Developer Platform Blog (Nov. 22, 2016), https://blog.twitter.com/developer/en_us/topics/community/2016/developer-policies-to-protect-peoples-voices-on-twitter; Post by Rob Sherman, Facebook Pub. Affs., Facebook (Mar. 13, 2017), https://www.facebook.com/fbpublicaf-fairs/posts/1617594498258356.

[40] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harvard L. Rev. 193 (1890), https://archive.org/details/jstor-1321160/page/n1/mode/2up.

prove further injuries stemming from that harm.[41] And as surveillance practices become more widespread and more sophisticated, "what people do in their homes, in their cars, in stores, and within their communities will be monitored and analyzed in ever more intrusive ways by corporations and, by extension, the government."[42] The erosion of space that belongs to an individual, free from observation and data collection, is not merely a cause of other harms; it ***is*** harmful to that person's dignity, autonomy, and privacy.

2. Commercial Surveillance Reveals Consumer Data to Adverse Parties, Including Law Enforcement, Exposing Consumers to Direct Harm

Personal data, collected surreptitiously via commercial surveillance and put up for sale on the data broker market, may end up in the hands of an entity with a specific interest in the person. In far too many instances, that interest is detrimental: a desire to take physical or legal action against the individual.

The realization that commercial surveillance might lead directly to harms to the consumer—and that the participants might profit from that—is, sadly, not new. In 2003, the ACLU documented the growth of technology-enabled surveillance in the private as well as government sector, and the links between the two.[43] In 2004 we emphasized that both the increased efficiencies of technology and the outsourcing of government surveillance to private actors could result in a dramatic expansion in government intrusion into individual lives.[44] We also raised the concern that protections for individual privacy, most notably the Fourth Amendment, needed to be expanded lest they be bypassed—much as consumer agency could be—by data surveillance, "allow[ing] the government to carry out privacy-invading practices at 'arm's length' by piggy-backing on or actually cultivating data collection in the private sector that it could not carry out itself without serious legal or political repercussions."[45]

Almost 20 years later, too many of those fears have come to pass. Governmental entities and private parties alike have exploited the rise of commercial surveillance to circumvent privacy protections and leverage personal data, resulting in tremendous harms to affected individuals and communities. For example, a Freedom of Information Act lawsuit filed by the ACLU and New York Civil Liberties Union revealed "the millions of taxpayer dollars DHS used to buy access to cell phone location information… The documents expose the companies'—and the government's—attempts to rationalize this unfettered sale of massive quantities of data in the face of the U.S. Supreme Court precedent protecting similar cell phone location data against warrantless government access."[46]

---

[41] *See, e.g., Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197, 1206 (Ill. 2019); *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1274 (9th Cir. 2019).

[42] Crump & Harwood, *supra* note 24.

[43] Jay Stanley & Barry Steinhart, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, ACLU (Jan. 2003), https://www.aclu.org/sites/default/files/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf.

[44] Jay Stanley, *The Surveillance-Industrial Complex*, ACLU (Aug. 2004), https://www.aclu.org/other/surveillance-industrial-complex.

[45] *Id.*at 2.

[46] Press Release, ACLU, New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data (July 18, 2022), https://www.aclu.org/press-releases/new-records-detail-dhs-purchase-and-use-vast-quantities-cell-phone-location-data-0.

While companies profit from these exchanges (and thus the commercial surveillance that enable them), consumers are subject to a wide range of threats and harms:

- A recent study found that 99.1% of abortion clinic web sites contained a third-party tracker, raising the potential that third parties could "sell or share browsing data with law enforcement or civil litigants."[47]

- U.S. Immigrations and Customs Enforcement has used the location information purchased from data brokers to locate and arrest undocumented immigrants, evading Fourth Amendment protections that apply to non-citizens and citizens alike.[48]

- A Catholic priest resigned after a publication, using purchased data, "alleged he had regularly used the LGBTQ dating app Grindr and visited gay bars."[49]

- Individuals seeking access to unemployment insurance were forced to give their biometric identifiers to a private vendor, who misled the public about how it was using that data. The company initially said that it only used face recognition technology to perform one-to-one matches to verify unemployment insurance applicants' identities, but later revealed it was running people's faceprints through one-to-many matches against large databases, and collecting other sensitive information including location.[50]

3. Commercial Surveillance Renders Consumers Vulnerable to Data Breaches

In additional to voluntary disclosures by companies, consumers subject to commercial surveillance are at risk of harm from involuntary disclosure of their personal data through a data breach. Companies argue, not without reason, that data breaches are not wholly preventable: while some are caused by failure to implement basic security practices, others occur despite significant efforts to thwart would-be attackers.

True though this may be, it ignores one critical element: the true victims of consumer data breaches, the consumers, are often impacted because their data was collected without their consent via commercial surveillance. The best protection against consumer data breaches is to minimize the amount of consumer data collected or retained in the first place. Commercial surveillance, however, aims for the opposite, encouraging the collection of vast stores of information and sharing or selling that information widely. Even in circumstances where companies have followed reasonable data security practices, they are still culpable for their choice to collect data through commercial surveillance and

---

[47] Ari B. Friedman et al., *Prevalence of Third-Party Tracking on Abortion Clinic Web Pages*, 182 JAMA Internal Med. 1221 (Sept. 8, 2022), https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/2796236.

[48] Nathan Freed Wessler, *The U.S. Government Is Secretly Using Cell Phone Location Data to Track Us. We're Suing.,* ACLU (Dec. 2, 2020), https://www.aclu.org/news/immigrants-rights/the-u-s-government-is-secretly-using-cell-phone-location-data-to-track-us-were-suing.

[49] Madeleine Carlisle, *How the Alleged Outing of a Catholic Priest Shows the Sorry State of Data Privacy in America*, Time (July 23, 2021), https://time.com/6083323/bishop-pillar-grindr-data/.

[50] *See* Jay Stanley & Olga Akselrod, *Three Key Problems with the Government's Use of a Flawed Facial Recognition Service*, ACLU (Feb. 2, 2022), https://www.aclu.org/news/privacy-technology/three-key-problems-with-the-governments-use-of-a-flawed-facial-recognition-service; Drew Harwell, *ID.me Gathers Lots of Data Besides Face Scans, Including Locations. Scammers Still Have Found a Way Around It*, Wash. Post (Feb. 11, 2022), https://www.washingtonpost.com/technology/2022/02/11/idme-facial-recognition-fraud-scams-irs/.

retain it. The less information a company possesses, the less harm will flow from any breach.

4. Commercial Surveillance Exacerbates Power Imbalances, Harming Consumers as a Whole

In any negotiation or confrontation, information is power. Understanding the other party's motivations, limitations, and likely responses provides a dramatic advantage. Commercial surveillance serves to widen the information gap between consumers and companies, to the inherent detriment of consumers.

The trajectory of targeted advertising provides a clear example of the harms of this practice. While presenting consumers with "ads relevant to [their] interests" may in fact be desirable to many consumers, few are likely to appreciate the use of their personal data to determine not merely what they might want to purchase but whether they are identified as "gullible"[51] or targeted precisely when they are most vulnerable to pitches[52]—yet that is precisely what targeted advertising is increasingly capable of accomplishing without regulation. Location information has also been used for targeting purposes, including location-based pricing that appears to be racially discriminatory.[53]

5. Commercial Surveillance Specifically Targets and Disproportionately Harms Marginalized Communities

As the Commission has long recognized, and as discussed further in Section III of this comment, the harms of unfair and deceptive practices are not distributed equally.[54] Like too many other harms, they fall disproportionately on populations that are already marginalized or disadvantaged, in part because these communities often lack the resources to defend themselves or otherwise protect their own interests.

Commercial surveillance exploits precisely this lack when it targets communities of color, low-income consumers, and other marginalized groups. Notice-and-choice privacy "protections" fail most egregiously with those groups that often lack the technological sophistication, support networks, and other resources to engage in even the limited self-protection available. They must "navigate a matrix of privacy and security vulnerabilities in their daily lives" while at risk of more severe consequences if their information is misused.[55]

---

[51] *See* Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. Times (May 20, 2007), https://www.nytimes.com/2007/05/20/business/20tele.html.

[52] *See* Joanna Syrycharz & Bram Duivenvoorde, *The Exploitation of Vulnerability Through Personalised Marketing Communication: Are Consumers Protected?*, 10 Internet Pol'y Rev. 1 (2021), https://policyreview.info/articles/analysis/exploitation-vulnerability-through-personalised-marketing-communication-are.

[53] Julia Angwin, Surya Mattu & Jeff Larson, *The Tiger Mom Tax: Asians Are Nearly Twice as Likely to Get Higher Price from Princeton Review*, ProPublica (Sept. 1, 2015), https://www.propublica.org/article/asians-nearly-twice-as-likely-to-get-higher-price-from-princeton-review.

[54] 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* (Oct. 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.

[55] Mary Madden, *The Devastating Consequences of Being Poor in the Digital Age*, N.Y. Times (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html.

Rather than receiving heightened protections, these groups have too often experienced the opposite: focused efforts to invade their privacy specifically to exploit their vulnerabilities. Consumers are singled out on account of their religion, race or ethnicity, sexuality, or socioeconomic status and their data marketed to precisely those groups who seek to harm them on that basis:

- Muslim Americans have been singled out for commercial surveillance "aimed at monetizing the special value of location data that is specific to the Muslim community."[56]
- As noted above, renters—who are disproportionately lower-income and Black or Brown—are increasingly subject to commercial surveillance in their own homes.[57]
- Black Lives Matters protesters have been subject to social media surveillance by companies seeking to market that information to state law enforcement agencies seeking to monitor First Amendment-protected activities.[58] Major social media platforms including Facebook, Instagram, and Twitter sold data to these companies until called out by the ACLU and other organizations.
- Low-income consumers are also particularly vulnerable to—and targeted by—exploitative data practices that take advantage of their lack of resources and alternatives.[59] They also may be negatively impacted by algorithmic pricing and similar practices.[60]

As discussed further in Section III, commercial surveillance also provides both training data for the development of algorithmic decision-making models and the inputs fed into those models. These models consistently reproduce historical biases, leading to adverse outcomes in the context of housing, employment, credit, education, medical treatment, and more.

D. Commercial Surveillance Harms That Are Hard to Recognize or Measure Must Still Be Taken into Account

Related Questions:

5. Are there some harms that consumers may not easily discern or identify? Which are they?

6. Are there some harms that consumers may not easily quantify or measure? Which are they?

7. How should the Commission identify and evaluate these commercial surveillance harms or potential harms?

---

[56] Complaint, *In re Request for Investigation of Alleged Violations of Section 5 of the FTC Act by Multiple Actors in the Location Data Industry* (Apr. 12, 2022), https://www.cair.com/wp-content/uploads/2022/04/FTCcomplaint.pdf.

[57] *See, e.g.*, Sarina Trangle, *Privacy Concerns Mount Over Tech-Based Apartment Building Access*, AM N.Y. Metro (Sept. 22, 2019), https://www.amny.com/real-estate/apartment-access-privacy-concerns-1-29927187/, *and* Hiawatha Bray, *In Smart Apartments, Is Tenants' Privacy For Rent?*, Bos. Globe (Feb. 11, 2020), https://www.bostonglobe.com/2020/02/11/business/smart-apartments-is-tenants-privacy-rent/.

[58] *See* Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access to 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.

[59] Michele Gilman, *Voices of the Poor Must Be Heard in Data Privacy Debate*, Jurist (May 14, 2019), https://www.jurist.org/commentary/2019/05/voices-of-the-poor-must-be-heard-in-the-data-privacy-debate/.

[60] *See* Jennifer Valentino-DeVries, Jeremy Singer-Vine & Askhan Soltani, *Websites Vary Prices, Deals Based on Users' Information*, Wall St. J. (Dec. 24, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

Of the harms noted above, several are difficult for consumers to recognize and/or measure. This does not, however, indicate that such harms are less significant. Instead, it points to the same issue as commercial surveillance practices themselves: consumers are often denied full knowledge of the risks and harms they face to minimize their desire or ability to respond.

It is critically important that the Commission address these harms, leveraging its own research and investigations as well as public-interest resources to drive home the message that harms that are difficult to perceive or quantify are not therefore exempt from its mission. Policymaking is often driven by demonstrable harms arising from high-profile incidents, but because the collection and use of personal information often proceeds surreptitiously and because the harms of abusive practices may come to light years down the line, if at all, consumers are poorly served by such reactive policymaking. Moreover, hindrances ranging from class-action barriers and standing doctrine barring legal recourse, to the dramatic power imbalance between consumers and corporations, end up precluding other remedies under existing law. FTC rulemaking provides a rare opportunity to *proactively* take on surveillance practices that substantially harm consumers and society as a whole.

1. Consumers Face Numerous Obstacles that Impede Their Personal Understanding of Many Commercial Surveillance Harms

Commercial surveillance is a tremendously complex enterprise, with dozens or even hundreds of trackers on a single web site and many thousands of entities seeking to buy, sell or use consumer data. The sheer scope makes it virtually impossible for individual consumers to understand how their data is collected and used, which not only renders "opt-out consent" a fallacy but also makes it difficult for users to discern the full range of actual consequences. As a result, consumers are most aware of harms that directly and obviously impact them personally or that accrue the most attention.

