Before the
Federal Trade Commission
Washington, D.C.

In the matter of	
Trade Regulation Rule on Commercial Surveillance and Data Security	R111004 Commercial Surveillance ANPR

Center for Democracy & Technology Comments on Commercial Surveillance ANPR

November 21, 2022

Lydia X. Z. Brown
Andrew Crawford
Nick Doty
Matt Scherer
Ridhi Shetty
Cody Venzke
Michael Yang

Elizabeth Laird
Eric Null
George Slover

Center for Democracy & Technology
1401 K St NW, Suite 200
Washington, DC 20005

Table of Contents

Introduction **1**

Part 1: A privacy rule should address the risks of private sector commercial surveillance practices **1**

I. There are many prevalent private sector data practices that cause harms **2**

A. Companies' excessive collection and secondary uses of sensitive data allow companies to monetize data while harming consumers. 3

i. Disability-related data 4

ii. Health Data 7

iii. Location Data 12

iv. Financial data 14

B. Data broker practices violate people's privacy. 16

C. Behaviorally targeted advertising misuses consumers' data to promote harmful advertisements to certain consumers or to prevent them from receiving beneficial advertisements. 20

D. Companies limit access to critical opportunities through decision-making systems that use data about protected characteristics, or process data in ways that have a disparate impact on marginalized people. 25

i. Housing and credit 26

ii. Employment 30

E. Companies utilize dark patterns designed to nudge consumers to enable access to their data. 36

II. Recommendations for privacy-protective measures in FTC rulemaking **39**

A. Require data minimization and use and purpose limitations in how companies handle consumer data. 39

B. Require companies to provide easily accessible consumer controls. 42

C. Require companies to abide by meaningful transparency measures. 44

III. The FTC should consider several competition issues **45**

Part 2: A privacy rule should be appropriately scoped to address impacts of commercial surveillance and lax data security practices in education and other government services **48**

I. The FTC should adopt measures to mitigate unintended consequences for educational and governmental entities **48**

A. Potential unintended consequences from overbroad regulations 48

B. To mitigate unintended consequences, the FTC should build on existing legal requirements, ensure that new regulations are harmonized with existing laws, and supplement existing civil rights enforcement 50

II. The FTC should address harms of commercial surveillance and lax data security practices in education 51

A. The FTC should address commercial surveillance in education by enforcing existing limitations, extending those limitations to all students, and utilizing its Section 5 authority to protect marginalized groups 52

i. Commercial Surveillance in Education Causes Discriminatory Harms to Students 52

ii. Emphasize Existing Limitations under COPPA 55

iii. Extend Certain COPPA Privacy Protections to Ed Tech Companies and Other Contractors that Provide Services in the Education Context to All Students 56

iv. Utilize FTC Authority to Protect Historically Marginalized Groups 59

B. The FTC should address lax data security practices in education by extending existing data security requirements to ed tech providers and other contractors in the education setting 61

i. Lax Data Security Practices Harm Students and Schools 61

ii. Emphasize Existing Security Requirements under COPPA 62

iii. Extend COPPA Data Security Requirements to Ed Tech Companies and Other Contractors Providing Services in the Education Context to All Students 63

III. The FTC should regulate private vendors that provide identity verification for government service delivery 64

A. The FTC should protect privacy in identity verification services 66

B. The FTC should reduce algorithmic bias in identity verification services 67

Conclusion 68

Introduction

The Center for Democracy & Technology (CDT) welcomes the Federal Trade Commission's (FTC) Advance Notice of Proposed Rulemaking (ANPR) on Commercial Surveillance and Data Security.[1] CDT is a nonprofit, 501(c)(3) organization dedicated to advancing privacy, consumer, and civil rights for all in the digital age. CDT and fellow civil society advocates have long pushed for robust privacy protections for consumers in an expanding landscape of data harms, and the ANPR is a promising step toward achieving this goal through the FTC's authority.

The ANPR focuses its inquiries into two broad areas – data security and commercial surveillance. Our comments will focus primarily on "commercial surveillance" as defined in the ANPR – the expanse of consumer data collection, sharing, and processing practices that have become commonplace online. Part 1 describes the injuries that prevalent private sector practices cause to marginalized communities and consumers, and discusses how the FTC's rulemaking authority can address enforcement gaps under existing laws. Part 2 explains the impacts of the data practices of private contractors for educational institutions and other governmental entities and discusses how FTC rulemaking should be carefully scoped to address these harms.

Part 1: A privacy rule should address the risks of private sector commercial surveillance practices

For decades, companies have played by their own data rules. While the FTC has taken numerous actions against companies under its Section 5 authority to address unfair and deceptive practices, by and large the data ecosystem online has been allowed to run rampant with few checks against those practices. Companies collect extensive data on all consumers for a variety of reasons from fraud prevention to targeted advertising, and then retain that data indefinitely, potentially causing more harm. Data practices may be disclosed in a privacy policy but those policies are not written for the average consumer. As a result, most consumers have no idea what is happening with their data, and even if they did, they are powerless to change those practices. Many harmful data practices have become commonplace, with companies turning a blind eye to the harms their practices cause as long as the practices benefit the company.

CDT is heartened to see the FTC recognize that rules of the road are necessary. The time has long since passed to put an end to, or at least substantially limit, these harmful and abusive

[1] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (Aug. 22, 2022), https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security#citation-24-p51290.

online data practices. Below, we discuss the harms caused by several prevalent online data practices. We then provide recommendations for the FTC's rulemaking. Specifically, we urge the FTC to ensure that its rules on commercial surveillance

- Require data minimization and prevent secondary uses of data that can harm consumers;
- Require companies to provide accessible consumer controls to help consumers limit data collection; and
- Establish effective mechanisms for meaningful transparency to consumers about how their data is treated.

Part I concludes with a discussion of competition considerations for the FTC's rulemaking.

I. There are many prevalent private sector data practices that cause harms

The FTC can establish rules against unfair or deceptive practices that are prevalent under its Magnusson-Moss rulemaking authority.[2] An act or practice is 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."[3] An act or practice is deceptive if "there is a [material] representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[4]

A number of prevalent practices in the online ecosystem are unfair and deceptive under the FTC's standards. Many online business models rely on the ability to gather data from, or profile based on, people's online and offline activities, providing incentives and capabilities for

- extensive data collection and retention in various settings;
- unexpected secondary use of data;
- identifying people and combining data across many different contexts;
- targeting intrusive messages, which may be upsetting, manipulative, or misinforming;
- disclosure of personal information to advertisers or others; and
- discrimination through data processing affecting critical opportunities.

Commercial surveillance practices with these outcomes produce systemic, widespread patterns of harms – targeted to individual people or certain groups, or encountered by society as a whole. We appreciate that the ANPR explicitly acknowledges data harms based on race, sex, and age, and that the Chair's statement regarding this proceeding inquires about harms based

[2] 15 USC 57a(a)(1)(B), (b)(3). Prevalent practices are those that the FTC has issued cease and desist letters regarding, or if there is other information available to the FTC that the practice is widespread. *Id*. at (b)(3)(A)-(B).
[3] 15 U.S.C. 45(n).
[4] Federal Trade Commission, *Policy Statement on Deception* (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

on religion and national origin as well. However, the ANPR is notably silent on harms to people in the disabled and LGBTQ+ communities. Inappropriate purposes for and inadequate guardrails in companies' data use and processing can present heightened safety concerns and barriers for all of these marginalized communities.[5]

We cannot practically address the numerous online commercial surveillance practices that are unfair and deceptive. Accordingly, we focus on five prevalent practices with harms to consumers that should be addressed in this proceeding:

- Overcollection and secondary uses of sensitive data;
- Sharing or sale of data by data brokers for purposes to which consumers cannot consent;
- Collection and use of consumer data to target advertising;
- Discriminatory data- or algorithm-driven decisions that limit access to housing, credit, and employment;
- Data collection through dark patterns that curtail consumer choice.

A. Companies' excessive collection and secondary uses of sensitive data allow companies to monetize data while harming consumers.

Many online companies collect, use, share, and otherwise process sensitive data. Sensitive data includes various types of data such as health and financial data, content of communications, identification numbers, biometric information, location, and demographic information.[6] It can reveal insights about people like their financial wellbeing, the parties to and substance of their communications, disability status, health, movements and travels, and sexual activity. Its inappropriate use can lead to financial, reputational, physical, and emotional harm.[7]

People want their sensitive data protected and kept private. For example, when it comes to data about peoples' health, a recent American Medical Association (AMA) survey of patients found that they "are deeply concerned over the lack of security and confidentiality of personal health information."[8] The survey found that more "than 92% of people believe privacy is a right and

---

[5] *See generally* Henry Claypool, Claire Carey, Alexander C. Hart, & Linnea Lassiter, *American Association of People with Disabilities and Center for Democracy & Technology*, Centering Disability in Technology Policy: Issue Landscape and Potential Opportunities for Action (2021), https://cdt.org/wp-content/uploads/2021/12/centering-disability-120821-1326-final.pdf.

[6] *See e.g.* § 2(28)(a) of the "American Data Privacy and Protection Act" (H.R. 8152).

[7] Daniel J. Solove & Danielle Keats Citron, *Privacy Harms*, 102 Boston U. L. Rev. 793, 831-45 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222. Simply knowing that you are being surveilled can have real consequences for peoples' mental health. *See* Saumya Kalia, *What is a Constant Lack of Digital Privacy Doing to Our Mental Health?*, The Swaddle (Jan. 26, 2022), https://theswaddle.com/what-is-a-constant-lack-of-digital-privacy-doing-to-our-mental-health/.