Harms may fail either or both of these for various reasons. Some are inherent in the harm itself: where commercial surveillance serves to influence, rather than outright constrain, consumers, it may be difficult both to recognize and to determine whether or to what degree it succeeded. But many harms—including harms of discrimination and biased algorithmic decisionmaking discussed further in Section III below—are hard to recognize because commercial surveillance actors take pains to disguise them, concealing the fact of surveillance at all or preventing an understanding of its impact. As such, it is particularly important that the Commission strive to understand and address harms that consumers at an individual level cannot.

a. Consumers Are Prevented from Recognizing Harms from Concealed Commercial Surveillance

Perhaps most obviously, consumers will be unlikely to recognize that a given outcome is the result of commercial surveillance if they are unaware that the commercial surveillance occurred. Even knowing that personal data was involved in the harm does not necessarily point the consumer at the source of the data and thus origin of the harm, particularly if the data at issue has passed through the hands of multiple data brokers or other third parties.

b. Consumers Are Prevented from Recognizing Downstream Harms

Even when consumers know that their data is being gathered by the website, mobile app, or other service they are using, they are overwhelmingly denied knowledge of where that data might travel after the fact, something no browser plugin or other consumer-facing solution can address. Even consumers sufficiently motivated to pore through privacy policies find at best broad generalizations of third parties that might receive their information: "business partners," "advertisers" and other rough sketches that

provide neither specific recipients nor even the number of third parties on the receiving end of consumer data transfers.

c. Consumers May Struggle to Recognize Harms Associated with Fundamental Rights

Ascertaining the true cost of identity theft or another concrete injury is often challenging enough. It is more difficult to quantify the impact of privacy violations on autonomy or dignity, or even to definitively recognize the harm. Is a teenager's decision not to seek online information about sexuality ascribable—wholly? partly?—to the chilling effects of commercial surveillance and the recognition that their search could potentially be exposed? Even if so, or if the harm is more apparent—such as the actual exposure of such information—how can it be measured?

d. Consumers May Struggle to Recognize Pervasive Small Harms

Harms that fall below a certain threshold are unlikely to even be noticed by consumers grappling with the inherent complexity of the modern world. This renders consumers vulnerable to a constant barrage of minor impingements that cumulatively cause them significant harm. For example, while consumers may howl in outrage at rideshare surge prices that vastly exceed the routine fare, it is much harder to recognize how price discrimination driven by consumer data subtly but persistently affects spending on everyday products[61] —even though the latter may have a more profound impact on many households' financial situation.

e. Consumers May Struggle to Address Harms Separated in Time from Privacy Violations

In many instances, harms arising from a privacy violation occur long after the violation itself. This presents two practical challenges for consumers. First, if they learn of the privacy violation, they may not understand the full scope of harms that it will eventually cause.[62] More commonly, however, consumers encounter the harms without prior knowledge that a privacy violation occurred. In that situation, a gap in time may make it difficult for consumers to connect the harm to misuse of their personal data at all, let alone to ascribe it to a specific incident or the full set of involved actors.

f. Individual Consumers May Struggle to Recognize Collective Harms

Some privacy harms are best understood at the collective level rather than ascribed to a given individual. Consumer data may be used to develop automated decision-making systems that are then deployed to consolidate commercial power or facilitate other commercial practices that harm consumers as a whole or a particular group (typically, though not necessarily, one to which the consumer belongs).

This is particularly true where the harm at issue is the use of a person's data in contravention of their values or intentions but not in a way that results in direct harm to that person. Supporters of immigration reform almost certainly would object to the use of their personal data to build and fuel technologies marketed to ICE and other federal agencies, but even if they are aware of Clearview AI,

---

[61] *See* Daisuke Wakbayashi, *Does Anyone Know What Paper Towels Should Cost?*, N.Y. Times (Feb. 26, 2022), https://www.nytimes.com/2022/02/26/technology/amazon-price-swings-shopping.html.

[62] This may also be a barrier to obtaining legal relief.

they have no way of knowing whether the company violated their privacy by scraping social media photos to feed into its algorithm.[63] But the opacity of machine learning means even consumers who are directly harmed by a tool built on their own personal data may not be able to recognize that fact.

g. Even When Consumers are Aware of Harms, They May be Unable to Obtain Relief on their Own

Even when consumers surmount these barriers and suspect or know that their personal data was collected without consent, or was used to their detriment, it can be extraordinarily difficult to obtain relief. Some privacy statutes that prohibit nonconsensual collection or harmful use of personal data lack private rights of action.[64] And when there is a cause of action, consumers must still surmount statutes of limitations, federal pleading requirements and standing doctrine, difficulties proving damages from sometimes intangible harms, lack of resources to investigate such harms, arbitration requirements, class action bars, and other barriers to obtaining relief.

2. The Commission Should Seek to Identify and Measure Harms That Individual Consumers Cannot

One of the primary reasons that individuals may struggle to identify and measure harms is because they are individuals, and as such lack a wider lens with which to understand the overall data ecosystem, identify practices that adversely impact large numbers of consumers or are otherwise best discerned in the aggregate, and measure the impact of those practices.

In response, the Commission should leverage the resources at its disposal to surface harms that individuals are not equipped to recognize and ensure that they too are remedied. Regulations should squarely address commercial surveillance and other practices that violate privacy, be they "Facebook running psychological experiments on people, a company like Ever building a surveillance tool from billions of private photos, or menstrual-tracking apps being used to monitor employees."[65] The Commission should be careful not to sideline such issues simply because they are more difficult to identify or measure than other harms. This may require regulations that support Commission or other public interest research that helps to surface and evaluate these harms alongside rules designed to counteract them. The Commission should also provide easy and effective means for consumers to alert the Commission to data privacy and security harms those consumers have suffered, so that the Commission can take action when consumers are unable to themselves.

Indeed, given the barriers to recourse for consumers facing these sorts of harms—from prohibitions on class-action suits that deter remedies for small-but-persistent harms to legal doctrines that require demonstration of economic consequences—FTC regulations present a rare opportunity to ensure that these harms are addressed. The Commission's long expertise with investigating commercial practices, comprehending the full scope of consequences they impose, and crafting rules that holistically address them are particularly needed to address precisely those harms that offer consumers little other recourse.

---

[63] *See* Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[64] *See, e.g.*, Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1311; Biometric Identifiers, Wash. Rev. Code § 19.375.030(2).

[65] Jacob Snow, *Your Personal Information is Yours, Not the Raw Material for Surveillance Technology*, ACLU of Northern California (May 09, 2019), https://www.aclunc.org/blog/your-personal-information-yours-not-raw-material-surveillance-technology,

E. FTC Enforcement Has Limitations that Trade Regulation Rules Should Rectify

Related Questions: *8. Which areas or kinds of harm, if any, has the Commission failed to address through its enforcement actions?*

9. Has the Commission adequately addressed indirect pecuniary harms, including potential physical harms, psychological harms, reputational injuries, and unwanted intrusions?

The ACLU has supported and appreciated the Commission's enforcement efforts over the years, including actions that have address specific harmful practices. That said, limitations on the Commission's enforcement authority have allowed other harmful practices to continue. We encourage the Commission to utilize its unfairness and deception authorities to address systemic commercial surveillance practices that harm consumers, including those that do not include direct pecuniary harms or are otherwise difficult for consumers to recognize and mitigate.

1. The Commission Should Require Consumer-Facing Services to Address Downstream Harms

The Commission has primarily targeted its enforcement actions at "bad actors": the participants in the commercial surveillance flow that breach their promises or directly harm consumers. This approach runs the risk of letting the consumer-facing services that provided the bad actors with access to consumer data in the first instance off the hook. In doing so, it fails to incentivize those services to interrogate their business partners to ensure that they protect consumer privacy.

As one example of this, in 2012 the Commission announced a settlement with Epic Marketplace in response to the company's exploitation of "history-sniffing" to collect information about previously visited websites.[66] The Commission did not, however, address the "failure by [websites that partnered with Epic Marketplace, including] CNN, Orbitz and the Red Cross to police the behavior of the advertising companies they partner with, and an unwillingness to protect the privacy of their own customers."[67]

The Commission's deception authority is an insufficient tool to address consumer-facing products that make few claims about downstream uses of data. The Commission's unfairness authority, as it currently exists as well as incorporated into trade regulation rules, provides a preferable approach.

2. The Commission Should Address the Potential for Consumer Harm via Government Surveillance

Relatedly, the Commission should recognize that the disclosure of consumer data to government entities can lead to dramatic adverse effects for consumers, and thus address commercial surveillance marketed to government actors as a practice that puts consumers at risk. Entanglement between

---

[66] Press Release, Fed. Trade Comm'n , FTC Settlement Puts an End to "History Sniffing" by Online Advertising Network Charged with Deceptively Gathering Data on Consumers, (Dec. 5, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/12/ftc-settlement-puts-end-history-sniffing-online-advertising-network-charged-deceptively-gathering.

[67] Chris Soghoian, *FTC Busts Advertisers in Browser Snooping Scandal, But Web Sites Shouldn't Be Off the Hook*, ACLU (Dec. 5, 2012), https://www.aclu.org/news/national-security/ftc-busts-advertisers-browser-snooping-scandal-web-sites-shouldnt-be-hook.

commercial actors and state or local law enforcement agencies would be a sensible place to focus, given the sheer number of local actors, and the relative lack of other accountability mechanisms at that level.

As the ACLU has long documented, government surveillance subjects consumers—especially activists, immigrants and others in marginalized communities—to increased scrutiny and numerous potential consequences, increasingly based on nothing more than digital profiles sourced via commercial surveillance.[68] It was heartening to see Commissioner Wilson raise such concerns, noting the lack of constitutional protection against warrantless collection of information subject to the "third-party doctrine" and the need to address the "linkage between large-scale collection of consumer data in the commercial arena and the potential for watering down Americans' civil liberties."[69] Rulemaking and enforcement activity should address government surveillance of consumer data conducted without judicial oversight as a harm to consumers, and the Commission should focus on companies that enable indiscriminate or warrantless surveillance in enforcing the FTC Act's prohibitions on unfair and deceptive business practices.

3. The Commission Should Address Unwanted Intrusions and Harms to Dignity and Autonomy

As noted above, the fact that harms to fundamental rights are difficult to quantify does not mean that they are of lesser importance. In fact, the opposite may be true: emphasizing the inherent harm in non-consensual commercial surveillance may allow the Commission to erect more comprehensive protections for privacy than focusing on specific harmful uses of consumer data.

In particular, embracing a definition of "harm" that extends beyond immediate physical or economic consequences would make it clear that misuse of consumer information is inherently an unfair business practice, thus ensuring the Commission's authority over actors that avoid making false statements about their practices by concealing their activities altogether. The Commission has already made progress in this direction in its recent enforcement actions addressing concealed spyware, asserting that the failure to ensure that products were used "only for legitimate and lawful purposes" was an unfair act.[70] The same is true of the collection, use, and sale of data: any actions that lacks a legitimate basis—not just violations of "notice-and-choice" consent for activities that risk harming consumers—should be presumptively unfair.

4. The Commission Should Learn from and Build Upon Its Kochava Enforcement Action

Many of these concerns are clearly reflected in the Commission's recent enforcement action against Kochava.[71] As the Commission's complaint makes clear, Kochava's sale of geolocation data has exposed sensitive data about consumers that raise many of the concerns expressed above:

- Sale of data concerning reproductive health clinic visits is particularly concerning given the

[68] *See, e.g.*, Cagle, *supra* note 38.

[69] Letter from Christine S. Wilson, Fed. Trade Comm'n Commissioner, to Sen. Ron Wyden (May 21, 2021), https://www.ftc.gov/system/files/documents/public_statements/1590440/wilson-fourth-amendment-wyden.pdf.

[70] Complaint, *In re Support King, LLC, and Scott Zuckerman*, No. 192 3003 (F.T.C. Aug. 21, 2022), https://www.ftc.gov/system/files/documents/cases/192_3003_spyfone_complaint.pdf.

[71] *See* Press Release, Fed. Trade Comm'n, FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

reversal of *Roe v. Wade* and subsequent criminalization of abortion in many states. Exposing data linking staff and patients to these clinics enables harms from law enforcement as well as private parties—even if the tracked individuals' actions were fully legal.

- Tracking data about places of worship chills the free expression of religion by subjecting practitioners to additional scrutiny
- Exposing individuals who pursue help in recovering from addiction can discourage them and others from receiving the treatment and support they need.
- Linking consumers to homeless and domestic violence shelters can expose them to physical threats from abusers who use it to track them down, to reputational consequences and emotional harm, or to predatory business practices that target them precisely due to their vulnerability.
- Commission enforcement action is particularly important because individual consumers are unlikely to be aware of this surveillance, and even if they were aware, any single consumer would be hard-pressed to demonstrate the concrete likelihood of any particular harm.

The Commission should continue to pursue enforcement against Kochava as well as other entities pursuing exploitative commercial surveillance practices. Promulgating regulations will help solidify the Commission's authority and means to pursue such actions, and will put actors on clear notice of meaningful constraints on commercial surveillance.