[8] American Medical Association, *Patient Perspectives Around Data Privacy* (2022), https://www.ama-assn.org/system/files/ama-patient-data-privacy-survey-results.pdf.

their health data should not be available for purchase by corporations or other individuals."[9] Regarding financial information, in a 2021 Financial Health Network survey of over 2,000 consumers, respondents overwhelmingly preferred limits to data collection and sharing and greater control: 94% prefer that financial institutions do not share their data for marketing purposes, and 87% want to minimize fintech platforms' data collection to only the data needed.[10] In addition, 89% of consumers prefer that financial institutions' and fintech platforms' data sharing be subject to consumers' express opt-in, and 93% do not want fintech platforms to share their data with third parties for marketing purposes.

Sensitive data should enjoy strong privacy protections. The FTC recently released guidance affirming that it will enforce against misuse of sensitive data.[11] To reduce the potential for harm, the Commission should limit how sensitive data is collected, shared, retained, and used only for purposes that are strictly necessary to provide a product or service that a person has specifically requested.

Unfortunately, contrary to peoples' desire to have their sensitive data kept private, companies often collect and use sensitive data in harmful ways. Below, we discuss harms resulting from the prevalent overcollection and use of four examples of specific types of sensitive data – namely disability-related data, health data, location data, and financial data – and we explain how this practice falls squarely under the FTC's authority against unfair and deceptive practices.

i. Disability-related data

The Commission's request for information on specific risks of harm and discrimination for marginalized communities did not reference the disability community, but its rules should incorporate how disabled people are affected by data practices. CDT's work has explored the wide-ranging impacts of commercial data practices on disabled people that cause or further perpetuate existing discrimination and prejudice.[12] Disabled people have a long history of

---

[9] *Id.* The Survey also found the following:
• Almost 80% of participants want to be able to "opt-out" of sharing some or all their health data.
• More than 75% of patients want to opt-in before a company uses any of their health data.
• More than 75% of people want to receive requests prior to a company using their health data for a new purpose.

[10] Dan Murphy, David Silberman, & Stephen Arves, Financial Health Network, *Financial Data: The Consumer Perspective* 9-15 (2021), https://finhealthnetwork.org/wp-content/uploads/2021/04/Consumer-Data-Rights-Report_FINAL.pdf.

[11] Federal Trade Commission, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data*, https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

[12] *See* Lydia X. Z. Brown, Ridhi Shetty, Matthew U. Scherer, & Andrew Crawford, Center for Democracy & Technology, *Ableism And Disability Discrimination in New Surveillance Technologies* (2022),

experiencing online discrimination. People with physical and mental disabilities face substantially higher likelihood of potentially invasive personal data collection for a range of reasons, including discrimination that creates further records such as through evictions or arrests,[13] and through interactions with governmental entities because of greater reliance on public benefits and social services.[14]

Some disabled people are also more likely to need or want to use health-related apps and platforms, but these apps and platforms can exploit the sensitive disability-related data people are required to share to use these services. For example, Mozilla researchers found that mental health (as well as prayer apps) fare worse than any other product category they examined with regards to protecting people's privacy and security.[15] The apps Mozilla reviewed routinely collected, retained, and shared sensitive data about users' conditions like depression, anxiety, suicidality, victimization by domestic violence, disordered eating, and post-traumatic stress disorder.[16] This includes heavily promoted therapy apps like BetterHelp and Talkspace that share user data with Facebook - and users' presence on these apps itself is a data point that can be exploited for marketing.[17] Pride Counseling, an app specifically designed for the LGBTQ+ community, suffers from similar concerns as its parent company, BetterHelp, and it does not clarify whether users have to opt in or opt out to avoid their data being repurposed for marketing.[18]

Mozilla found that certain apps also allow weak passwords, target users with personalized ads, and feature vague and poorly written privacy policies that are too ambiguous regarding the kinds of data they accumulate and how they use it. For instance, the Better App Company's suicide prevention app offers a privacy policy that appears incomplete and is certainly unclear about its data collection and sharing and how its data use supports people experiencing suicidality or a mental health crisis, both of which are disability-related experiences.[19] NOCD, which aims to help people manage obsessive compulsive disorder, shares personal non-health

---

https://cdt.org/insights/ableism-and-disability-discrimination-in-new-surveillance-technologies-how-new-surveillance-technologies-in-education-policing-health-care-and-the-workplace-disproportionately-harm-disabled-people/ [hereinafter Brown, *Surveillance Technologies*].

[13] *See* Part 1, Sec. I(D)(i).

[14] *See* Part 2, Sec. III.

[15] 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/.

[16] *Id.*

[17] Thomas Germain, *Mental Health Apps Aren't All as Private as You May Think*, Consumer Reports (Mar. 2, 2021), https://www.consumerreports.org/health-privacy/mental-health-apps-and-user-privacy-a7415198244/.

[18] Pride Counseling, *Privacy Policy* (last updated Sept. 21, 2022), https://www.pridecounseling.com/privacy/ (stating that data will be disclosed to advertising partners if users opt in to targeting cookies, but also that users should follow certain steps to opt out of cookies).

[19] The Better App Company, *Privacy* (last updated Sept. 14, 2018), https://www.thebetterappcompany.com/privacy.

user data (of a user base defined by a disability diagnosis) with data analytics providers like Google and Meta for targeted advertising.[20]

Some companies collect people's mental health data from social media posts and then take further, potentially harmful or unhelpful, action related to that information. For instance, social media platforms like Facebook have algorithms that purport to detect suicide risk, and they may flag content and either transmit this information to law enforcement that is ill-equipped to engage disabled people in need of support, or refer people to resources that they may not find helpful either to address an immediate crisis or seek long-term support.[21]

Many Internet of Things (IoT) devices and internet-connected assistive technologies can store excessive amounts of data – the inherent privacy risk is a tradeoff that people with certain disabilities may be obligated to accept because they rely on the support these technologies can offer to independently perform certain tasks that might otherwise require another person's assistance.[22] These technologies can, for instance, help people with physical disabilities manage their home lighting, temperature, or security systems without having to do so manually.[23] However, the data collected through these technologies is subject to third-party data-sharing and cloud storage, which could make users vulnerable to data breaches.[24]

Some of this data includes biometric data processed for security purposes, while other data can convey information about a person's daily habits and activities to third parties. For instance, data analytics company Verisk gathers behavioral data from smart home devices to inform insurers' risk evaluations for life, auto, and property insurance products.[25] This practice increases the risk of harm to disabled people who rely on internet-connected assistive

---

[20] NOCD, *Privacy Policy* (last updated Aug. 3, 2022), https://www.treatmyocd.com/privacy-policy.

[21] Karen L. Celedonia, Marcelo Corrales Compagnucci, Timo Minssen, & Michael Lowery Wilson, *Legal, Ethical and Wider Implications of Suicide Risk Detection Systems in Social Media Platforms*, J. L. Biosci. (2021), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8284882/; Benjamin Goggin, *Inside Facebook's Suicide Algorithm: Here's How the Company Uses Artificial Intelligence to Predict Your Mental State From Your Posts*, Bus. Insider (Jan. 6, 2019, 11:19 AM), https://www.businessinsider.com/facebook-is-using-ai-to-try-to-predict-if-youre-suicidal-2018-12.

[22] *See* Claypool et al., *supra* n. 5, at 41.

[23] *Id.*

[24] Lauren Smith, Carson Martinez, Chanda Marlowe, & Henry Claypool, Future of Privacy Forum, *The Internet of Things (Iot) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions* 10-14 (2019), https://fpf.org/wp-content/uploads/2019/01/2019_01_29-The_Internet_of_Things_and_Persons_with_Disabilities_For_Print_FINAL.pdf.

[25] Verisk, *The Verisk Data Exchange: Personal and Commercial Property IoT*, https://www.verisk.com/insurance/capabilities/telematics/property-iot/; Sandra Maples, *How Smart Devices are Providing the Data Claims Professionals Need*, Verisk (Oct. 3, 2017), https://www.verisk.com/insurance/visualize/how-smart-devices-are-providing-the-data-claims-professionals-need/.

technologies because insurers can repurpose data collected from these devices to terminate coverage or increase premiums for a group of people more likely to include disabled users.[26] The risk is even greater in light of the fact that smart home devices are already known to be susceptible to security breaches – for example, hackers have been able to take control of Google Nest and Amazon Ring devices to harass consumers in their homes.[27]

For the above reasons, the FTC's privacy rules should incorporate protections for disabled people, including prohibitions on the use of data to discriminate against disabled people.

ii. Health Data

Health data (both disability-related and unrelated to disability) is particularly private and has historically been provided extra protections like those found in the Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA and its associated Privacy Rule place limitations on the disclosure and sharing of protected health information.[28] However, HIPAA does not address all health data. Instead, HIPAA's privacy protections affect health data only when it is in the possession of "covered entities" – doctors, insurance companies, and those who support them. HIPAA does not apply when health data is held by a non-covered entity – like health and wellness apps, wearable fitness trackers, websites, and data brokers. The ever-increasing use and popularity of these health-related apps, devices, online services, and IoT has resulted in extraordinary amounts of information reflecting mental and physical health being collected, retained, shared, and used by entities that are not bound by HIPAA obligations. Regulations finalized in spring 2020 further shrunk the categories of HIPAA-protected data.[29]

---

[26] Tenzin Wangmo, Mirjam Lipps, Reto W. Kressig, & Marcelo Ienca, *Ethical Concerns With the Use of Intelligent Assistive Technology*, 20 BMC Med. Ethics 8, https://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-019-0437-z.