II. Trade Regulation Rules Should Be Informed by, but not Limited to, Harms Arising from Commercial Surveillance Involving Biometric and Location Data

Related Questions: *10. Which kinds of data should be subject to a potential trade regulation rule? Should it be limited to, for example, personally identifiable data, sensitive data, data about protected categories and their proxies, data that is linkable to a device, or non-aggregated data? Or should a potential rule be agnostic about kinds of data?*

38. Should the Commission consider limiting commercial surveillance practices that use or facilitate the use of facial recognition, fingerprinting, or other biometric technologies? If so, how?

Some proposals have sought to regulate commercial surveillance based on the sensitivity of the data at issue: if abuse of more sensitive data might result in more dire harms, the thinking goes, then regulation can impose stricter limitations on collection and use of "sensitive" data and use a lighter touch elsewhere. These proposals are not sound. Although, as discussed below, the obvious sensitivity of some kinds of data illustrates the urgent need for more robust protections, any regulatory regime that tries to provide different levels of protection to "sensitive" and "non-sensitive" data will fail to adequately protect consumers. That is both because any attempt to enumerate "sensitive" categories of data is likely to become obsolete as technology advances, and because the entire point of mass aggregation and processing of consumer data is to infer revealing (and often sensitive) information from many data points that, when viewed individually, reveal little.

With that in mind, there are some types of information, such as biometric and location data,[72] that are particularly sensitive and prone to abuse and misuse. Biometric and location data both provide a way to bring real-world activities into the commercial surveillance ecosystem, and in doing so threaten to expose a vast amount of information that would otherwise be difficult to infer: romantic relationships, daily habits, religious practices, political activities, health care needs, and many others. Moreover, the use of biometric and location data is particularly difficult for consumers to control; consumers rarely leave their phones behind and literally cannot change their biometric markers, and both can be tracked and recorded silently. The combination of heightened potential for harm and lack of consumer consent indicate that commercial surveillance based on biometric or location data should be squarely in the Commission's sights as it prepares regulations.

Recognizing these harms, it remains critical that the Commission's rules and enforcement actions not be tied exclusively to protecting biometric or location data. There are two fundamental reasons for this. First, tying rules explicitly to the data and technologies of today leaves the rules vulnerable to obsolescence when new technologies emerge; face recognition and other surveillance practices centered on biometric data are themselves a recent invention, after all. In addition, targeting specific data types for regulation may be ineffective as commercial surveillance practices shift to using proxies for that data, whether explicitly or by leveraging machine learning to attempt to replicate prior results using other data. And there may be contexts in which "non-sensitive" data presents as much risk of harm as location or biometric data; for example, location data can reveal a person's visits to locations providing sensitive, private, or embarrassing services, but so can Internet browsing history.

Because there are few, if any, contexts in which location or biometric data present a low risk of harm, the Commission must ensure that its rules adequately regulate—which in many cases may mean curtail—commercial surveillance practices built around location or biometric data, even as it ensures that its rules provide robust protections well beyond these two types of data.

A. Commercial Surveillance of Location Data Harms Consumers in Many Ways

Location data is about places. Nominally, place is indicated with positional coordinates, a latitude, longitude, and possibly altitude that indicate a specific point on the globe, derived from one of several technological mechanisms with varying degrees of accuracy, combined with a timestamp indicating precisely when the device was there.[73] It is collected automatically, and in many cases constantly.

---

[72] For purposes of this comment, by "location data" we mean data generated by and obtained from a computer or other electronic device, most commonly a mobile device. This is, of course, not the only way to track a consumer's location. Biometric data can serve that purpose, as described below; so can other tools, such as automated license plate readers and social media surveillance. The degree to which data is fungible is a major factor in our recommendation that regulations not be limited to specific forms of data such as location or biometric data.

[73] For a mobile device, location data is generally derived from one or more of the following:

1. Global Positioning System (GPS) reckoning, which derives the device's location based on signals received from orbital satellites.
2. Wi-Fi Triangulation, which derives location from the availability and signal strength of nearby wireless networks.
3. Cell Site Location data (CSLI), which derives location from the distance and direction of nearby cell towers.

In addition, mobile devices may communicate with local Wi-Fi and Bluetooth devices, exposing their proximity to those devices in the process.

For commercial surveillance purposes, location data is typically not about coordinates and timestamps but a "point of interest." What makes a particular point "interesting" may vary. It may be the site of a restaurant or a strip club. It may be the site of a baseball game or political rally that was happening at a specific time and place. Or it may be the other people who were there. But it is rarely just a point on a map.

There is one prominent exception to the above: the raw coordinates contained in a trove of location data allow surveillance practitioners to combine data sets containing location data by identifying matches. Despite the assertion by data brokers that the data they sell is "anonymized," location data is in fact highly (re-)identifiable.[74] Location data can be linked to other location data based on only a few records, most commonly a consumer's home and/or work location. Efforts to dispute this fact serve primarily to confuse consumers about the true impact of location surveillance.

In other words, location data is, in many senses, a comprehensive record of a consumer's life, containing information about their activities, associations, and more. For that reason, its collection and disclosure puts consumers at significant risk of harm.

1. Commercial Location Surveillance Causes Numerous Harms to Consumers

Because location data can reveal so many details about an individual's life, commercial surveillance involving location data creates countless opportunities for harm, including both harms to individual consumers and societal harms.

First, the surveillance of location data creates the risk that the information will be publicly exposed, putting consumers at risk of both emotional harm and adverse responses from others. Location data can reveal:

- That a Catholic priest visited a gay bar, forcing him to resign.[75]
- That a consumer is grappling with cancer based on visits to a chemotherapy center.[76]
- That a consumer has recently spent the night at a domestic violence shelter—and which one.

As the Commission itself has recognized, the revealing nature of location data exposes individuals "to stigma, discrimination, physical violence, emotional distress, and other harms."[77]

These harms are particularly acute for people experiencing or trying to disengage from violent domestic relationships, those targeted by stalkers, and people subjected to threats and harassment due to their political or social views or their race, sexuality, or gender. They are also presently heightened

---

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

[75] Carlisle, *supra* note 49.

[76] *See* Anya E. R. Price, *Location Data Are Revealing Health Information* (Aug. 19, 2021), https://www.theregreview.org/2021/08/19/prince-location-data/.

[77] Press Release, Fed. Trade. Comm'n, FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

for both patients seeking reproductive healthcare and providers who offer abortion services. The *Dobbs v. Jackson Women's Health Organization*[78] ruling and the subsequent criminalization of basic health care in many states—and the ensuing threat of harassment or worse from private individuals—is a timely example of why location data, and the detailed information that can be drawn from it, is so dangerous.

More broadly, the sale of location data jeopardizes the exercise of many constitutional rights, including First Amendment rights. Consumers who wish to attend a pro-choice rally, a gun show, or a mosque cannot do so without that fact being available for purchase and added to their permanent record. Purchasers include state and federal law enforcement agencies, raising serious questions about circumvention of Fourth Amendment protections against warrantless cell phone location tracking by police.[79]

This risk creates a more immediate threat: that consumers will respond by simply choosing not to engage in activities that could cause harm if revealed. As surveillance expands into the real world, so do its chilling effects, discouraging consumers from attending addiction support meetings, pursuing romantic relationships, or otherwise exercising their rights without fear of retaliation.

2. Commercial Surveillance Involving Location Data Lacks Adequate Safeguards

Despite the risks posed by location data, there have been few efforts to constrain its collection, use and disclosure. Courts have recognized the significance of location data; in particular, in *Carpenter v. United States*, the Supreme Court held that cell phone location data merited greater protection under the Fourth Amendment than at least some other information collected and held by third parties.[80] That decision was grounded both in the intimate details that location data exposes and in the practical impossibility of avoiding the current commercial surveillance practices that result in its collection.

But, to date, the location data market has made few changes in response. Apart from the Commission's recent enforcement action against Kochava, no federal law has been used to challenge the practice of collecting vast amounts of location data about adults for commercial purposes. And corporate practices have by and large remained unchanged, continuing to broker vast amounts of data while cutting consumers out of the loop; even when users turn location services off in their iPhone settings, companies are using SDKs to collect it anyway.[81]

All of this activity amounts to a market estimated at $12 billion a year, in which data brokers "boast about the scale and precision of the data they've amassed" while concealing their practices from the consumers whose data they collect.[82] In other words, it is a regime in need of significant attention as the Commission prepares its trade regulation rules.

---

[78] 142 S. Ct. 2228 (2022).

[79] *See, e.g.*, *ACLU v. Dep't of Homeland Sec'y*, No. 1:20-cv-10083-PGG (S.D.N.Y. filed Dec. 3, 2020), document productions available at https://www.aclu.org/cases/aclu-v-department-homeland-security-commercial-location-data-foia.

[80] 138 S. Ct. 2206 (2018).

[81] Alfred Ng & Jon Keegan, *Who is Policing the Location Data Industry?*, The Markup (Feb. 24, 2022), https://themarkup.org/the-breakdown/2022/02/24/who-is-policing-the-location-data-industry. For a similar example, see Bryan Pietsch, *Google Reaches Record $392M Privacy Settlement Over Location Data*, Wash. Post (Nov. 15, 2022), https://www.washingtonpost.com/technology/2022/11/15/google-privacy-settlement-location-data/.

[82] John Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, The Markup (Sept.30, 2021), https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.

B. Face Recognition and Other Surveillance Practices Using Biometric Data Harm Individuals in Similar Ways

If location data is about places, biometric data is about people. Again, however, the value of biometrics, at least in the commercial surveillance context, is not in the raw data (typically a mathematical model of some physical characteristic, such as a faceprint, voiceprint or retina scan) but its power to link a consumer to places, events or other people.

As a result, biometric surveillance raises much the same set of concerns as location surveillance. But its unique characteristics also surface other threats—and may require a different regulatory approach to address the fact that biometric surveillance is more commonly offered as a service than as raw data available for purchase.

1. Collection of Biometric Identifiers Raises Substantial Risks to Consumers

Biometric identifiers are typically used in two distinct ways. First, they can be used as authenticators, to limit access to appropriate parties, such as fingerprint and face recognition tools used to unlock smartphones. Second, they can be used to try to identify a given person by comparing captured or extracted biometric information against a database, such as automated tools that tag photos with the names of people therein.

Both of these approaches require the collection or creation of biometric information about consumers. As a result, they create the risk that those faceprints, fingerprints or other biometric identifiers may be misused, resold, or lost in a data breach. And the theft or abuse of a biometric identifier is particularly harmful because those identifiers are immutable. As one writer put it when addressing the breach of 5.6 million fingerprint records held by the Office of Personnel Management, "[w]hen hackers steal your password, you change it. When hackers steal your fingerprints, they've got an unchangeable credential that lets them spoof your identity for life."[83] Moreover, while password management tools allow users to use a different password for each site, limiting the impact of a single data breach, biometric identifiers are typically used across sites. And while biometric authentication has been viewed as difficult to hack, advances in technology make that challenge (among many others) easier over time.[84]

The use of biometric identifiers in any context also raises concerns about inaccuracy and bias. Face recognition algorithms in particular have consistently failed to perform as well on darker-skinned faces as lighter-skinned.[85] As a result, the ACLU has noted that biometric technologies "can lead to significant civil rights violations, including false arrests and denial of access to benefits, goods, and

---

[83] Andy Greenberg, *OPN Now Admits 5.6m Feds Fingerprints Were Stolen by Hackers* (Sep. 23, 2015), https://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/.

[84] *See id.* (noting that "hackers' ability to exploit the stolen fingerprints 'could change over time as technology evolves.'").

[85] *See, e.g.*, Joy Buolamwini et al., *Gender Shades*, MIT Media Lab, https://www.media.mit.edu/projects/gender-shades/overview (last visited Nov. 16, 2022).

services. These problems disproportionately affect people of color and members of other marginalized communities."[86]

Some biometric systems also purport to extract more than just the identity of the data subject from their biometric data. Technology vendors increasingly assert that biometric data can be used to recognize emotion or affect, despite decidedly "shaky evidence" in support.[87] Others promise to detect "suspicious activity" or distinguish truth from lies—a notoriously unreliable pursuit.[88] As with misidentifications, though inaccurate inferences drawn from biometric analysis can lead to harm for any consumer, both inaccuracies and resulting harms will be more frequent and severe for members of Black and other underrepresented communities.[89]

Finally, biometric identifiers collected for authentication purposes can all too easily be used for identification and surveillance purposes. The ACLU and its partners' opposition to the use of ID.me's face recognition tools was grounded in part in the fact that ID.me claimed it used only one-to-one recognition (which provides a yes/no answer as to whether the face matches a specific record) when in fact it also used a one-to-many form of recognition that allows linking to any record in a potentially-vast database.[90] Doing so raises the same concern as many other practices discussed in this Comment: it takes data collected for a specific purpose that is purported to benefit consumers and reuses it in unexpected ways to further commercial surveillance.

2. Commercial Biometric Surveillance Causes Numerous Harms to Consumers

The second way that biometric identifiers can be used is to "look up" an unidentified consumer in a database comprised of biometric data. Doing so enables commercial surveillance by associating that consumer with the place, group or event in which they were observed, again allowing data collection to expand to the real world.

Biometric surveillance raises many of the same concerns as location surveillance. As the ACLU has previously noted, "biometric technologies pose severe threats to civil rights and civil liberties by enabling privacy violations—including loss of anonymity in contexts where people have traditionally expected it [and] persistent tracking of movement and activity."[91] Like location surveillance, using biometric identifiers to track real-world activities can reveal individuals' social networks, sexual orientation, political affiliation, diet and exercise habits, and more. Both the potential exposure of such data and the chilling effects arising from the mere collection and use of intimate information harm consumers.