[27] Hayley Peterson, *Wisconsin Couple Describe the Chilling Moment That a Hacker Cranked Up Their Heat and Started Talking to Them Through a Google Nest Camera in Their Kitchen,* Bus. Insider (Sept. 25, 2019, 4:12 PM), https://www.businessinsider.com/hacker-breaks-into-smart-home-google-nest-devices-terrorizes-couple-2019-9; Kari Paul, *Dozens Sue Amazon's Ring After Camera Hack Leads to Threats and Racial Slurs*, The Guardian (Dec. 23, 2020, 4:40 PM), https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats.

[28] Department of Health & Human Services, *Summary of the HIPAA Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[29] 85 Fed. Reg. 25642 (May 1, 2020) and 85 Fed. Reg. 25510 (May 1, 2020). For a comprehensive review of the current legal landscape governing health data and the gaps in protection for the same, *see* Robert Belfort, William S. Bernstein, Alex Dworkowitz, Brenda Pawlak, and Po Yi, Manatt, *A Shared Responsibility: Protecting Health Data Privacy in an Increasingly Connected World* (2020), https://www.manatt.com/Manatt/media/Media/PDF/White%20Papers/Healthcare-Whitepaper-RWJF-Protecting-Consumer-Health-Data-Privacy-in-an-Increasingly-Connected-World_e.pdf.

The Commission itself has long recognized the sensitivity of health data and the harms associated with unfair and deceptive data practices that result when consumer data is shared and used in unanticipated and unknown ways. Recently, for example, the Commission took enforcement action against Flo, a reproductive health app, collected sensitive health data (like dates of menstrual cycles, when pregnancies started and ended, menstrual and pregnancy-related symptoms, weight, and temperature) from its millions of users and shared that data with outside analytics providers.[30] Flo told consumers that their sensitive health data would be shared and used in limited ways.[31] However, in practice, Flo was sharing consumers' data with a number of third parties for purposes unrelated to the core service provided by the app.[32] The FTC put an end to this practice and ultimately ordered Flo to obtain affirmative express consent from consumers before sharing sensitive health data with third parties.[33] More recently, Flo began offering an "anonymous mode" that allows users to prevent the sharing of any unique user identifiers.[34]

Health-related data collected, shared, and used by consumer-facing tech can be extremely personal and sensitive, and inappropriate use or sharing of such data can lead to a variety of harms. For example, data about conditions that are especially sensitive because of accompanying, unwarranted prejudice can lead to social stigmatization, discrimination or even threats of violence. An analysis of the 2017 National Crime Victimization Survey found that LGBTQ+ people are nearly four times more likely than non-LGBTQ+ people to experience violent victimization by people they know and by strangers.[35] Because parts of the LGBTQ+ community experience disproportionately higher rates of HIV, exposing that a person is HIV-positive potentially puts them at heightened risk of violence.[36]

Just such a risk arose when an app used by members of the LGBTQ+ community, the dating app Grindr, shared user data in an unfair and harmful manner.[37] Grindr "provided users' HIV status

---

[30] Complaint, In the Matter of Flo Health, Inc., File No. 1923133 (2021), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf.
[31] *Id.*
[32] *Id.*
[33] Decision and Order, In the Matter of Flo Health, Inc, File No. 1923133 (2021), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_decision_and_order.pdf.
[34] Flo, *Flo Anonymous Mode Overview* (2022), https://flo.health/flo-health-inc/news/anonymous-mode-whitepaper.
[35] Andrew R. Flores, Lynn Langton, Ilan H. Meyer, and Adam P. Romero, *Victimization Rates and Traits of Sexual and Gender Minorities in the United States: Results from the National Crime Victimization Survey, 2017* (2020), https://www.science.org/doi/10.1126/sciadv.aba6910.
[36] Human Rights Campaign, *How HIV Impacts LGBTQ People* (Feb. 2017), https://www.hrc.org/resources/hrc-issue-brief-hiv-aids-and-the-lgbt-community.
[37] Alison Bateman-House, *Why Grindr's Privacy Breach Matters to Everyone*, Forbes (Apr. 10, 2018, 10:09 AM), https://www.forbes.com/sites/alisonbatemanhouse/2018/04/10/why-grindrs-privacy-breach-matters-to-everyone/?sh=2a09490567f4.

and GPS location data, along with other profile details including email addresses, to two companies hired to test the app's technical performance."[38] News accounts noted that "[b]ecause Grindr users would have reasonably expected the app to be vigilant in guarding such information, its failure to do so is not only a breach of their privacy but an actual harm."[39]

Potential harms from collection and sharing of health information can also extend to risk of investigation, litigation, and prosecution. The recent overturning of *Roe v. Wade* in *Dobbs v. Jackson Women's Health Organization*,[40] and subsequent criminalization of abortion in some states, has created new cause for concern about reproductive health data. Such data, whether collected directly from an online company or from a data broker, could be used to enforce those laws if it reveals that a person obtained, or attempted to obtain, an abortion or aided another in doing so. For example, anti-choice groups have used data linked to people's advertising IDs on their smartphones to target patients and send pro-life advertisements "directly to a woman's phone while she is in a clinic waiting room."[41] The same technology "also has the capability to hand the names and addresses of women seeking abortion care, and those who provide it, over to anti-choice groups."[42] In the wake of *Dobbs,* that data could be used in some states by law enforcement to launch criminal investigations and prosecutions, as well as civil suits by "bounty hunters" against those seeking abortions.[43] That risk remains even when people go out of their way to attempt to keep their reproductive health data private since it is difficult to avoid collection of all data that may be revealing about reproductive health care choices.[44]

In recognition of this risk of harm, the FTC recently took action against data broker Kochava for allegedly selling location information about millions of mobile devices that can reveal people's visits to sensitive locations like reproductive healthcare clinics, houses of worship, and addiction treatment facilities.[45] Kochava is not the only data broker putting people's health data at risk: SafeGraph and PlacerAI are among others collecting and sharing data about the locations and durations of people's visits to reproductive health clinics, which could cause significant

---

[38] *Id.*
[39] *Id.*
[40] 597 U.S. ___ (2022).
[41] Sharona Coutts, *Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits*, Rewire News Group (May 25, 2016, 6:52 PM), https://rewirenewsgroup.com/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/.
[42] *Id.*
[43] Albert Fox Cahn & Eleni Manis, *Surveillance Technology Oversight Project, Pregnancy Panopticon: Abortion Surveillance After Roe* (2022), https://www.stopspying.org/pregnancy-panopticon.
[44] Anya E.R. Prince, *I Tried to Keep My Pregnancy Secret*, The Atlantic (Oct. 10, 2022), https://www.theatlantic.com/ideas/archive/2022/10/can-you-hide-your-pregnancy-era-big-data/671692.
[45] Complaint, Federal Trade Commission v. Kochava, No. 2:22-cv-377 (D. Idaho Aug. 29, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf.

monetary harm or even imprisonment.[46] This risk is particularly troubling as new, obscure sources of reproductive health data emerge: one new wellness start-up called 28 uses basic menstrual cycle data to make lifestyle recommendations; while it claims to only "voluntarily collect" data and to keep it "strictly confidential," its privacy policy indicates more expansive collection of data that will be disclosed to third parties.[47]

Consumers can be harmed when health data is used as part of a profile that results in them being denied, or not even offered, economic opportunities. A *New York Times* investigative piece from May 2021 examined the data and privacy practices of 250 iPhone apps and revealed that of the twenty health apps they reviewed, "13 apps shared with an average of three third-party trackers."[48] The *Times* piece goes on to note that, while it is difficult to track exactly how some of the third parties that receive data about users' health use that information, they do know that some data is used by tools that can "generate a health-risk prediction score that is then provided to life insurance companies to assess whether people may be interested in their product."[49] Researchers at the University of Pennsylvania have also documented how most health-related websites track people who visit each site.[50] The researchers note that this health data can not only be used to target ads but may also include "much more damaging privacy loss and the domino effect that could have on credit scores, insurance coverage, and many as-yet-undiscovered facets of someone's life."[51] Likewise, sharing consumer health data with an employer can have real-life impacts on access to a job.[52]

When data from consumer-facing tech is being used for health purposes like diagnosis or access to benefits, inaccurate, unrepresentative, or incomplete data can result in negative health outcomes, or in lost or denied services and benefits, especially for people from

---

[46] Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, Vice (May 3, 2022), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood; Joseph Cox, *Location Data Firm Provides Heat Maps of Where Abortion Clinic Visitors Live*, Vice (May 5, 2022, 8:24 PM), https://www.vice.com/en/article/g5qaq3/location-data-firm-heat-maps-planned-parenthood-abortion-clinicsplacer-ai.

[47] Natasha Lomas, *Cycle-Focused Femtech Startup, 28, Grabs Backing From Thiel Capital*, TechCrunch (Aug. 23, 2022, 9:10 AM), https://techcrunch.com/2022/08/23/28-seed-thiel-capital/; 28, *Privacy Policy* (last modified Sept. 7, 2022), https://28.co/privacy.