Biometric surveillance imposes additional risks distinct from those generally associated with location data. First, biometric surveillance can be even more difficult to recognize and respond to than

---

[86] *See* ACLU Letter to Office of Sci. & Tech. Policy re: Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies (FR Doc. 2021-21975) (Jan. 14, 2022), https://www.ai.gov/rfi/2022/86-FR-56300/ACLU-Biometric-RFI-2022.pdf. (hereinafter "ACLU Letter to OSTP re: Public and Private Sector Uses of Biometric Technologies").

[87] Kate Crawford, *Artificial Intelligence is Misreading Human Emotion*, The Atlantic (Apr. 27, 2021), https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/.

[88] *See* ACLU Letter to OSTP re: Public and Private Sector Uses of Biometric Technologies, *supra* note 86.

[89] *See* Lauren Rhue, *Racial Influence on Automated Perceptions of Emotion* (Dec. 6, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765.

[90] ACLU et al., *A Call to Federal and State Agencies to End the Use of ID.me and Other Facial Recognition Identity Verification Systems* (Feb. 14, 2022), https://www.aclu.org/sites/default/files/field_document/coalition-letter-id.me-and-face-verification-feb2022.pdf.

[91] ACLU Letter to OSTP re: Public and Private Sector Uses of Biometric Technologies, *supra* note 86.

location surveillance. Location surveillance operates through the mobile phone operating system and app ecosystem, and as such is at least subject to some forms of identification and analysis, even if individual consumers lack the expertise to identify or analyze it. Remote deployment of face or gait recognition, on the other hand, is all but impossible to detect: if a hidden camera matches your face with a biometric database, consumers have absolutely no indication that they are being tracked.

The scope of biometric surveillance also extends further, at least in some ways, than that of location surveillance. While face recognition cameras are not ubiquitous (at least in the U.S.) and thus may not track individuals as pervasively as mobile location data, face recognition also can be deployed to discern individuals' past activities from the ever-increasing trove of online photos. Biometric surveillance systems can exploit the availability of photographs online, using proprietary algorithms to extract faceprints and other biometric identifiers from those photos, and thus amassing a type of information (biometrics) and a surveillance potential that few individuals would have contemplated when posting a family photo on social media or providing a headshot for a company's employee directory page.[92]

3. Commercial Biometric Surveillance Lacks Meaningful Safeguards Against Harms

Like location surveillance, the use of biometric identifiers to surveil consumers is largely unregulated. And while the emergence of biometric surveillance is relatively new, the example of location surveillance suggests that biometric surveillance is unlikely to organically self-regulate to protect consumers from harm.

The need for strong regulation of biometric surveillance is reflected in robust efforts by state and local lawmakers seeking to curtail abuses. Many local governments have banned or sharply curtailed government use of certain biometric technologies.[93] Others, including the state of Illinois, have strictly regulated the nonconsensual collection and use of biometric information by private parties.[94] The ACLU recently settled a lawsuit with Clearview AI requiring the company to comply with the Illinois Biometric Information Privacy Act's provisions—nationwide.[95]

C. Trade Regulation Rules Should Address, but Not Be Tied Exclusively to, Commercial Location and Biometric Surveillance

Despite these efforts, the commercial use of biometric information continues to proliferate. As it grows, so does the need for effective protections for consumer privacy. The Commission should ensure that its rules adequately address the harms and challenges presented by biometric information and particularly commercial biometric surveillance.

Many data privacy laws offer heightened protection for "sensitive" data, which frequently

---

[92] *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[93] *See, e.g.*, Siladitya Ray, *Boston Bans Municipal Use Of Facial Recognition*, Forbes (June 24, 2020), https://www.forbes.com/sites/siladityaray/2020/06/24/boston-bans-municipal-use-of-facial-recognition/?sh=4f3d8d80286f.

[94] Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1—14/25.

[95] Press Release, ACLU, In Big Win, Settlement Ensures Clearview AI Complies with Groundbreaking Illinois Biometric Privacy Law (May 9, 2022), https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois.

includes both location and biometric information, among other categories.[96] The logic behind such categorization is self-evident, if misguided: if certain types of data present the greatest risk to consumers, then strictly regulating those data types while allowing greater use of others appears to be a calibrated policy response.

The ACLU has opposed, and continues to oppose, comprehensive privacy rules that take such a two-tiered approach.[97] There are several reasons that this approach is inadvisable.

First, as the examples of location and biometric data show, some categories of data could be considered "sensitive" by virtue of the wide range of harms that the improper collection, use, or disclosure of that data may trigger. While it is true that few other data types so clearly link so many real-world activities with digital profiles, it does not follow that profiles that consist of vast quantities of "non-sensitive" data will not do so. Limiting rules to location and biometric data may thus fail to address even the specific harms most closely associated with those data types.

Moreover, restrictions or prohibitions on specific categories of data can often be circumvented by proxies and inferences. Limitations on the explicit use of protected characteristics does not preclude outcomes that correlate strongly with those, including results that disparately impact protected classes. Instead, information like zip codes continue to serve as proxies for race, allowing the "digital redlining" that privacy laws explicitly protecting protected characteristics seek to prevent.[98] Even location itself may be derived from social media surveillance, purchase records, transit toll or fare payments, and the vast amount of other data available in the commercial surveillance ecosystem.

Attempting to address proxies eliminates the clear distinction between "sensitive" and "non-sensitive" data entirely. Doing so is particularly problematic in the context of machine learning, where it is typically impossible to know whether a model has implicitly derived proxies for protected categories even if such data was entirely excluded from its training set.

We believe that the best approach to protecting consumer privacy is to impose strong basic requirements for all data, coupled with context-specific decisions about privacy and security safeguards that consider the potential ways that the practices or data at issue benefit or harm the consumer. As stated previously, trade regulation rules should, at minimum:

- Ensure that **harmful data uses are prohibited.**
- **Impose purpose limitations and data minimization requirements** that prevent exploitation of consumer data for purposes unrelated to that for which the data was provided.
- Require **informed, opt-in consent** for any use that is not strictly required by the service offered to the consumer.
- **Protect data from misuse** by implementing appropriate privacy and security practices.

---

[96] *See, e.g.*, American Data Privacy Protection Act, H.R. 8152 § 2(24) (2022), https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

[97] *See* Letter from ACLU to Pallone, Chairman, House Energy & Commerce Committee, and Cathy McMorris Rodgers, Ranking Member, House Energy & Commerce Committee, on American Data Privacy Protection Act (July 18, 2022), https://www.aclu.org/letter/aclu-letter-house-energy-and-commerce-committee-american-data-privacy-protection-act.

[98] *See* Linda Morris & Olga Akselrod, *Holding Facebook Accountable for Digital Redlining*, ACLU (Jan. 27, 2022), https://www.aclu.org/news/privacy-technology/holding-facebook-accountable-for-digital-redlining.

- **Maintain transparency** so that consumers can understand how their data is used.

The practical result of such rules may well be to end certain commercial surveillance practices, including the brokerage of location data and the provision of biometric surveillance services, as it is hard to see how those practices could comport with robust data privacy laws. But explicitly limiting the strongest protections only to an exclusive list of "sensitive" data categories threatens to simply drive commercial surveillance practices to other types of data that lead to the same outcomes. A robust but flexible ruleset that inherently takes context into account will better protect consumers from the harms of all types of commercial surveillance, including but not limited to location and biometric surveillance.

III. FTC Rulemaking Can and Should Address Algorithmic Discrimination and Other Prevalent Harms of Automated Decision-Making Systems

A. As Automated Decision-Making Systems are Used to Make Key Decisions about Consumers, Algorithmic Error and Algorithmic Discrimination are Highly Prevalent

Related Questions:

53. How prevalent is algorithmic error? To what extent is algorithmic error inevitable? If it is inevitable, what are the benefits and costs of allowing companies to employ automated decision-making systems in critical areas, such as housing, credit, and employment? To what extent can companies mitigate algorithmic error in the absence of new trade regulation rules?

65. How prevalent is algorithmic discrimination based on protected categories such as race, sex, and age? Is such discrimination more pronounced in some sectors than others? If so, which ones?

Automated decision-making tools are a prevalent and entrenched part of modern economic and social systems. These tools are often built and deployed in ecosystems and institutions marked by entrenched discrimination— from the criminal legal system, to the family regulation system, to systems of housing, employment, and financial services. Built and evaluated by humans, automated decision-making tools are often developed using data that reflects systemic discrimination and abusive data collection practices, as discussed in Sections I and II above. Automated decision-making tools often attempt to predict outcomes that reflect systemic biases and can create feedback loops that serve to further systemic discrimination. These compounding issues can rear their heads throughout an automated decision-making system's design, development, implementation, and use, enabling algorithmic error, algorithmic discrimination, and other harmful effects.[99]

To understand the prevalence of algorithmic error, it is important to recognize that algorithmic error can take many different forms and can stem from a variety of sources, including the multi-faceted

[99] *See generally* ACLU Letter to the Nat'l Inst. of Standards & Tech. re: Call for Comments AI Risk Management Framework: Second Draft (Sept. 29, 2022), https://www.aclu.org/letter/aclu-comment-nists-second-draft-ai-risk-management-framework. (hereinafter "ACLU Letter to NIST re: Call for Comments on AI Risk Management"); ACLU Letter to the Nat'l Inst. of Standards & Tech. re: A Proposal for Identifying and Managing Bias within Artificial Intelligence (Spec. Pub. 1270) (Sept. 10, 2021), https://www.aclu.org/sites/default/files/field_document/2021.09.10_aclu_comment_on_nists_managing_ai_bias_proposal.pdf. (hereinafter "ACLU Letter to NIST re: Identifying and Managing Bias within AI").

decisions made in the process of designing and deploying algorithmic systems.[100] For example, mathematical mistakes, rounding errors, and software bugs can be considered algorithmic errors, as can individual instances of inaccurate predictions or classifications by an automated system. More broadly, the performance of proposed or deployed algorithmic systems may not always align with claims about the system's performance, and the potential mismatch between a system's claimed and actual performance also represents a form of algorithmic error. Through a systematic review of case studies about deployed artificial intelligence (AI) systems, Raji et al. (2022) provide a taxonomy of AI system failures that can also be used to understand types of algorithmic error – including failures or errors stemming from engineering and design processes, post-deployment processes, and communications about AI systems wherein developers make deceptive claims about AI systems' capabilities.[101]

Algorithmic error is also closely related to algorithmic discrimination – which may or may not be an intentional result of the deployment of an automated system. For example, an algorithmic system may have unequal error rates for different racial groups, reflecting the product of algorithmic bias and the system's potential to enable algorithmic discrimination. Algorithmic errors and bias also have the potential to propagate into datasets, models, and systems that are built on such artefacts, whether the errors are known or unknown, potentially contributing to further error or discrimination. Remedying downstream impacts of algorithmic errors – let alone identifying that they exist – may not always be straightforward.

In many instances, algorithmic discrimination occurs without the relevant protected characteristics being used as inputs to the algorithmic system. For example, in the health care context, a 2019 study found systemic racial bias in an algorithmic tool – which did not consider race as an input—used to recommend levels of patient care.[102] Another recent study found that an AI system trained on medical images, including X-rays and CT scans, learned to predict patient race based on the images, even when clinicians could not – raising serious questions about the potential for algorithmic bias.[103] These issues are compounded by the fact that many algorithmic systems are opaque, 'black box' systems, where users often do not understand how algorithmic decisions are being made or that algorithms are being used at all.[104]

---

[100] *See generally* Nicholas Diakopoulos, *Algorithmic Accountability: On the Investigation of Black Boxes*, Tow Ctr. Digit. Journalism (Dec. 3, 2014), https://www.cjr.org/tow_center_reports/algorithmic_accountability_on_the_investigation_of_black_boxes.php (discussing different sources of error and corresponding approaches to algorithmic accountability).

[101] *See* Inioluwa Raji et al., *The Fallacy of AI Functionality*, Assoc. for Computing Machinery (June 20, 2022), https://dl.acm.org/doi/abs/10.1145/3531146.3533158.

[102] Ziad Obermeyer et al., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, 366 Sci. 447 (Oct. 25, 2019), https://www.science.org/doi/10.1126/science.aax2342.

[103] Judy Gichoya et al., *AI Recognition of Patient Race in Medical Imaging: A Modelling Study*, 4 Lancet Digit. Health e406 (May 11, 2022), https://www.thelancet.com/pdfs/journals/landig/PIIS2589-7500(22)00063-2.pdf; *see also* Crystal Grant, *ACLU White Paper: AI in Health Care May Worsen Medical Racism*, https://www.aclu.org/legal-document/aclu-white-paper-ai-health-care-may-worsen-medical-racism (hereinafter "ACLU White Paper re: AI in Health Care").

[104] *See generally* ACLU Letter to NIST re: Identifying and Managing Bias within AI, *supra* note 99, at 7; *see also* ACLU White Paper re: AI in Health Care, *supra* note 103.