[48] Thorin Klosowski, *We Checked 250 iPhone Apps – This is How They're Tracking You*, N.Y. Times: Wirecutter (May 6, 2021), https://www.nytimes.com/wirecutter/blog/how-iphone-apps-track-you/.

[49] *Id.*

[50] Michele W. Berger, *What Can Browser History Inadvertently Reveal About a Person's Health?*, University of Pennsylvania: Penn Today (Apr. 29, 2022), https://penntoday.upenn.edu/news/what-browser-history-inadvertently-reveals-Penn-CMU-digital-health-privacy-initiative.

[51] *Id.*

[52] Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data With Your Boss?*, Wash. Post (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/.

underrepresented and overlooked communities.[53] For instance, *Wired* reported that predictive health technologies frequently rely upon skewed, unrepresentative data sets that "are the norm in health AI research, due to historical and ongoing health inequalities."[54]

Finally, certain data practices limit individual autonomy and can cause collateral harms in other areas of life. For example, people used the Crisis Text Line, a nonprofit mental health hotline, to seek help for problems such as suicidal thoughts, anxiety, and emotional abuse. When using the service, people disclosed highly personal and sensitive information. While users expected their data would be kept private, news reports exposed how the Crisis Text Line shared people's personal and sensitive data with a for-profit spinoff.[55] The company ended this data-sharing relationship after reports detailing its troubling data practices emerged.[56]

The risk of these and other harms is unfortunately high. Many health apps are failing at protecting privacy. Last year, the International Digital Accountability Council (IDAC) released a report that assessed the consumer protection risks of 152 digital health apps that utilize the most sensitive personal information, and classified these apps into three categories: femtech, mental health, and fitness and weight loss.[57] IDAC's report details that "some widely-used apps fail to meet even basic platform requirements because they send unencrypted user data, have inadequate or missing privacy policies, or collect granular information about user location without adequate explanation."[58]

The findings did not stop there. IDAC continued that "the majority of apps investigated have questionable practices and disclosures around third-party data sharing, illustrating a clear mismatch between current legal protections and the widespread collection and sharing of sensitive health information."[59] For example, in some instances IDAC investigators "observed

---

[53] Andrew Crawford, Center for Democracy & Technology, *Placing Equity at the Center of Health Care & Technology* 13 (2022), https://cdt.org/wp-content/uploads/2022/03/2022-03-22-CDT-Placing-Equity-at-the-Center-of-Health-Care-Technology-final.pdf [hereinafter Crawford, *Placing Equity*].

[54] Tom Simonite, *When It Comes to Health Care, AI Has a Long Way to Go*, Wired (Jan. 16, 2022, 7:00 AM), https://www.wired.com/story/health-care-ai-long-way-to-go/.

[55] John Hendel, *Crisis Text Line Ends Data-Sharing Relationship With For-Profit Spinoff*, Politico (Jan. 31. 2022, 8:37 PM), https://www.politico.com/news/2022/01/31/crisis-text-line-ends-data-sharing-00004001.

[56] *Id.*

[57] The report examined 152 Android health apps that were available in the Google Play Store as of November 10, 2021, selected using keyword search results. Holden Williams, Ginny Kozemczak, and Dan Kinney, Int'l Digital Accountability Council, *Digital Health is Public Health: Consumers' Privacy & Security in the Mobile Health App Ecosystem* (2021), https://secureservercdn.net/198.71.190.114/99x.577.myftpupload.com/wp-content/uploads/2022/01/Digital-Health-is-Public-Health-Consumers-Privacy-and-Security-in-the-Mobile-Health-App-Ecosystem.pdf.

[58] *Id*. at 1.

[59] *Id.* at 2.

transmission of users' advertising identifiers to at least one third-party endpoint that was not disclosed in the app's privacy policy."[60] Even when apps made some disclosures to users, some failed to state all the third-party services that IDAC observed.[61] IDAC noted that even in instances when "apps carefully follow existing rules, most users have little visibility into how their information is collected or shared."[62]

There are myriad ways that health data can cause harm, and the FTC's privacy rulemaking should incorporate protections for that data.

iii. Location Data

A broad variety of apps and tools collect and then share users' location data with third parties. The *New York Times'* examination of 250 apps, discussed above, found that numerous shopping, news, and dating apps gather and share location data.[63] Of the twenty weather apps examined, for example, fourteen used location information to track devices.

When used in unwanted, unanticipated, or unknown ways, location data can harm people, and even more so when it allows inferences specific to marginalized consumers. Knowing a person's current or previous physical movements can be very intrusive and cause significant harm.[64] The Commission's recent action against Kochava, discussed above, stated that the data broker collected and then sold people's precise geolocation data in a format that allowed entities to track people's "movements to and from sensitive locations, including, among others, locations associated with medical care, reproductive health, religious worship, mental health, temporary shelters, such as shelters for the homeless, domestic violence survivors, or other at risk populations, and substance use recovery."[65]

Additionally, late last year, *The Markup* published a story that detailed how Life360, a popular family safety app, was selling location data about its users to data brokers.[66] After the story was

[60] *Id.* at 12.
[61] *Id.*
[62] *Id.* at 2.
[63] Klosowski, *supra* n. 48.
[64] Andrew J. Blumberg & Peter Eckersley, Electronic Frontier Foundation, *On Locational Privacy, and How to Avoid Losing it Forever* (2009), https://www.eff.org/wp/locational-privacy; Samantha Lai & Brooke Tanner, Examining the Intersection of Data Privacy and Civil Rights, Brookings (July 18, 2022), https://www.brookings.edu/blog/techtank/2022/07/18/examining-the-intersection-of-data-privacy-and-civil-rights .
[65] Complaint, Federal Trade Commission v. Kochava, *supra* n. 45.
[66] Jon Keegan & Alfred Ng, *The Popular Family Safety App Life 360 is Selling Precise Location Data on Its Tens of Millions of Users*, The Markup (Dec. 6, 2021, 8:00 AM), https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user.

published, "Life360 announced that it will stop sales of precise location data to the dozen or so data brokers it had been working with, and will now sell only precise location data to Arity and 'aggregated' location data to PlacerAI."[67] However, precise location data is not the only type of location data that poses risks: the *New York Times* was able to review anonymized location data and conclude that "[i]n most cases, ascertaining a home location and an office location was enough to identify a person."[68] As a result, companies can use location data to infer people's activities and make decisions accordingly, such as increasing insurance rates based on where people are traveling, or scrutinizing prospective rental applicants' activities.[69]

The problem extends to other types of apps and tools as well. Last year, a priest resigned after a Catholic media site obtained location data from the dating app Grindr to reveal his visits to gay bars.[70] A user's location data indicating that they have gone to a venue catering to LGBTQ+ communities was also shared with the app's advertising partners to target LGBTQ+-related advertisements that others accessing the user's device may see, which could out the user to those close to them.[71] Some prayer apps share users' location data, which can be obtained by the government.[72] Indeed, the Council on American-Islamic Relations filed a complaint with the FTC earlier this year describing how the sale of location data to government agencies constitutes a deceptive practice for users in general and an unfair practice particularly for historically hyper-surveilled communities.[73]

Similar concerns extend to apps that do not need location data to function and only collect it for purposes such as advertising. For example, the FTC took action in 2013 against Goldenshores Technologies, the developer of the Brightest Flashlight app, for its location data collection and

---

[67] *Id.*
[68] Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.
[69] Keegan, *supra* n. 66; Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone,* Vice Motherboard (Jan. 18, 2019, 12:08 PM).
[70] Michelle Boorstein, Marisa Iati, and Annys Shin, *Top U.S. Catholic Church Official Resigns After Cellphone Data Used to Track Him on Grinder and to Gay Bars*, Wash. Post (July 21, 2021, 8:21 AM), https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-burrill/.
[71] Sarah Syed, Natalia Drozdiak, & Nate Lanxon, *Grindr Shares Location, Sexual Orientation Data, Study Shows*, The Detroit News (Jan. 14, 2020, 10:22 AM), https://www.detroitnews.com/story/business/2020/01/14/grindr-shares-location-sexual-orientation-data-study-shows/40997573/; Chris Wood, Katelyn Ringrose, Carlos Gutierrez, Amie Stepanovich, & Connor Colson, LGBT Tech and Future of Privacy Forum, *The Role of Data Protection in Safeguarding Sexual Orientation* 9, 13 (2022), https://www.lgbttech.org/_files/ugd/1b643a_21883c316e1547c99c6a1d997688f975.pdf.
[72] Mozilla, *supra* n. 15; Joseph Cox, *How the U.S. Military Buys Location Data From Ordinary Apps*, Vice (Nov. 16, 2020, 10:35 AM), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.
[73] Complaint, In the Matter of Request for Investigation of Alleged Violations of Section 5 of the FTC Act by Multiple Actors in the Location Data Industry (2022), https://www.cair.com/wp-content/uploads/2022/04/FTCcomplaint.pdf.

sharing practices.[74] Mobile game apps like "Angry Birds" were also reported to collect location and other data and transmit it to government entities.[75] And many of the data brokers collecting location data for reproductive purposes came from the software development kits of apps that were collecting location for no, or other, purposes.[76]

iv. Financial data

Consumers have more options than ever to make payments and transfer funds online, which means that financial data is proliferating online and can put consumers at risk. This information includes names, addresses and other contact information, credit card numbers, bank account information, dates of birth, Social Security numbers, banking activity, transaction history, and purchase activity, which can make consumers vulnerable to data misuse when accessed by third parties.[77] Much of this data is stored not only by financial institutions, but also by online retailers and large and start-up financial technology (or fintech) platforms.[78] One risk arising from the overcollection and sharing of financial data is that of identity theft, fraud, and other financial crimes. For example, the more entities that possess and store this information, the greater the risk of a breach or other unauthorized access by bad actors.