In the last several years alone, we have seen numerous examples of algorithmic discrimination resulting in serious harm to people and communities who are evaluated improperly by algorithmic systems. Automated decision-making is prevalent in many areas,[105] including housing, credit, and employment, and as a result, algorithmic discrimination can have serious implications for consumers' ability to access key financial services,[106] secure employment,[107] and obtain housing.[108]

In the context of housing, automated systems are highly prevalent. For one example, landlords frequently use automated systems to screen potential tenants. To evaluate tenants, these systems may pull in credit scores, legal records, previous housing history, and other information from data brokers and other sources. As highlighted in a recent report by the Consumer Financial Protection Bureau (CFPB),[109] these systems are prone to algorithmic errors and discrimination, which disproportionately impact Black and Latinx applicants, with devastating effects for consumers' ability to access housing.[110] When employers conduct background checks of applicants or financial institutions evaluate potential borrowers using similar technologies, these same problems also impact consumers' ability to access employment and credit. Similarly, in the financial services contexts, discriminatory algorithmic systems are regularly used, including for approving mortgages,[111] making credit decisions,[112] insurance

---

[105] ReNika Moore, *Biden Must Act to Get Racism Out of Automated Decision-Making*, Wash. Post (Aug. 9, 2021), https://www.washingtonpost.com/opinions/2021/08/09/biden-must-act-get-racism-out-automated-decision-making/.

[106] *See, e.g.*, Letter from ACLU et al., to Consumer Fin. Prot. Bureau et al. re: Addressing Technology's Role in Financial Services Discrimination (July 13, 2021), https://www.aclu.org/sites/default/files/field_document/2021-07-13_coalition_memo_on_technology_and_financial_services_discrimination.pdf (hereinafter "ACLU Letter to CFPB re: Technology's Role in Financial Services Discrimination")

[107] *See, e.g.*, Letter from the ACLU et al. to Equal Emp. Opportunity Comm'n et al. re: Addressing Technology's Role in Hiring Discrimination (July 13, 2021), https://www.aclu.org/sites/default/files/field_document/2021-07-13_coalition_memo_on_technology_and_hiring_discrimination.pdf (hereinafter "ACLU Letter to EEOC re: Tech.'s Role in Hiring Discrimination"). *See generally* Letter of ACLU et al. re: Centering Civil Rights in Artificial Intelligence and Technology Policy, to Dr. Eric S. Landor, Dir., White House Off. of Sci. & Tech. Pol'y et al. (July 13, 2021), https://www.aclu.org/sites/default/files/field_document/2021-07-13_letter_to_white_house_ostp_on_centering_civil_rights_in_ai_policy_1.pdf.

[108] *See, e.g.*, Letter from the ACLU et al. to HUD et al. re: Addressing Technology's Role in Housing Discrimination (July 13, 2021), https://www.aclu.org/sites/default/files/field_document/2021-07-13_coalition_memo_on_technology_and_housing_discrimination.pdf (hereinafter "ACLU Letter to HUD re: Tech.'s Role in Housing Discrimination").

[109] Consumer Fin. Prot. Bureau, *Tenant Background Checks Market* (Nov. 2022), https://files.consumerfinance.gov/f/documents/cfpb_tenant-background-checks-market_report_2022-11.pdf.

[110] Lauren Kirchner & Matthew Goldstein, *Access Denied: Faulty Automated Background Checks Freeze Out Renters*, The Markup (May 28, 2020), https://themarkup.org/locked-out/2020/05/28/access-denied-faulty-automated-background-checks-freeze-out-renters.

[111] Emmanuel Martinez & Lauren Kirchner, *The Secret Bias Hidden in Mortgage-Approval Algorithms*, The Markup (Aug. 25, 2021), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.

[112] Karen Hao, *The Coming War on the Hidden Algorithms that Trap People in Poverty*, MIT Tech. Rev. (Dec. 4, 2020), https://www.technologyreview.com/2020/12/04/1013068/algorithms-create-a-poverty-trap-lawyers-fight-back/.

underwriting,[113] and setting lending terms[114] – all areas where algorithmic discrimination and errors can be incredibly harmful.

Automated decision-making and algorithmic discrimination are also prevalent in many aspects of the hiring processes used by a high percentage of employers, as companies increasingly use outside platforms, vendors, and software in all stages of the process, including targeting job advertisements, attracting applicants, ranking and filtering resumes, testing applicants, analyzing interviews, and more.[115] The ACLU, other civil rights and technology organizations, and many researchers have raised concerns about hiring discrimination facilitated or exacerbated by these technologies,[116] and there have been many examples to date of algorithmically-driven or amplified racial discrimination,[117] gender discrimination,[118] and disability discrimination[119] in this area. For one example of algorithmic discrimination in this context, a job applicant may be rejected from an opportunity by an automated hiring system, even though a human reviewer at the company would consider the applicant to be highly qualified. A 2021 analysis of predictive hiring technologies found that the overwhelming majority of employers surveyed agreed that qualified candidates were being screened out by their current hiring processes, which rely heavily on automated filtering and ranking mechanisms.[120] Beyond improper rejections, as discriminatory ad delivery and matching mechanisms control which job advertisements consumers see in the first place, algorithmic discrimination can also prevent consumers from knowing about relevant job opportunities at all.[121] We discuss the dynamics and effects of targeted online

---

[113] Ronda Lee, *AI Can Perpetuate Racial Bias in Insurance Underwriting*, Yahoo Money (Nov. 1, 2022), https://money.yahoo.com/ai-perpetuates-bias-insurance-132122338.html.

[114] *See* Student Borrower Prot. Ctr., Educational Redlining (2020), available at https://protectborrowers.org/wp-content/uploads/2020/02/Education-Redlining-Report.pdf; Robert Bartlett et al., *Consumer-Lending Discrimination in the Fin-Tech Era* (Nov. 2019), https://faculty.haas.berkeley.edu/morse/research/papers/discrim.pdf (evaluating fin-tech products and finding Latinx and Black borrowers are rejected approximately 6% more often than white borrowers for loans, and those who receive mortgages pay 7.9 and 3.6 points more in interest for purchase and refinance mortgages, respectively, averaging a total of $765 million in extra interest per year).

[115] *See generally* Aaron Rieke & Miranda Bogen, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, Upturn (Dec. 10, 2018), https://www.upturn.org/work/help-wanted/; Aaron Rieke et al., *Essential Work: Analyzing the Hiring Technologies of Large Hourly Employers*, Upturn (July 6, 2021), https://www.upturn.org/work/essential-work.

[116] *See, e.g.*, ACLU Letter to EEOC re: Tech.'s Role in Hiring Discrimination, *supra* note 107, available at https://www.aclu.org/sites/default/files/field_document/.

[117] *See, e.g.*, Muhammad Ali et al., *Discrimination Through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes*, 3 Proceedings of the ACM on Human-Computer Interaction 1 (Nov. 7, 2019), https://dl.acm.org/doi/abs/10.1145/3359301.

[118] *See, e.g.*, Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*, Reuters (Oct. 10, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

[119] *See, e.g.*, Ctr. Democracy & Tech., *Algorithm-Driven Hiring Tools: Innovative Recruitment or Expedited Disability Discrimination?* (Dec. 2020), https://cdt.org/wp-content/uploads/2020/12/Full-Text-Algorithm-driven-Hiring-Tools-Innovative-Recruitment-or-Expedited-Disability-Discrimination.pdf.

[120] *See* Joseph Fuller et al, *Hidden Workers: Untapped Talent*, Harv. Bus. Sch. Proj. on Managing the Future of Work (Oct. 4, 2021), https://www.hbs.edu/managing-the-future-of-work/Documents/research/hiddenworkers09032021.pdf.

[121] *See, e.g.*, Morris & Akselrod, *supra* note 98; *see also* Ali et al., *Discrimination Through Optimization*, *supra* note 117, available at https://dl.acm.org/doi/abs/10.1145/3359301.

advertising in more detail in Section III.C.2. Whether the effect of algorithmic discrimination or error, and whether intentional or unintentional, the impact for consumers and employers can be devastating.

Algorithmic discrimination is prevalent in many other areas beyond housing, credit, and employment. When government entities use automated systems, whether created internally, developed through RFPs, or purchased from for-profit vendors, algorithmic discrimination and errors can result in wrongful denials of benefits or services,[122] false arrest and imprisonment,[123] and other serious harms. For example, in Michigan, an algorithmic system adopted by the state in 2013 that purported to be able to accurately flag fraudulent unemployed claims turned out to be systematically inaccurate. These algorithmic errors were incredibly costly – the state wrongfully seized millions of dollars from thousands of people, some of whom lost their jobs or homes as a result of the improper seizures.[124] Likewise, facial recognition and face surveillance technology is sold by a variety of private entities and used in predictive hiring technologies, remote proctoring, and law enforcement surveillance, where the ACLU has raised repeated concerns about its use and harms.[125] Facial recognition and facial analysis systems suffer from many kinds of algorithmic discrimination and errors and systematically misclassify Black people at higher rates than people of other races.[126]

There are many examples of algorithmic bias beyond these instances,[127] including potentially many types of algorithmic harms that are currently unknown or unmeasured. As these examples highlight, the costs of algorithmic discrimination and errors can vary amongst the contexts in which automated systems are deployed. Across contexts, these costs often disproportionately impact communities of color. In some settings, it may be extremely difficult or impossible to fully eliminate algorithmic error. For instance, an AI system may produce extremely low – but non-zero – error rates, as achieving perfect classification or prediction accuracy in deployment is extremely unlikely. For another example, as Raji et al. (2022) highlight, developers sometimes claim that AI systems have

---

[122] Dillon Reisman, *How the Government Relies on Algorithms to Allocate Healthcare Benefits—and Why These Secret Formulas Threaten Patients' Fundamental Rights*, ACLU NJ (Aug. 9, 2022), https://www.aclu-nj.org/en/news/how-government-relies-algorithms-allocate-healthcare-benefits-and-why-these-secret-formulas.

[123] *See* Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*, Wired (Mar. 7, 2022), https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/; *also see* Press Release, ACLU, Michigan Father Sues Detroit Police Department For Wrongful Arrest Based on Faulty Facial Recognition Technology (Apr. 13, 2021), https://www.aclu.org/press-releases/michigan-father-sues-detroit-police-department-wrongful-arrest-based-faulty-facial.

[124] *See* Julia Angwin, *The Seven-Year Struggle to Hold an Out-of-Control Algorithm to Account*, The Markup (Oct. 8, 2022), https://themarkup.org/newsletter/hello-world/the-seven-year-struggle-to-hold-an-out-of-control-algorithm-to-account; *see also* Press Release, Mich. Att'y Gen., State of Michigan Announces Settlement of Civil Rights Class Action Alleging False Accusations of Unemployment Fraud (Oct. 20, 2022), https://www.michigan.gov/ag/news/press-releases/2022/10/20/som-settlement-of-civil-rights-class-action-alleging-false-accusations-of-unemployment-fraud.

[125] See, e.g., Press Pause on Face Surveillance, ACLU Mass., (last visited Nov. 21, 2022), https://www.aclum.org/en/campaigns/press-pause-face-surveillance; Kade Crockford, *How is Face Recognition Surveillance Technology Racist?*, ACLU (June 16, 2020), https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist.

[126] *See, e.g.*, Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PMLR 77 (2018), https://proceedings.mlr.press/v81/buolamwini18a.html; Patrick Grother et al., Face Recognition Vendor Test, Nat'l Inst. Of Standards & Tech. (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf; Joy Buolamwini, *Facial Recognition Technologies: A Primer*, Algorithmic Just. League & MacArthur Found. (May 29, 2020), https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf.

[127] Resources like the AI Incident Database are focused on tracking examples of harms stemming from algorithmic error and algorithmic bias. *See* AI Incident Database, https://incidentdatabase.ai/.

capabilities that are impossible to have in practice.[128] So in addition to the statistical probability of error inherent in any complex system, hyperbolic claims about the system's functionality introduce yet another way in which the system can fail, by not meeting the unreasonable expectations created by the vendor. Though error may be inevitable at times, organizations building or using algorithmic systems should not be permitted to downplay evidence of discriminatory performance or disparate impacts simply because some level of error may be inevitable. Relatedly, the use of an algorithmic system should not be justified solely because humans are also prone to error.

There are various measures that private companies could and should take to proactively address or self-scrutinize their algorithmic systems before designing and deploying them to identify and remediate discrimination and errors. The precise steps that companies should take depend on the structure of the algorithmic system and the context surrounding its use.[129] However, for-profit entities may have little interest or incentive to make their algorithms more open, transparent, and accountable, or to regularly evaluate their systems for consequential errors or disparate impact. Indeed, "it is unrealistic to expect companies to decide, through voluntary internal auditing, whether they should attempt to seek profit from a tool in which they've invested. Absent a regulatory body or a binding third-party agreement ensuring thorough and transparent examination of AI tools, incentive structures will continue to favor profit and the resulting externalized harms of technology."[130] Moreover, algorithmic decision-making systems are often operated and deployed in such a way that the general public or impacted communities might not even know about these systems or their inner workings – and yet could still be materially affected by their decision-making process and errors.

In light of these dynamics and the serious socio-economic effects they generate, new federal regulation requiring thorough and transparent auditing is appropriate and essential. Moreover, there are many situations – particularly where the algorithmic tool is used in making critical decisions concerning liberty, livelihood, or other fundamental areas – where the danger of bias or error is intolerable and the algorithmic tool should be terminated. The Commission and other federal agencies have a critical role to play in helping to establish standards, with meaningful engagement with impacted communities, to evaluate the nature and magnitude of the risks as they are experienced by individuals and whether the potential harms associated with the algorithm outweigh or otherwise complicate assessments of the potential benefits.

B. Algorithmic Systems Must be Independently and Transparently Audited Throughout Their Design, Development, Deployment and Use

Related Questions:

54. What are the best ways to measure algorithmic error? Is it more pronounced or occurring with more frequency in some sectors than others?

56. To what extent, if at all, should new rules require companies to take specific steps to prevent algorithmic errors? If so, which steps? To what extent, if at all, should the Commission require firms to evaluate and certify that their reliance on automated decision-making meets clear standards concerning accuracy, validity, reliability, or error? If so, how? Who should set those standards, the FTC or a third-party entity? Or should new rules require businesses to evaluate and certify that the

[128] Raji et.al., *supra* note 101.

[129] ACLU Letter to NIST re: Call for Comments on AI Risk Management, *supra* note 99.

[130] *See generally* ACLU Letter to NIST re: Call for Comments on AI Risk Management, *supra* note 99.

accuracy, validity, or reliability of their commercial surveillance practices are in accordance with their own published business policies?

66. How should the Commission evaluate or measure algorithmic discrimination? How does algorithmic discrimination affect consumers, directly and indirectly? To what extent, if at all, does algorithmic discrimination stifle innovation or competition?

Algorithmic discrimination and error are best assessed as part of holistic efforts to evaluate algorithmic systems, both before they are developed, throughout the development and deployment processes, and after deployment to monitor their real-world functioning. While specific techniques for measuring and addressing algorithmic discrimination and error in particular areas should be selected based on the contexts in which the systems are developed and deployed, several general principles can guide these approaches. As highlighted in the ACLU's recent comments in response to the National Institute of ("NIST")'s publication of the "AI Risk Management Framework: Second Draft," these continuous approaches to audit algorithmic systems should center the communities directly impacted by system deployment, include both technical and non-technical analyses, and evaluate the broader contexts and organizations in which the systems function to truly understand how they do and do not work.[131]A holistic approach is essential to measuring algorithmic discrimination and error because they may be difficult to measure directly or impossible to anticipate before a thorough inquiry into an algorithmic system has been conducted. This issue is especially pertinent for "black box" algorithmic systems, and conducting comprehensive inquiries to measure algorithmic discrimination and error may increase the likelihood that these types of issues can be identified and prevented or stopped.

New federal regulations and binding rules are important to identify and address algorithmic discrimination and prevent harmful forms of algorithmic error, as well as to address other harmful impacts of the deployment of algorithmic systems. The Commission should consider requiring companies to adopt a comprehensive auditing framework to govern the use of automated decision-making systems and setting clear standards for that framework. To ensure the independence and objectivity of any organization tasked with measuring algorithmic discrimination and error, assessments should be carried out by independent external auditors, informed by these collaboratively developed standards, who are provided with real access to internal systems under appropriate privacy controls, and under conditions to prevent corporate capture in the auditing process.[132] For example, AI Now's framework for governing algorithmic use in public entities contains several prongs that could effectively apply to public-facing commercial entities whose products publicly depend on automated decision making, including requirements for external and independent review processes, notice to consumers about the use of automated decision-making systems and associated reviews, opportunities for public input, and avenues for recourse for impacted communities.[133] The ACLU set out a similar framework in its 2021 comments about NIST's special publication "A Proposal for Identifying and Managing Bias within Artificial Intelligence." There, we made the following recommendations for an auditing framework:

---

[131] *See generally* ACLU Letter to NIST re: Call for Comments on AI Risk Management, *supra* note 99.

[132] For more information about the importance of independent auditors and best practices for algorithmic audits, *see, e.g.*, Sasha Constanza-Chock et al., *Who Audits the Auditors? Recommendations from a Field Scan of the Algorithmic Auditing Ecosystem*, FAccT (June 2022), https://facctconference.org/static/pdfs_2022/facct22-126.pdf.

[133] Dillon Reisman et al., *Algorithmic Impact Assessments: A Practical Framework For Public Agency Accountability* 4, AI Now (Apr. 2018), https://ainowinstitute.org/aiareport2018.pdf.

> Audits and impact assessments should be conducted according to standards that set out necessary evaluation points, and at minimum should require: regular evaluation for discriminatory effects throughout the model's conception and development, and—if not terminated during development due to an unacceptable risk of bias or other reasons—in its implementation and use; proactive searches and adoption of less discriminatory alternatives; and assessments of whether data used in training technologies is representative and accurate, and that the technologies measure lawful and meaningful attributes and seek to predict valid target outcomes. . . . When an audit or impact assessment is conducted, it is important that information about the evaluation be publicly available, including information about the content and reasoning behind the evaluation, who is conducting the evaluation, and what their relationship is to the entity being evaluated. Audits and impact assessments should ideally only be conducted by independent third-party actors who do not have a stake in whether a system will ultimately be utilized or not, but in some instances, internal audits by neutral actors with no stake in whether a system is ultimately used may also be valuable. Additionally, the entity should be transparent about the scope of the audit or impact assessment. Results should also be made public.…Standards will also need to lay out what kind of information should be retained and documented about the technology, its development, and internal auditing sufficient to allow for third party auditing.[134]

The Commission could also consider requirements that might be more appropriate for particular sectors – for example, in a response to a multi-agency RFI, the ACLU and other advocacy organizations offered specific recommendations for assessments of AI systems used by financial institutions.[135] All of these types of requirements for companies could help ensure that products are fair and product-related statements are not deceptive.

The Commission's regulatory framework can and should coexist with other agencies' standards and sector-specific guidance, as well as with robust public enforcement. For example, NIST's proposal for "Managing Bias within Artificial Intelligence" included discussion of "technical characteristics needed to cultivate trust in AI systems: accuracy, explainability and interpretability, privacy, reliability, robustness, safety, and security (resilience)—and that harmful biases are mitigated."[136] The ACLU has raised concerns that NIST's proposal "reflects an overly tech-determinist approach to mitigating bias in AI," and made "recommendations addressing these technical characteristics as well as non-technical sociological and ethical considerations."[137] While NIST's development of the proposal and related frameworks thus remain works in progress, these efforts nevertheless provide the Commission an

---

[134] *See* ACLU Letter to NIST re: Identifying and Managing Bias within AI, *supra* note 99.

[135] Letter from the ACLU et al. to Financial Institutions re: Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning (July 1, 2021), https://nationalfairhousing.org/wp-content/uploads/2021/07/Federal-Banking-Regulator-RFI-re-AI_Advocate-Letter_FINAL_2021-07-01.pdf (hereinafter "ACLU Letter to Fin. Insts. re: RFI & Comment on AI Use").

[136] Reva Schwartz et al., *A Proposal for Identifying and Managing Bias in Artificial Intelligence*, Nat'l Inst. Standards & Tech., Spec. Pub. 1270 (June 2021), https://doi.org/10.6028/NIST.SP.1270-draft.

[137] ACLU Letter to NIST re: Identifying and Managing Bias within AI, *supra* note 99.

opportunity for inter-agency collaboration in developing clear standards for assessments and rules around when an AI tool in a particular context poses too great a risk and should be terminated. We discuss the topic of inter-agency collaboration further in Section III.C. Collaboration with non-government actors is also critical. The Commission's process for standards development should include meaningful consultation with impacted communities, external researchers, and advocacy organizations.[138]

1. Audit Requirements Should Not Vary According to the Weight That a Company Claims to Give to Algorithmic Outputs

Related Questions: *55. Does the weight that companies give to the outputs of automated decision-making systems overstate their reliability? If so, does that have the potential to lead to greater consumer harm when there are algorithmic errors?*

As discussed in Section III.A, vendors or developers of algorithmic systems may make misleading claims about a system's performance or design, and false or misleading claims about an algorithmic system's capabilities can contribute to or create serious harm for consumers.[139] These harms may be exacerbated in settings where AI systems are given undue reliance or deference. For instance, automated speech recognition systems are more likely to misidentify the speech of Black people compared to white people – yet these types of systems are used to inform important decision-making in health care and other settings.[140] As highlighted by Raji et al. (2022), false or misleading communications about an automated decision-making system can stem from claims that the system can perform a task that is impossible to perform.[141] For instance, in the context of hiring, software vendors claim to be able to estimate subjective and vague qualities in job applicants – such as how "adventurous" or "cultured" they are – through extremely short videos or gamified assessments.[142]

Unfortunately, under the status quo, the opaque nature of automated decision-making systems and algorithms means that it is often difficult, if not impossible, to determine what weight companies are placing upon certain outputs or applications. A company deploying these tools may itself not be able to clearly characterize how it is "weighting" these systems: for example, when a human content moderator is tasked with assessing dubious content, automated systems typically queue and prioritize what specific content is sent to human moderators for review, and how that content is annotated (ranked, tagged, etc.) before the human receives it. The human may ultimately make the decision about any particular piece of content, but they only review the content that the tools queue up. Some content never makes it to the reviewer, either because it was rejected automatically, or because it was automatically ranked as less urgent than other content in need of review. Similarly, hiring algorithms often rate applicants through fitness scores or rankings, and research has shown that even though there

---

[138] ACLU Letter to NIST re: Call for Comments on AI Risk Management, *supra* note 99.

[139] *See* Raji et Al., *supra* note 101.

[140] *See* Allison Koenecke, *Racial Disparities in Automated Speech Recognition*, Procs. Nat'l Acad. Scis. (Mar. 23, 2020), https://www.pnas.org/doi/10.1073/pnas.1915768117.

[141] *See* Raji et al., *supra* note 101.

[142] Luke Stark & Jevan Hutson, *Physiognomic Artificial Intelligence*, Fordham Intell. Prop., Media & Ent. L. J. (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3927300.

may be very little statistical difference between candidates within a range of rankings, the ranking order may significantly impact how an employer views a candidate. Some employers may choose to automatically reject an applicant below a certain cut off score, but even if an employer chooses not to use the score to automatically reject a candidate, in practice applicants with lower scores may never get reviewed by a human because the candidates with the higher score will get the greater attention.[143] What "weight" are these companies putting on the automated queuing system?

Given these realities and dynamics, the Commission should adopt a framework that requires companies to proactively, independently, and regularly evaluate the impact of automated systems and algorithmic error. These audit requirements should not depend on the claims of system vendors or users about their reliance on or weighting of algorithmic inputs or outputs unless those claims have been independently and transparently verified.

C. The Commission Has the Authority and Mandate to Issue Rules to Address Discrimination in Automated Decision Systems and Other Commercial Practices.

1. Section 5 Gives the Commission the Authority and Mandate to Prevent Discrimination

Related Questions: *71. To what extent, if at all, may the Commission rely on its unfairness authority under Section 5 to promulgate antidiscrimination rules? Should it? How, if at all, should antidiscrimination doctrine in other sectors or federal statutes relate to new rules?*

The Commission has a key role to play in addressing discrimination in consumer practices through its unfairness authority, and the exercise of that authority is not only permitted but mandated by statute. Under Section 5 of the FTC Act, "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful" and the Commission is "empowered and directed to prevent" companies from engaging in such practices. 15 U.S.C. § 45(a)(1). Section 5 further defines an act or practice as unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n).

Discrimination is inherently unfair and meets each of the prongs of the unfairness test under Section 5, including in the context of commercial data and automated decision-making practices. Responses to Questions 53 and 65–in Section III.A–discuss in detail the ample evidence of the "substantial injury" that such practices can cause, including exacerbating existing disparities and creating new roadblocks for already-marginalized groups in core areas such as economic opportunities, liberty, and health. Indeed, these practices can have lifechanging consequences for people, including limiting access to housing, employment, insurance and financial services, subjecting them to improper healthcare treatment based on systemic racial discrimination built into diagnostic tools, or leading to a denial of benefits or bail.

Second, the black box nature of many commercial data practices and algorithmic tools as well as the ubiquity of their use make it difficult if not impossible for consumers to avoid their harms. For example, consumers cannot reasonably choose whether a job to which they have applied or a bank from whom they have sought a loan uses algorithmic tools, and most people are wholly unaware that an algorithmic tool is being used in a company's process, what it considers, or how it works. When someone is excluded from receiving an ad for an economic opportunity through an advertiser's use of

[143] Upturn, *supra* note 115.

selection tools or the workings of a discriminatory ad delivery algorithm, they are unaware that the ad for the opportunity was shown to others or exists at all. Moreover, even where consumers are somehow aware that a discriminatory tool is being used, consumers often do not have alternative options, and it would be inherently unreasonable to place the onus on consumers to forego an economic opportunity in order to avoid a company's discriminatory practice. And of course, with respect to government uses of automated decision making or other tools, the people most often impacted have the least say in what the government chooses to use and typically never have a say at the moment when the tool is used to make an individual decision. People cannot avoid the injury – the FTC needs to use the full scope of its authority to prevent it.

Third, there are no "countervailing benefits to consumers or to competition" that outweigh the harms from discrimination. Discrimination not only harms the individuals and communities against whom adverse decisions are made, but also erodes the efficiency, productivity, and fairness of systems and institutions. Modern day commercial data or automated tools can serve to further entrench and compound existing discrimination, and the complexity of the tools and the lack of transparency in their use makes it even harder to identify and address the sources of the harm. As discussed in more detail in response to Question 70 in Section III.D, strong protections against algorithmic discrimination have the potential to benefit all consumers.