Misuse of financial data also gives rise to other risks. Technology companies that have historically used consumer data for a whole host of non-financial purposes, from communication and social networking to navigation to media streaming, have introduced payment processing services. This adds financial data to the wealth of data that companies with burgeoning online advertising businesses can wield to profile consumers' behavior for potential profit. For instance, Meta and Amazon use and share consumers' purchase activity, along with other data such as location and device identifiers, to tailor advertisements, measure how well

[74] Federal Trade Commission, Press Release, Android Flashlisht App Developer Settles FTC Charges it Deceived Consumers (Dec. 5, 2013), https://www.ftc.gov/news-events/news/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived-consumers.
[75] James Ball, *Angry Birds and 'Leaky' Phone Apps Targeted by NSA and GCHQ for User Data*, The Guardian (Jan. 28, 2014, 2:51 AM), https://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data.
[76] Joseph Cox, *Data Broker is Selling Location Data of People Who Visit Abortion Clinics*, Vice Motherboard (May 3, 2022, 12:46 PM), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood.
[77] Center for Democracy & Technology, Comments Regarding CFPB Inquiry Into Big Tech Payment Platforms 3, (Dec. 20, 2021), https://cdt.org/wp-content/uploads/2021/12/CDT-Comments-to-CFPB-on-Big-Tech-Payment-Systems-Docket-No-CFPB-2021-0017.pdf.
[78] Stan Adams & John Morris, Jr., Center for Democracy & Technology, *Open Banking: Building Trust* (2021), https://cdt.org/wp-content/uploads/2021/05/CDT-2021-05-25-Open-Banking-Building-Trust-FINAL.pdf.

products are meeting the companies' goals, and inform new products.[79] This also makes it harder for consumers to discern the purposes for which they can expect the companies to use financial data.

Companies that have mainly used consumers' financial data to provide online payment processing services now use and share data for marketing as well. PayPal shares consumers' contact information, bank account and purchase data, and IP addresses with a wide network of third parties for more expected purposes like payment processing and fraud detection, but also for less anticipated purposes like personalization and marketing.[80] In 2019, Mozilla researchers demonstrated the ease with which Venmo users' transaction data could be used to gain insights about users' social connections and financial and non-financial personal activity, which in turn facilitates stalking and fraudulent use of identifiable data.[81]

Existing laws relevant to protecting financial data only go so far. The Gramm-Leach-Bliley Act only applies to financial institutions, which have not been clearly defined to include the technology companies and data aggregators whose access to and control over financial data has grown.[82] The Fair Credit Reporting Act (FCRA) imposes obligations on entities who evaluate and assemble consumer data to furnish it to other entities for enumerated permissible purposes.[83] Marketing is not among these permissible purposes, but companies that use consumer data for marketing argue that they are not consumer reporting agencies and thus are not liable under the FCRA.

As a result, there remains a significant gap in which the privacy of financial data remains unregulated, and the FTC can fill that gap in its privacy rule.

* * *

[79] Meta, *Privacy Policy* (effective July 26, 2022), https://www.facebook.com/privacy/policy/?section_id=2-HowDoWeUse; Amazon, *Amazon.com Privacy Notice* (last updated Jun. 29, 2022), https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ.
[80] PayPal, *List of Third Parties (Other Than PayPal Customers) With Whom Personal Information May be Shared* (effective Oct. 1, 2022), https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list.
[81] Letter from Electronic Frontier Foundation and Mozilla to PayPal (Aug. 28, 2019), https://www.eff.org/document/open-letter-venmo.
[82] *Cyber Threats, Consumer Data, and the Financial System: Hearing before the H. Subcomm. on Consumer Prot. and Fin. Inst. of the H. Comm. on Fin. Serv.* (2021) (testimony of Samir Jain, Director of Policy, Center for Democracy & Technology), https://cdt.org/wp-content/uploads/2021/11/hhrg-117-ba15-wstate-CDT-Samir-Jain20211103-House-Financial-Commitee-testimony.pdf.
[83] 15 U.S.C. §1681b.

The overcollection and secondary uses of sensitive data constitute an unfair practice for the following reasons:

- *Substantial injury:* As set forth above, the overcollection and misuse of disability-related, health, location, and financial data causes substantial injury to consumers. If companies need such data to provide their service to their customers, then collection should be allowed. But companies should not be allowed to collect any data they want in the hopes that they can monetize it through advertising or sale, or otherwise use it for purposes unrelated to the service.
- *Not reasonably avoidable:* Overcollection of data online is everywhere. There are few if any requirements against collecting any data a company wants, so long as it is not deceptive about the collection, or otherwise unfair in its practices. While there are some smaller privacy-protective companies, most large tech companies, including the most prominent social media companies, overcollect data and consumers cannot avoid it by moving to competing services because few exist. Those competitors that do exist suffer from lack of network effects, making them undesirable for most consumers to join. For example it is likely impossible for most people to recreate their Instagram networks on BeReal.
- *Not outweighed by countervailing benefits to consumers or competition:* Overcollection of data is not outweighed by countervailing benefits to consumers or competition. What minor revenue-based benefit a company may receive by overcollecting data does not justify the extensive harms, discussed above, caused by the careless and wonton collection of data for its own sake.

Because the prevalent collection and secondary use of sensitive disability-related, health, location, and financial data poses such heightened risks as to amount to an unfair practice, restrictions on this collection and use should be a priority for FTC rulemaking.

B. Data broker practices violate people's privacy.

As described above, sensitive health, location, and financial data are major targets for data brokers, which are companies that knowingly collect data about consumers from sources other than the consumer themselves and sell the data to third parties.[84] However, data brokers traffic in all kinds of data, as we learned from the 2013 and 2014 reports from the Senate Committee on Commerce, Science, and Transportation and the FTC (respectively) analyzing the privacy risks

[84] Justin Sherman, *Federal Privacy Rules Must Get "Data Broker" Definitions Rights*, Lawfare (Apr. 8, 2021, 11:00 AM), https://www.lawfareblog.com/federal-privacy-rules-must-get-data-broker-definitions-right.

and lack of transparency with respect to data brokers' practices.[85] Little has changed since this extensive work – in fact, the data broker industry has since expanded to derive consumer data from a wider network of data sources. California and Vermont have established data broker registries that each surpass five hundred data brokers.[86]

Consumers have little insight into how these profiles are formed and how the data broker network uses this data. Companies that purport to inform consumers about how their data is shared often bury details about sprawling networks of third parties that receive and use consumer data, within voluminous privacy policies. Consumers do not have to go far to run into data brokers – as the FTC reports, even internet service providers sell and share online users' data with third parties.[87] For example, Comcast's privacy policy puts the burden on consumers to opt out of the sharing of non-personally identifiable information, which includes IP addresses and account numbers.[88] AT&T's privacy policy goes further, stating that it does not require consumer consent to share consumers' personal data with vendors that provide services such as marketing and advertising delivery.[89]

Accountability is difficult to achieve in the data broker network, because the data can be repurposed for uses other than the purpose for which it was previously sold, and certainly for uses other than what consumers reasonably expect based on any insight they do have.[90] This is complicated further by the fact that the roles of companies that share consumer data have blurred or expanded, leaving consumers even more uncertain about exactly what data is shared and where. For instance, platforms like Facebook that were once mainly spaces for socializing have grown into spaces for advertising, shopping, and processing financial transactions, while

---

[85] Staff of S. Comm. on Com., Sci., and Transp., 113th Cong., *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes* (2014), https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577; Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[86] California Department of Justice, https://oag.ca.gov/data-brokers; Vermont Secretary of State, https://bizfilings.vermont.gov/online/DatabrokerInquire/DataBrokerSearch.

[87] Federal Trade Commission, *A Look at What ISPs Know About You: Examining Privacy Practices of Six Major Internet Service Providers* (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.

[88] Comcast Xfinity, *Our Privacy Policy Explained* (effective Oct. 12, 2021), https://www.xfinity.com/privacy/policy#privacy-who.

[89] AT&T, *AT&T Privacy Policy* (effective June 6, 2022), https://about.att.com/privacy/full_privacy_policy.html.

[90] Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim, and Dhanaraj Thakur, *Legal Loopholes and Data for Dollars* 12 (2021), https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers/.

platforms like Venmo that are primarily payment platforms have adopted features of social media.[91]

Third-party data sharing can have even more severe consequences for marginalized communities. For instance, LexisNexis and Thomson Reuters are among the most prominent data brokers compiling large quantities of personal data to sell to immigration authorities. The compiled data includes publicly available information as well as data from utility companies' records, but reports show it is then used to target immigrant communities and punish immigration activists for exercising their rights to free speech and protest.[92] Another example is Verisk, which reportedly sells the data it collects from companies that provide connected home and mobile devices, as well as personally identifying information like phone numbers and addresses, to insurers who use the data to set rates for insurance products.[93]

Other data brokers take the form of people-search platforms like Spokeo that combine personal data with publicly available data, providing more granular information to users who pay for premium access.[94] When accurate, the resulting information can enable abusers to stalk victims of intimate partner violence, and it can in turn be shared to other websites.[95] When inaccurate, the data may erroneously influence decisions that involve background checks, such as in housing or employment.[96] The FTC has taken action in the latter circumstance, arguing that Spokeo violated the FCRA when it failed to maintain reasonable procedures to verify the users of its information and whether the use was for a permissible purpose.