Finally, as discussed in response to Question 69 in Section III.C.3, anti-discrimination prohibitions under other statutes and sectors will also continue to apply, and the Commission's rules should complement anti-discrimination enforcement under other statutes and fill gaps in their reach. Inter-agency coordination would best allow for a whole-of-government approach to addressing discrimination in a given sector while allowing agencies to share expertise and maximize resources. Sometimes the Commission or another agency may decide that it is prudent for a single agency to take enforcement action against a discriminatory entity, and at other times multiple claims or separate enforcement actions will be the preferred approach. Sometimes claims brought by individuals or classes of consumers may intersect with federal enforcement activities. These multiple forms and spheres of enforcement can complement one another and play an important role in ensuring that anti-discrimination protections are robustly applied.

2. Section 5 Provides the Commission the Authority to Address Unfair and Deceptive Practices in Targeted Advertising

a. Targeted Advertising is Prevalent and Often Pernicious

Related Questions: *62. Which, if any, legal theories would support limits on the use of automated systems in targeted advertising given potential constitutional or other legal challenges?*

The FTC has considerable authority under Section 5 and 18, including to promulgate and enforce rules regarding acts or practices that are unfair or deceptive and affect commerce. The rules could apply straightforwardly to a range of software-based products and services, including automated systems involving targeted advertising in contexts where existing antidiscrimination laws also apply.[144]

[144] *See generally* Letter from Laura Murphy and Rachel Goodman, on behalf of ACLU, to Fed. Trade Comm'n re: Big Data: A Tool for Inclusion or Exclusion?, https://web.archive.org/web/20170221082053/https://www.ftc.gov/system/files/documents/public_comments/2014/10/00

Targeted advertising is widespread, invasive, and often discriminatory and unfair. It is nearly ubiquitous on the Internet: these systems are embedded both on large platforms with internal targeting systems, and on smaller sites which contract out to third-party networks which base ads on user profiles. Targeted advertising systems have also spread well beyond the Internet, including mobile apps,[145] television,[146] and billboards.[147]

While modern advertising networks typically target viewers on the basis of an individualized user profile, ads are typically placed—either by the advertising network or by the advertiser themselves—on the basis of real or inferred personal characteristics. Effectively opting out of this targeting process is nearly impossible.[148] The result of this placement scheme is that people with different characteristics, from different walks of life, are likely to see different advertisements.

Advertising today can be life-shaping. The presence or absence of particular advertisements can guide people to (or away from) potential products, social groups, political organizations, jobs, credit or other economic opportunities, education, or housing. When advertising filters the perspective of a person to the point that they cannot make effective comparisons or even be effectively aware of reasonable opportunities, it has the potential to cause lasting harm. When that advertising is targeted based on individualized profiles or personal characteristics, those harms are compounded by unfairness in delivery.

For example, on some advertising networks, an advertiser may deliberately and explicitly target an ad including a job description to men, leaving women and non-binary people at a manifest disadvantage in the labor market. An advertiser may also target categories which happen to be strong correlates (or "proxy variables") for other protected classes, such as preferred musical genre, or geolocation in segregated areas. Advertisers may also target by so-called "look-alike" audiences, where the advertiser gives a list of individual identifiers to the ad network and asks the network to show the advertisement to "similar" people, leaving it to the network to define similarity.[149] Finally, an advertising network that itself optimizes ads on the basis of expected engagement rates may unfairly include or exclude individuals from opportunities related to essential goods and services.[150]

059-92874.pdf (discussing the FTC and CFPB's authority under the FTCA and ECOA, respectively, to respond to discriminatory effects of targeted advertising).

[145] Suman Nath, *MAdScope: Characterizing Mobile In-App Targeted Ads*, Microsoft (2015), https://www.microsoft.com/en-us/research/publication/madscope-characterizing-mobile-in-app-targeted-ads/.

[146] Thomas Germain, *Targeted Ads Have Come to Your TV*, Consumer Reps. (Aug. 30, 2021), https://www.consumerreports.org/advertising-marketing/targeted-ads-have-come-to-your-tv-a2176040919/.

[147] Big Brother Watch, *The Streets Are Watching: How Billboards Are Spying on You* (Oct. 2022), https://bigbrotherwatch.org.uk/wp-content/uploads/2022/10/The-Streets-Are-Watching-You.pdf.

[148] Daniel Kahn Gillmor, *Facebook is Tracking Me Even Though I'm Not on Facebook*, ACLU (Apr. 5, 2018), https://www.aclu.org/news/privacy-technology/facebook-tracking-me-even-though-im-not-facebook.

[149] Jinyan Zang, *How Facebook's Advertising Algorithms Can Discriminate by Race and Ethnicity*, Tech. Sci. (Oct. 19, 2021), https://techscience.org/a/2021101901/.

[150] Ali et al., *supra* note 117.

b. Neither the First Amendment Nor Section 230 of the Communications Decency Act Prevent the Commission From Issuing Rules Regarding Targeted Advertising

Related Questions: *63. To what extent, if at all, does the First Amendment bar or not bar the Commission from promulgating or enforcing rules concerning the ways in which companies personalize or deliver targeted advertisements?*

64. To what extent, if at all, does Section 230 of the Communications Decency Act, 47 U.S.C. 230, bar the Commission from promulgating or enforcing rules concerning the ways in which companies use automated decision-making systems to, among other things, personalize services or deliver targeted advertisements?

The Commission can promulgate and enforce rules regarding targeted advertising consistent with the strictures of the First Amendment and Section 230 of the Communications Decency Act.[151] Indeed, large technology companies have recently settled legal claims involving discriminatory ad targeting and reformed some of their practices,[152] which underscores the core importance of enforcement action in this field.

For decades, the ACLU has fought to vindicate individuals' First Amendment rights across a wide range of situations and contexts. These constitutional rights remain vitally important, particularly when a government official seeks to restrict or punish an individual or organization from engaging in protected speech or expression.

The ACLU has also long made clear that discriminatory conduct can be proscribed consistent with the First Amendment. Just this year, the ACLU filed a brief in the U.S. Supreme Court stressing that "[t]here is no First Amendment right to discriminate" and urging the Court to decline to undermine civil rights laws by creating amorphous new exceptions under the Free Exercise or Free Speech clauses.[153]

Such discrimination can therefore constitutionally be prohibited in the case of targeted advertising, where advertisers and platforms target (or exclude) people on the basis of protected class status, such as race, sex, age, or disability, for opportunities in critical sectors like housing, employment, credit, or education. The same is true for advertising delivery practices or systems that result in a disparate impact based on protected class status in areas covered by civil rights laws—regardless of whether the ad delivery is effectuated by an automated decision-making system. The First

---

[151] *Accord* Amicus Curiae Brief of ACLU Foundation et al., *Opiotennione v. Bozzuto Mgmt. Co.*, No. 21-1919 (4th Cir. filed Dec. 17, 2021), available at https://www.aclu.org/sites/default/files/field_document/49-2_2021.12.17_bozzuto_civil_rights_amicus_brief.pdf; Amicus Curiae Brief of the ACLU Foundation et al., *Vargas v. Facebook, Inc.,* No. 21-16499 (9th Cir. filed Jan. 26, 2022), https://www.aclu.org/sites/default/files/field_document/22-2_2022.1.26_updated_vargas_amicus.pdf (hereinafter "ACLU *Vargas* Amicus Brief").

[152] *E.g.*, Press Release, ACLU, Facebook Agrees to Sweeping Reforms to Curb Discriminatory Ad Targeting Practices (Mar. 19, 2019), https://www.aclu.org/press-releases/facebook-agrees-sweeping-reforms-curb-discriminatory-ad-targeting-practices. *See generally* Morris & Akselrod, *supra* note 98.

[153] Press Release, ACLU Files Amicus Brief Urging Supreme Court to Reject Attempt to Weaken Civil Rights Law (Aug. 19, 2022), https://www.aclu.org/press-releases/aclu-files-amicus-brief-urging-supreme-court-reject-attempt-weaken-civil-rights-law.

Amendment is not a barrier to regulating such discriminatory conduct. Indeed, federal civil rights laws have long prohibited discriminatory advertisements, such as offering housing to only residents of one racial group.[154]

Section 230 of the Communications Decency Act also need not impede the Commission's rulemaking where it touches on matters of discrimination against protected classes by the platform operators themselves. Section 230 was "designed to protect internet publishers from liability for third-party content, like content posted on message boards or a user's Facebook feed. [But the] law offers no protection for [an internet publisher's] own conduct, such as its design and sale of discriminatory ad-targeting tools and its use of a discriminatory ad-delivery algorithm."[155] The ACLU recently filed a brief in the U.S. Court of Appeals for the Ninth Circuit detailing how Section 230 does not apply when a social media platform "put its users into cohorts based on protected characteristics or proxies thereof, designed drop down menus that enabled advertisers to exclude some users from seeing ads on those bases, created ad audiences based on those selections, and used its ad algorithm to discriminate in the delivery of the ads."[156] When a platform makes "a business decision to use stereotypes to segregate users,"[157] in matters related to protected sectors like housing, employment, credit, or education, those decisions may be legally actionable under both the federal Constitution and federal statutes, and tailored rules by authorities like the FTC can be brought to bear without contravening Section 230.

3. The Commission's Issuance of Rules on Algorithmic Discrimination and Other Consumer Surveillance Practices Can Complement the Work of Other Federal Agencies and Civil Rights Statutes

a. The Commission's Rules Have Always Reached Areas That Are Covered By Other Laws and Should Do So in this Context

Related Questions: *69. Should the Commission consider new rules on algorithmic discrimination in areas where Congress has already explicitly legislated, such as housing, employment, labor, and consumer finance? Or should the Commission consider such rules addressing all sectors?*

The Commission can and should consider and develop new rules to address algorithmic discrimination. The Commission's anti-discrimination work under Section 5 – discussed further in response to Question 71 in Section III.C.1 – should complement and support enforcement by other agencies of other federal and state anti-discrimination laws, as the Commission regularly does in other contexts. Indeed, the Commission's jurisdiction and enforcement activities often coincide with sister agencies and other sector-specific laws. For example, FTC "authority covers for-profit entities such as mortgage companies, mortgage brokers, creditors, and debt collectors,"[158] which are also implicated or regulated by a range of other federal statutes. In addition, the FTC regularly collaborates with the

[154] *See, e.g.*, U.S. Dep't Hous. & Urb. Dev., *Advertising and Marketing*, https://www.hud.gov/program_offices/fair_housing_equal_opp/advertising_and_marketing.

[155] Morris & Akselrod, *supra* note 98.

[156] ACLU *Vargas* Amicus Brief, *supra* note 151, at 4–5.

[157] *Id.* at 27–31.

[158] Fed. Trade Comm'n, *Consumer Finance*, https://www.ftc.gov/news-events/topics/consumer-finance.

Justice Department and the Consumer Financial Protection Bureau,[159] notwithstanding the fact that Congress has given each entity their own set of authorities and, in some instances, industries to focus on. Each agency may bring their own expertise, resources, and perspective to bear on these intricate national problems. Here, the Commission's anti-discrimination work under Section 5 can also fill critical gaps in the application of other federal civil rights laws. For example, Title VII protections against employment discrimination apply to employers and actions by employment agencies, and it is unsettled how modern-day vendors of technologies used in the employment space fit under the traditional definition of employment agency. 42 U.S.C. § 2000e(c). Title VI of the Civil Rights Act of 1964 only applies to race and national origin, thus failing to provide protection for people who are impacted by discrimination due to other characteristics. 42 U.S.C. §§ 2000d.

The ACLU has urged a number of federal agencies to concurrently exercise their existing statutory authority, rulemaking processes, and investigatory powers to address technology-enabled discrimination within their respective purview. For instance, the ACLU has urged the Federal Trade Commission to collaborate with other agencies, including CFPB and HUD, to conduct investigations into the tenant screening industry, to provide guidance on tenant screening practices that may be unfair or deceptive under Section 5 of the FTC Act, and to publish guidance for tenant screening companies on complying with the Fair Credit Reporting Act (FCRA).[160]

Beyond the FTC, the ACLU encouraged the Board of Governors of the Federal Reserve System and other financial agencies to develop an action plan and potentially "a proposed framework for the regulation of AI in financial services," including CFPB regulations addressing the "complications raised by AI/ML [machine learning] models [and how they] do not relieve creditors of their obligations."[161] The ACLU has urged the EEOC to use its existing authority, *inter alia*, to collect greater information about algorithmic discrimination in hiring technologies, to strengthen audits and audit-related rules, and to update employee selection procedures.[162] The ACLU also urged the U.S. Department of Housing and Urban Development, *inter alia* to update its guidelines about online advertising practices that can violate the Fair Housing Act and to promulgate guidance regarding technology and the Affirmatively Furthering Fair Housing (AFFH) rule.[163] The ACLU, in recent comments to HHS concerning their proposed rule barring discrimination in clinical tools, urged the

---

[159] *See, e.g.*, Press Release, Fed. Trade Comm'n, Federal Trade Commission and Justice Department Seek to Strengthen Enforcement Against Illegal Mergers (Jan. 18, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/01/federal-trade-commission-justice-department-seek-strengthen-enforcement-against-illegal-mergers; Press Release, Fed. Trade Comm'n, Federal Trade Commission, Consumer Financial Protection Bureau Pledge to Work Together to Protect Consumers (Jan. 24, 2022), https://www.ftc.gov/news-events/news/press-releases/2012/01/federal-trade-commission-consumer-financial-protection-bureau-pledge-work-together-protect-consumers.

[160] ACLU Letter to HUD re: Tech.'s Role in Housing Discrimination, *supra* note 108.

[161] ACLU Letter to Fin. Insts. re: RFI & Comment on AI Use, *supra* note 135. *See also* Press Release, ACLU, ACLU Comment on Release of White House Blueprint for an Artificial Intelligence Bill of Rights (Oct. 4, 2022), https://www.aclu.org/press-releases/aclu-comment-release-white-house-blueprint-artificial-intelligence-bill-rights.

[162] ACLU Letter to EEOC re: Tech.'s Role in Hiring Discrimination, *supra* note 107.

[163] ACLU Letter to HUD re: Tech.'s Role in Housing Discrimination, *supra* note 108.

agency to extend this rule-making to include other technologies used in medical and clinical care.[164] Additionally, the ACLU urged the CFPB and other agencies to update guidance about digital advertising about financial services and to consider rulemaking related to the use of alternative data for underwriting.[165] The EEOC and DOJ Civil Rights Division have also taken other recent actions on algorithmic discrimination and artificial intelligence,[166] and the CFPB is continuing to investigate the tenant screening industry.[167] While these actions are encouraging, much more investment should be made to address algorithmic discrimination, including through the development of new rules by the Commission. Additional enforcement action, inter-agency coordination, and new rules can significantly improve the status quo when it comes to algorithmic discrimination.

b. The Commission Brings Critical Expertise and Investigative Authority That Are Essential for Addressing Algorithmic Discrimination and Other Harms

Related Questions: *72. How can the Commission's expertise and authorities complement those of other civil rights agencies? How might a new rule ensure space for interagency collaboration?*

The Federal Trade Commission has robust investigatory authority and considerable expertise – particularly in assessing anti-competitive behavior and unfair or deceptive practices. The Commission's economic expertise, in particular, will prove highly valuable in assessing "privacy issues raised by behavioral advertising."[168] Additionally, the Commission has benefited from a series of skilled Chief Technology Officers,[169] privacy experts, and other technologists, who can and do provide technical input, including on the complexities of algorithmic discrimination, for investigations and original research. In some instances, the Commission also may conduct international investigations,[170] which could be quite useful in the case of sprawling multi-national companies or software services that

[164] See Letter from the ACLU to the Department of Health and Human Services, *Proposed Rule at 87 Fed. Reg. 47,824, RIN 0945-AA17 titled "Nondiscrimination in Health and Health Education Programs or Activities"*, https://www.regulations.gov/comment/HHS-OS-2022-0012-72816.

[165] ACLU Letter to CFPB re: Technology's Role in Financial Services Discrimination, *supra* note 106.

[166] Press Release, U.S. Equal Emp. Opportunity Comm'n, EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairness (Oct. 28, 2021), https://www.eeoc.gov/newsroom/eeoc-launches-initiative-artificial-intelligence-and-algorithmic-fairness; U.S. Dep't of Just., Civ. Rts. Div., *Algorithms, Artificial Intelligence, and Disability Discrimination in Hiring* (May 12, 2022), https://www.ada.gov/resources/ai-guidance/; U.S. Equal Emp. Opportunity Comm'n, *The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees* (May 12, 2022), https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence.

[167] Consumer Fin. Prot. Bureau, *supra* note 109.

[168] *Accord* Michael R. Baye, Dir., Fed. Trade. Comm'n Bureau of Econ., *Is There a Doctor in the House? The Value of Economic Expertise in Antitrust, Consumer Protection, and Public Policy*, Prepared Remarks for Breakfast with the Federal Trade Commission Bureau Directors, 56th Antitrust Law Spring Meeting (Mar. 28, 2008), https://www.ftc.gov/sites/default/files/documents/public_statements/there-doctor-house-value-economic-expertise-antitrust-consumer-protection-and-public-policy/080328aba.pdf.

[169] Fed. Trade Comm'n, *FTC Chief Technologists*, https://www.ftc.gov/about-ftc/commissioners-staff/ftc-chief-technologists.

[170] *See, e.g.*, Fed. Trade Comm'n, *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, https://www.ftc.gov/about-ftc/mission/enforcement-authority.

are developed or hosted in one country but offered to consumers in another. The Commission's expertise in enforcement actions to prevent or stop companies from deceptive practices will be a critical resource in addressing misrepresentations regarding the capabilities of automated tools or regarding the assessments that have been conducted on these tools prior to their use. Finally, some data privacy or algorithmic discrimination issues may worsen or become more entrenched when two large companies seek to merge, or when a large company seeks to buy out a small rival – and therefore the Commission's antitrust authorities and expertise could dovetail with anti-discrimination interest.

As the ACLU recently underscored in a memo to the Domestic Policy Council, the "creation of a robust interagency coordination process [about AI and equity] is essential…."[171] At a high level, this will require a coordinated, interagency effort, demonstrated commitment through leadership and senior engagement, and consistently being attuned to the concerns and needs of impacted communities.[172] The problem of algorithmic bias spans across all issue areas that touch civil rights and requires both technical and legal expertise, so the federal government should have a well-coordinated interagency strategy that allows agencies to share resources and expertise and collaborate in complementary ways. Towards that end, the FTC's "unfairness" authority under Section 5, discussed further in Section III.C.1, can work hand-in-hand with the traditional authorities of civil rights enforcement agencies. For example, in some instances, EEOC would focus on discriminatory actions brought by employers and employment agencies – and in others, the FTC can investigate technology vendors that sell "unfair" or "deceptive" products that facilitate discriminatory screening in recruiting or hiring but might not be considered an employer or employment agency within the scope of Title VII. The Commission, together with other agencies, can and should work together in order to address problems through their respective lenses. The FTC may also want to collaborate with federal agencies which issue guidance and strategies to the private sector, like NIST and the FDA, to ensure that industry best practice can be brought into alignment with reasonable reliability, privacy, transparency, and anti-discrimination rules. A new FTC rule might set up a mechanism for the Commission to enter into collaboration agreements (similar to recent ones with DOJ and CFPB) with other civil rights agencies specifically about discrimination claims. On a case-by-case basis, it may be advantageous to let other agencies take the lead on particular issues or statutory applications.

The dilemmas and damage associated with algorithmic discrimination transcend easy classification or simple reduction to a single federal agency or federal statute, and FTC's rule making and enforcement is a critical piece of the necessary federal response.

D. Robust Protections Against Algorithmic Discrimination and Other Harms Benefit All Consumers

Related Questions:

57. To what extent, if at all, do consumers benefit from automated decision-making systems? Who is most likely to benefit? Who is most likely to be harmed or disadvantaged? To what extent do such practices violate Section 5 of the FTC Act?

66. How should the Commission evaluate or measure algorithmic discrimination? How does algorithmic discrimination affect consumers,

[171] ACLU Memo to Ambassador Susan Rice et al. re: Recommendations to the Interagency Policy Committee on AI and Equity (July 5, 2022), https://www.aclu.org/letter/ipc-memo-dpc-and-ostp.

[172] *Id.*

directly and indirectly? To what extent, if at all, does algorithmic discrimination stifle innovation or competition?

70. How, if at all, would restrictions on discrimination by automated decision-making systems based on protected categories affect all consumers?

Identifying whether consumers benefit in practice from automated decision-making systems requires a complex and careful analysis of how those systems are built, deployed, and monitored. As discussed in the ACLU's recent comments about NIST's AI Risk Management Framework, the same automated decision-making system may have vastly different effects for different individuals or communities – for instance, it may be the case that "a tool poses a low risk to users in some locations and in some contexts but higher risk to others."[173] Efforts to understand potential harms and benefits must be informed by this reality, and ultimately must include "meaningful input from the communities that will be affected by a given algorithmic deployment. That input should include the nature and magnitude of the risks as they are experienced by individuals and whether the potential harms associated with the algorithm outweigh or otherwise complicate assessments of the potential benefits."[174] Thus, while automated decision-making systems may have the potential to benefit consumers, to realize these benefits, such systems must be carefully considered, designed and deployed with proactive and continuous safeguards to anticipate, identify, and appropriately address issues.

As discussed in Sections III.A and III.B, there is clear evidence of the severe and prevalent harms of automated systems – from targeted advertising and discriminatory delivery of job, housing, and credit advertisements, to biased facial recognition systems, and more. As outlined in the examples of algorithmic bias and algorithmic error in Section III.A, algorithmic discrimination can harm consumers in both direct and indirect ways. For example, as discussed in Section III.A, predictive hiring systems can directly lead to discriminatory or erroneous rejections of job applicants. They can also indirectly hamper employment opportunities by skewing the job advertisements a prospective employee sees online, impacting their ability to know about relevant job opportunities in the first place. Moreover, the collective effects of algorithmic discrimination impede free and fair competition and consumer choice. For instance, in addition to being racially discriminatory, an algorithm that shows Black customers one product or price and white customers another product or price also distorts market dynamics and vigorous competition over products and prices.[175]

Frameworks like that of Suresh and Guttag (2021) can be used to contextualize the harms of these systems, including how harms can stem from decisions made during the machine learning development life cycle.[176] Similarly, resources like the Algorithmic Equity Toolkit created by the

---

[173] *See generally* ACLU Letter to NIST re: Call for Comments on AI Risk Management, *supra* note 99.

[174] *Id.*

[175] *See, e.g.*, Mary Pattillo, *Making Fair (Public) Housing Claims in a Post-Racism Legal Context*, 18 J. Affordable Hous. & Cmty. Dev. L. 215, 217–18 (2009) ("Past racism has [] distorted the functioning of institutions and markets – here, the housing market"); Amicus Curiae Brief of NAACP Legal Def. & Educ. Fund, Inc. at 14, *Tex. Dep't of Hous. & Cmty. Affairs, et al., v. The Inclusive Cmtys. Proj., Inc.* No. 13-1371 (filed Dec. 24, 2014), https://www.naacpldf.org/wp-content/uploads/Texas-v-ICP-LDF-Brief-in-Support-of-Respondents-13-1371-1-1.pdf.

[176] Harini Suresh & John Guttag, *A Framework for Understanding Sources of Harm Throughout the Machine Learning Life Cycle*, Assoc. Computing Mach. (Oct. 2021), https://dl.acm.org/doi/fullHtml/10.1145/3465416.3483305.

ACLU of Washington can be used to identify and understand harms of automated decision-making systems used in government contexts.[177] As discussed further in Section III.C.1, products that differentiate and disadvantage consumers on the basis of protected and innate characteristics, such as race or sex, generally violate Section 5 of the FTC Act, namely because it is inherently unfair to limit or exclude access to goods and services for discriminatory reasons.

Strong protections that address algorithmic discrimination – including transparency protections, independent and continuous auditing, thoughtful decommissioning decisions, opportunities for recourse, and more – have the potential to benefit all consumers. For example, transparent and accountable documentation and audits of machine learning models and datasets can help surface algorithmic discrimination, but they can also help improve system documentation, promote reproducibility, address data leakage issues, provide crucial technical information to downstream users of algorithmic systems, and provide myriad other benefits.[178] All of these improvements can make AI systems work better for everyone. If the Commission enacts robust anti-discrimination protections, combined with active enforcement and other related protections such as data privacy rules and other protections discussed in Sections I and II, all consumers could substantially benefit from such combined and inter-related protections.

* * *

CONCLUSION

The ACLU applauds the Commission for soliciting input on these crucial issues, and urges the Commission to follow up with deliberate and speedy movement toward promulgation of meaningful protections in the form of trade regulation rules. Deep and widespread harms caused by abusive collection and use of consumers' data have been allowed to continue, virtually unchecked, for far too long. The time for action is now.

If you have any questions about this comment, please do not hesitate to contact Nathan Freed Wessler at nwessler@aclu.org, or Olga Akselrod at oakselrod@aclu.org.

Sincerely,

American Civil Liberties Union

---

[177] *See generally* ACLU Wash., *Algorithmic Equity Toolkit*, https://www.aclu-wa.org/AEKit#:~:text=WHAT%20IS%20THE%20AEKit%3F,impacts%2C%20effectiveness%2C%20and%20oversight.

[178] *See, e.g.*, Timnit Gebru et al., *Datasheets for* Datasets, 64 *Comms. Of the Assoc. Computing Mach.* 86, https://cacm.acm.org/magazines/2021/12/256932-datasheets-for-datasets/abstract; Margaret Mitchell et al., *Model Cards for Model Reporting*, FAT*'19: Conf. on Fairness, Accountability & Transparency (Jan. 14, 2019), https://arxiv.org/abs/1810.03993; Saran Holland et al., *The Dataset Nutrition Label: A Framework to Drive Higher Data Quality Standards*, arXiv (May 9, 2018), https://arxiv.org/abs/1805.03677; Sayash Kapoor & Arvind Narayanan, *Leakage and the Reproducibility Crisis in ML-based Science*, arXiv (July 14, 2022), https://arxiv.org/abs/2207.07048.