---

[91] Jack Morse, *Payment Apps Collect and Share Your Data. Here's How to Lock Them Down.*, Mashable (June 9, 2021), https://mashable.com/article/venmo-cash-app-paypal-data-privacy. *See also* Comments Regarding CFPB Inquiry Into Big Tech Payment Platforms, *supra* n. 77.

[92] *LexisNexis Illegally Collected and Sold People's Personal Data, Lawsuit Alleges*, CBS News (Aug. 16, 2022, 3:16 PM), https://www.cbsnews.com/news/lexisnexis-lawsuit-collected-sold-personal-data-immigration-advocates-allege/; Max Rivlin-Nadler, *How ICE Uses Social Media to Surveil and Arrest Immigrants*, The Intercept (Dec. 22, 2019, 8:00 AM), https://theintercept.com/2019/12/22/ice-social-media-surveillance/.

[93] Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals*, Duke U. Sanford Cyber Policy Program 6-7 (2021), https://sites.sanford.duke.edu/techpolicy/wp-content/uploads/sites/17/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.

[94] Mara Hvistendahl, *I Tried to Get My Name Off People-Search Sites. It Was Nearly Impossible.*, Consumer Reports (Aug. 20, 2020), https://www.consumerreports.org/personal-information/i-tried-to-get-my-name-off-peoplesearch-sites-it-was-nearly--a0741114794/.

[95] Kaveh Waddell, *How FamilyTreeNow Makes Stalking Easy*, The Atlantic (Jan. 17, 2017), https://www.theatlantic.com/technology/archive/2017/01/the-webs-many-search-engines-for-your-personal-information/513323/.

[96] Steven Melendez, *When Background Checks Go Wrong*, Fast Company (Nov. 17, 2016), https://www.fastcompany.com/3065577/when-background-checks-go-wrong.

The CFPB recently took steps to clarify that the permissible purposes for compiling and furnishing data under the FCRA apply only with respect to the consumer whose data is the subject of the data user's request. The CFPB explained that consumer reporting agencies violate the FCRA when sharing consumer report data of multiple consumers because the shared data would include consumers for whom the user did not have a permissible purpose to request the data.[97]

Companies' sharing of consumer data with data brokers constitutes a deceptive practice because companies use hard-to-read privacy policies and vague notices, that may also be difficult to find, to make confusing, unclear, and misleading representations to consumers about how, when, and with whom their data is shared, inducing consumers to continue interacting with a website or app they have been misled to trust. Further, because data brokers repurpose consumer data in ways that consumers cannot reasonably expect, consumers cannot be truly informed about how their data is accessed and used – an omission that misleads consumers to their detriment when their data is abused.

Data brokers' sharing of consumer data also constitutes an unfair practice:

- *Substantial injury:* The sharing of consumer data with data brokers exposes consumers to secondary uses and repurposing of their data by companies that consumers do not choose to interact with and that consumers may not even be aware of. This practice allows consumer data to be obtained by third parties that may handle the data in ways that are adverse to consumers, from advertising harms to disclosures of personal information in public spaces or to governmental entities.
- *Not reasonably avoidable:* When companies' data sharing practices are buried in burdensome, unclear privacy policies, consumers are not truly informed about the fact that their data is shared, the purposes for which it is shared, or the parties that will receive it. And consumers typically lack direct relationships with data brokers that collect their data and so have little ability to limit or restrict what those brokers do with that data. With an ever-expanding network of ad partners and third-party affiliates, consumers cannot reasonably track everywhere their data is shared.
- *Not outweighed by countervailing benefits to consumers or competition:* Data brokers do not share data with other third parties for consumers' benefit. Rather, consumer data is a commodity from which data brokers benefit. When data sharing is not necessary for consumers to use the apps or websites where they initially provide data, data sharing does not positively contribute to consumers' online or in-app experiences. Nor do these practices promote competition; indeed, they undermine it by disadvantaging companies that respect consumer privacy interests.

[97] 87 Fed. Reg. 41243.

C. Behaviorally targeted advertising misuses consumers' data to promote harmful advertisements to certain consumers or to prevent them from receiving beneficial advertisements.

Behaviorally targeted advertising is used to deliver advertisements to a designated audience based on a range of data, including characteristics about consumers that represent a particular combination of demographic data and proxies for this data, and behavioral data such as consumers' online browsing or offline activity. This model of advertising typically depends on extensive commercial surveillance and the easily debunked idea that past behavior accurately forecasts future tendencies. For instance, a person's browsing history is not a very good proxy for future behavior because there are many reasons unrelated to purchase interest that a person would go to a website (misclicked a link, a friend or family member could have been using their device, or no longer be interested in the product or service they browsed).

Nevertheless, companies are incentivized to collect more and more data about a person and their activities, interests and vulnerabilities, in an attempt to more effectively target advertising. This incentive for collection of data leads to a variety of harms to consumers resulting from practices, including, as noted above: unwanted data collection and retention; unwanted and unexpected secondary use of data; unwanted combination of data across contexts; and unwanted disclosure of personal information to advertisers or to others. The opaque system of online behavioral advertising provides both incentives for over-collection and retention of data and an infrastructure to more broadly disperse and disclose that data throughout an unregulated ecosystem.

Behavioral advertising has provided an incentive for over-collection of data by a broad range of parties. Consumer Reports has cataloged the extensive tracking of online activities throughout consumers' day-to-day life by several major technology platforms, often incentivized or practiced by ad tech companies.[98] With other civil rights and consumer protection organizations, we previously collected dozens of different kinds of harm from commercial data practices, particularly invasions of privacy.[99]

---

[98] Justin Brookman, *Understanding the Scope of Data Collection by Major Technology Platforms*, Consumer Reports (May 2020), https://digital-lab.consumerreports.org/wp-content/uploads/2021/02/Understanding-the-scope-of-data-collection-by-major-platforms_2020_FINAL.pdf.

[99] Letter from Civil Society Organizations to FTC Chair Lina Khan and FTC Commissioners, (Aug. 4, 2021), https://cdt.org/wp-content/uploads/2021/08/2021-08-04-FTC-civil-rights-and-privacy-letter-Final.pdf

Importantly, data overcollection for behavioral advertising is practiced not just through websites and smartphone apps, but through other parties as well. For example, the FTC's investigation of Internet Service Providers found that ISPs were collecting data unnecessary for the provision of Internet service, sharing that data with third parties and using that data to target advertising.[100] Surveillance by a network provider is especially opaque: the user may not know or intentionally interact with a network provider (for example, at your workplace, school or a friend's home) and typically does not involve directly using a piece of software with a clear user interface or privacy information. Furthermore, the network provider has access to all traffic, even if the consumer switches to a different app, or uses another device altogether. And network providers have access to consumer data that may frustrate attempts to use technical precautions to protect privacy. For example, encrypting network traffic may help users, but a network provider can still learn about online activity through traffic analysis. Turning off location services in your smartphone's operating system will not prevent cellular carriers from learning your location when you make and receive calls. And network providers can collude with online trackers to undermine the ability to clear cookies or reset data from one's own device.[101] Ubiquitous online behavioral advertising without user understanding or control has provided an incentive for this class of businesses not just to provide the Internet access that a consumer believes they're purchasing, but also to start additional businesses in ad targeting, or to sell data to third parties.

Behavioral advertising contributes not just to the incentive for overcollection, but also to the broad dispersion and disclosure of data, including sensitive information. As noted above, consider the example of location information accessible by mobile apps, including dating apps. Location might be useful for finding nearby matches and people to talk to. But the incentive to sell data for behavioral advertising has led in some cases to sale of that location data for ad targeting and to data brokers, and in one notable case the disclosure of someone's sexual orientation and activity. This was not limited to a single transaction between an app and an ad network. Instead, detailed location information was distributed through the real-time bidding process that allows advertisers to bid on placements of ads to people based on that behavioral data. As a result, one spokesman for a broker of consumer data concluded that "every single entity in the advertising ecosystem has access to the information shared by Grindr and every other app that uses the real-time bidding system. That means thousands of entities have such access."[102]

---

[100] Federal Trade Commission, *A Look at What ISPs Know About You: Examining Privacy Practices of Six Major Internet Service Providers* (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.

[101] In 2017, the FTC approved a settlement with Turn, an ad targeting firm, for working with cellular carrier Verizon Wireless to track online activity even after the user had specifically cleared cookies.

[102] Byron Tau & Georgia Wells, *Grindr User Data Was Sold Through Ad Networks*, Wall St. J. (May 2, 2022), https://www.wsj.com/articles/grindr-user-data-has-been-for-sale-for-years-11651492800.

Some advertising providers have re-assured the public in saying that they do not disclose the information collected about the consumer, they just use that to provide an opportunity for an advertiser to promote a targeted product.[103] While ad targeting criteria may not always be revealed to those who bid or even those who win an ad auction slot, consumers also occasionally click on the ads they see. Consumers rarely if ever know exactly what criteria were used to target an ad to them through behavioral targeting systems;[104] if they click on an ad and subsequently share identifying information (for example, in the course of purchasing a product), then they also reveal to the advertiser that they met the targeting criteria of the original ad, which could include their location, stated interests, employment history or online activity.

But the impacts of behaviorally targeted advertising extend well beyond the unwanted collection of online browsing activities. The FTC has recognized that certain advertisements are in fact dangerous to certain audiences – specifically, recent FTC actions have focused on the marketing of these products to children and failure to comply with the COPPA rule's parental notice and consent requirements.[105] But behaviorally targeted advertising can cause deep and lasting harms to all consumers, and most especially to marginalized populations, including psychological and physical harms, unwanted intrusion, discrimination, or unfair manipulation. For instance, a recent study shows that across Facebook, Twitter, Instagram, and TikTok, advertisements and other sponsored content for weight loss products have been targeted to adult consumers identified as more susceptible to disordered eating.[106] This susceptibility is inferred from data collected about their online activities, such as signals of demographic information, searches for health- or nutrition-related information, and participation in online communities that are related to health or exercise or that encourage disordered eating.[107] These advertisements also tend to be targeted based on data related to gender, which causes the targeted audience to include consumers whose actual gender identities do not align with the gender norms that inform the parameters designating the audience.[108] This targeting

[103] For example, from Meta's Privacy Center: "We don't sell any of your information to anyone, and we never will."
[104] Signal experimented with including the direct targeting criteria as the text of Instagram ads; for example, "You got this ad because you're a newlywed pilates instructor and you're cartoon crazy. This ad used your location to see you're in La Jolla. You're into parenting blogs and thinking about LGBTQ adoption." But these ads were not shown. Jun Harada, *The Instagram Ads Facebook Won't Show You*, Signal blog (May 4, 2021), https://signal.org/blog/the-instagram-ads-you-will-never-see.
[105] Complaint, United States v. Kurbo, Inc., No. 22-CV-946 (N.D. Cal. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/filed_complaint.pdf.
[106] Liza Gak, Seyi Olojo, & Niloufar Salehi, *The Distressing Ads That Persist: Uncovering The Harms of Targeted Weight-Loss Ads Among Users with Histories of Disordered Eating*, 1 Assoc. For Computing Mach. 9 (April 2022), https://arxiv.org/pdf/2204.03200.pdf.
[107] *Id.* at 4, 10.
[108] *Id.* at 12.

contributes to anxiety, depression, low self-esteem, and physical harms like unhealthy dieting or exercise, or taking pills with harmful side effects.

The use of data collected about someone's online activities makes these harms more persistent and repeated than the more universal encounters of diet culture in broadcast media. The lack of rules to protect consumers from intrusion related to online activity may also create a chilling effect and discourage consumers from seeking out information on important but sensitive topics. Consumers increasingly recognize that surveillance is pervasive and hard to control, and regularly report altering their behavior and avoiding seeking out content because of the risks of pervasive tracking and disclosure through online advertising or recommendation systems.[109]

With the correct incentives, including strong rules that require targeted advertising systems to protect consumer privacy, technology that is more fit-for-purpose and privacy-preserving is more likely to be deployed. This is an opportunity for alternative advertising practices and monetization technology that provide greater support for publishers and creators of online content and better privacy and security that people can rely on.

The Commission correctly highlights the potential for alternative advertising practices once new rules are in force. Most important in this category would be the growing shift to contextual advertising. Advertising that is relevant to a person's current interests can be delivered based on the type of website they are visiting or the details of an article they have chosen to read. This form of advertising is well-established, as it has been in use in some form since well before the Internet was created; however, it also has particular efficacy advantages online, where context can be analyzed quickly and classified in great detail. Consumers show strong preferences for contextual advertising, there are far fewer privacy concerns with it, and it can be very effective advertising, both for publishers in gaining revenue and for advertisers in reaching new customers. Advertisers are already anticipating this shift, describing it as an important strategy and expecting to increase spending on contextual advertising.[110]

---

[109] Nick Doty, *Competing and Collaborating for Better Web Privacy*, Center for Democracy & Technology (Aug. 4, 2022), https://cdt.org/insights/competing-and-collaborating-for-better-web-privacy/; Scott Ikeda, *Study Shows Privacy Awareness is the "New Normal" for Consumers, Online Behavior is Much More Guarded,* CPO Magazine (Nov. 4, 2022), https://www.cpomagazine.com/data-privacy/study-shows-privacy-awareness-is-the-new-normal-for-consumers-online-behavior-is-much-more-guarded/; DataGrail, *The Great Privacy Awakening (2022),* https://www.datagrail.io/resources/interactive/2022-consumer-privacy-survey/people-take-action-for-privacy-online.

[110] For two very different organizational viewpoints on this topic that nonetheless draw similar conclusions about the growing importance of contextual advertising, *see* The Greens/European Free Alliance in the European Parliament, *What Does a Future Without Manipulation Look Like?*, https://afuturewithoutmanipulation.eu/; Interactive Advertising Bureau Europe, *IAB Europe's Guide to Contextual Advertising* (2021), https://iabeurope.eu/knowledge-hub/iab-europes-guide-to-contextual-advertising/.

The behavioral advertising practices described above constitute unfair practices:

- *Substantial injury:* Behavioral advertising relies on collection of extensive information without consumer knowledge, control, or consent. Sensitive data is dispersed without control to thousands of parties and may be disclosed, causing embarrassment, and personal and professional consequences. Online advertising that promotes products with potentially dangerous effects such as weight loss drugs can cause psychological and physical harms to consumers. Behavioral advertising is also causing intense psychological distress and even physical harm by targeting vulnerable populations with persistent intrusive messaging.
- *Not reasonably avoidable:* Online advertising uses consumers' online activities to direct advertisements based on the context of consumers' visits to apps or websites, the content on these apps or websites, and direct and inferred data about their demographics. Avoiding this practice would require consumers to avoid engaging in many basic online activities, from communicating to shopping to researching, altogether. Case studies demonstrate that even experts who go to extraordinary lengths fail to keep sensitive, private information from being collected, sold and used in intrusive and distressing ways by behavioral advertising.[111]
- *Not outweighed by countervailing benefits to consumers:* Directing advertisements that encourage consumers to engage in dangerous behaviors does not benefit any consumers. Consumers do not lack for means of finding out about products that may be of interest: online search tools and social media systems make it easier than ever to learn about commercial products and share experiences with them; advertising can be targeted without relying on ubiquitous surveillance (contextual advertising, for example); consumers who wish to receive more targeted offers could directly participate in willingly providing such information.
- *Not outweighed by countervailing benefits to competition:* Online publishers currently lack transparency and trust in the online advertising that they rely on for funding, and cross-context behavioral targeting lets online advertisers use detailed information gleaned from surveillance of a user on high-quality context-rich sites to advertise in other contexts, drawing money away from those publishers who might otherwise benefit from providing high-value contextual advertising. The model of building behavioral profiles that combine data across all online and offline activities creates incentives towards consolidation, and consolidation of the advertising market has inhibited competition. Publishers and content creators who rely on online advertising for funding pay what is in effect a heavy tax, to the dominant advertising technology firms and to a variety of vendors needed to mitigate losses within an untrusted ecosystem.

[111] Prince, *supra* n. 44.

Moves toward innovative models that would let consumers actively and voluntarily participate in customizing and selecting relevant online advertising have been undermined by advertising services that see no need to provide meaningful transparency or effective controls.

D. Companies limit access to critical opportunities through decision-making systems that use data about protected characteristics, or process data in ways that have a disparate impact on marginalized people.

Data- and algorithm-driven decision-making systems influence decisions in multiple critical areas, including housing, credit, and employment. Consumers cannot reasonably avoid being subjected to these systems, because doing so may obligate consumers to forego the opportunities about which the systems make decisions, and because consumers may not be able to anticipate these systems' harms.

The Commission should ensure that data-driven decision-making systems do not disproportionately harm certain communities. Unregulated and inappropriate data use can result in biased training data for AI systems, compound historical discrimination, and yield incorrect assumptions. Unfortunately, all too often, these risks are disproportionately borne by historically marginalized groups, including people of color, immigrants, Indigenous populations, women, people with disabilities, and the LGBTQ+ community.[112]

The resulting harms can take a number of different forms, and can occur for a number of reasons:

- Companies train these systems on data sets that do not accurately represent all consumers on which the systems are used – or conversely, the training data may incorporate substantial data that overrepresents a particular protected class.
- Companies may design these systems to evaluate consumer data from which protected characteristics could be inferred, which could enable or result in discrimination.
- Companies may not design these systems to ensure that all consumers subject to the systems can successfully navigate and use them.
- Companies may fail to establish processes for auditing the systems for inaccuracies or biases sufficiently to address and correct all harms.[113]

[112] *See generally* Crawford, *Placing Equity, supra* n. 53.

[113] While the ANPR asks about algorithmic error, it should be noted that these shortcomings are not always entirely unintentional. System design often executes the priorities and policies of the companies developing and using these systems, as well as societal biases regarding which consumers are entitled to have their fundamental needs met. In particular, people with a range of different disabilities, including chronic illnesses and mental health disabilities, face significant discrimination by algorithm-driven decision-making systems in a wide swath of areas, both because of exclusionary design and because of discriminatory targeting or profiling. Companies are neglecting disability-specific considerations when their decision-making systems rely on training data and operations

The lack of transparency in how these decision-making systems work makes it difficult for consumers to vindicate their rights under current federal civil rights laws. It impairs the ability to establish each of the three elements of a discrimination claim when brought against a company for engaging in discriminatory data practices:

- First, consumers must establish a prima facie case. One way is to present direct evidence of discrimination. Another way is for consumers to show they belong to a protected class and received an unfavorable outcome that similarly situated people outside of the same protected class did not experience. Either way, consumers are unlikely to have enough information about how an opaque data practice works to compare their outcomes to those of similarly situated people.
- From here, the burden shifts to the company to articulate a legitimate, non-discriminatory reason for the practice. This would not necessarily require the company to offer any insight into how the data practices involved actually work.
- If the company articulates this reason, consumers must then demonstrate that the articulated business interest is pretextual – for instance, by showing that a less discriminatory alternative satisfies that interest. Again, consumers would need access to enough information about how the data practice works to meaningfully compare it to other less discriminatory practices that satisfy the same business interest.

Below, we discuss how companies are misusing data-driven systems in ways that make it difficult for consumers to attribute discriminatory housing, credit, and employment decisions to the data practices responsible for them.

i. Housing and credit

To inform mortgage and other lending decisions and to screen rental applicants, "fintech" companies deploy systems that evaluate credit history, employment and income data, banking and purchase activity, rental payment history, eviction records, arrest and court records, education history, and other data.[114] These data points are supposed to predict whether applicants will fulfill the obligations that come with the housing or loan opportunities for which they are applying. However, fintech companies' systems have been shown to charge higher

---

parameters that under-represent disabled people, and companies can enable targeting of disabled people when training data and parameters overrepresent disabled people.

[114] Jung Choi, Karan Kaul, & Laurie Goodman, *FinTech Innovation in the Home Purchase and Financing Market*, Urban Inst. 9 (2019), https://www.urban.org/sites/default/files/publication/100533/fintech_innovation_in_the_home_purchase_and_financing_market_2.pdf; 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/.

interest rates to low-income and Black borrowers, and the systems are not designed to account for the context in which this data is generated.[115]

For instance, data about past arrest records, eviction proceedings, and financial, employment, and education history may not reflect consumers' *current* ability to make regular rental payments or loan repayments.[116] Meanwhile, data that would reliably indicate current ability to make regular payments, such as recent history of on-time utility payments, is not considered.[117] As a result, consumers can remain trapped in a cycle of poor access to credit because they are punished for past records despite changes in their circumstances or qualifications. In addition, tenant screening companies like CoreLogic use algorithms that consider data such as arrest and eviction records, which are unreliable predictors for how applicants will treat other tenants or property.[118] Higher volumes of arrest data are generated in overpoliced neighborhoods, disproportionately affecting Black, Indigenous, and Latinx communities, disabled people, and transgender people. Landlords often evict tenants after calls to police related to domestic violence, which occurs even more frequently for disabled people and people of color, and contributes to unreliable eviction data.[119]

Biometric data can also contribute to housing decisions. Besides tenant screening and other functions, property technology companies also provide video surveillance and facial recognition to monitor properties for any unpermitted activity or unauthorized presence, and biometric entry systems to prevent such situations.[120] In these cases, biometric data can also trigger evictions or arrests, further criminalizing people who are already disproportionately surveilled, and for whom facial analysis has been shown to produce unreliable matches.[121] Disabled people

---

[115] Choi et al., *supra* n. 114, at 10-11.
[116] Christopher K. Odinet, *The New Data of Student Debt*, 92 Southern Cal. L. Rev 1617, 1667 (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3349478; https://cdt.org/wp-content/uploads/2021/07/2021-07-01-CDT-Request-for-Information-and-Comment-on-Financial-Institutions-Use-of-Artificial-Intelligence-including-Machine-Learning.pdf.
[117] *Id.* at 1663; Emmanuel Martinez & Lauren Kirchner, *The Secret Bias Hidden in Mortgage Approval Algorithms*, The Markup (Aug. 25, 2021, 6:50 AM), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.
[118] Lydia X. Z. Brown, *Tenant Screening Algorithms Enable Racial and Disability Discrimination at Scale, and Contribute to Broader Patterns of Injustice*, Center for Democracy & Technology (July 7, 2021), https://cdt.org/insights/tenant-screening-algorithms-enable-racial-and-disability-discrimination-at-scale-and-contribute-to-broader-patterns-of-injustice/ [hereinafter Brown, *Tenant Screening Algorithms*].
[119] Am. Civ. Liberties Union, *Calling 911 Shouldn't Lead to an Eviction* (Mar. 15, 2022, 1:45 PM), https://www.aclu-wi.org/en/news/calling-911-shouldnt-lead-eviction.
[120] Avi-Asher Schapiro, *Good Business or Digital Bias? The Divisive Rise of 'Proptech',* Thomson Reuters (July 15, 2020, 5:14 PM), https://news.trust.org/item/20200715162819-bngcy; Anti-Eviction Mapping Project, Landlord Tech Watch, https://antievictionmappingproject.github.io/landlordtech/.
[121] *See generally* Sophia Maalsen, Peta Wolifson, Dallas Rogers, Jacqueline Nelson, and Caitlin Buckle, AHURI, *Understanding Discrimination Effects in Private Rental Housing* (2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3916655. *See also* Joy Buolamwini & Timnit Gebru, *Gender*

are currently at extraordinary risk of compounded discriminatory effects of rapidly expanding surveillance technologies. For instance, studies estimate up to 85% of incarcerated youth have learning or behavioral disabilities.[122] Use of tenant screening software, employment background checks, and predictive policing tools that inappropriately and sometimes illegally use arrest or conviction records thus has an outsized impact on disabled people, creating further inequities down the line in access to housing, employment, and social services.

Housing discrimination also occurs through behaviorally targeted advertising, which has been shown to direct advertisements for critical opportunities and services to, or away from, certain categories of consumers who would be interested in acting on the advertisements. In such cases, targeted advertising can either deny these consumers access to information that could help them access opportunities and services, or relegate them to receiving advertisements for more unfavorable opportunities or products.[123] For example, a Department of Justice (DOJ) lawsuit alleged that Meta's advertising system enabled advertisers to use categories created based on race, color, religion, sex, disability, familial status, and national origin, and proxies for these characteristics, to designate eligible audiences for delivery of housing advertisements.[124]

While the companies responsible for data-driven discrimination in lending and housing should be subject to liability under federal civil rights laws, the information asymmetry between consumers and companies erects barriers for consumers to vindicate their civil rights even against entities that are subject to civil rights laws. The Fair Housing Act prohibits discrimination in advertisements, offers, and sale or rental of housing on the basis of race, color, religion, sex, disability, familial status, or national origin.[125] The DOJ advises that it will pursue cases against these companies when there is evidence of a pattern or practice of discrimination, as it did against Meta's targeted advertising tool, which it settled this year.[126] However, the tool in question was supposed to be an improvement on a previous targeted advertising tool that was

---

Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 Proceedings Of Machine Learning Research 2 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[122] Daja E. Henry & Kimberly Rapanut, *How Schools and the Criminal Justice System Both Fail Students with Disabilities*, Slate (Oct. 21, 2020, 9:00 AM), https://slate.com/news-and-politics/2020/10/students-disabilities-criminal-justice-system.html.

[123] *See e.g.*, Julia Angwin & Terry Parris, Jr., *Facebook Says It Will Stop Allowing Some Advertisers to Exclude Users by Race*, ProPublica (Nov. 11, 2016, 10:00 AM), https://www.propublica.org/article/facebook-to-stop-allowing-some-advertisers-to-exclude-users-by-race.

[124] Department of Justice, *Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising* (June 21, 2022), https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known.

[125] 42 U.S.C. §3604 *et seq*.

[126] Department of Justice, *supra* n. 124.

the subject of a 2019 settlement.[127] This leaves consumers with some uncertainty about whether the next iteration of the tool will produce fairer results.

As for systems that affect housing decisions, the Department of Housing and Urban Development (HUD) has warned that the use of criminal arrest records can have a disparate impact based on race and national origin.[128] HUD has also advised that evictions following domestic violence-related calls to police can indicate disability or gender discrimination,[129] which can make housing decisions relying on eviction records more likely discriminatory as well. This has not deterred the use of tenant screening algorithms that include these records, though.[130]

The Equal Credit Opportunity Act (ECOA) prohibits discrimination against applicants in any aspect of a credit transaction on the basis of race, color, religion, national origin, sex, marital status, age, or income derived from a public assistance program.[131] The CFPB recently issued guidance stating that the ECOA requires creditors to provide consumers with a specific and accurate statement of principal reasons for adverse actions resulting from an algorithmic system.[132] Data practices that make or inform decisions regarding the extension of credit can violate the ECOA by using data that functions as proxies for these protected characteristics, but this does not extend to disability discrimination. The ECOA requires creditors to inform credit applicants in writing about the reasons for an adverse credit decision or about the applicants' right to receive such a notice upon request, including for adverse actions resulting from algorithmic systems.[133] This does not give applicants an opportunity to verify the accuracy of the data being evaluated during the approval process, or to provide additional information to

---

[127] Alfred Ng & Corin Faife, *Facebook Pledges to Remove Discriminatory Credit and Loan Ads Discovered by The Markup*, The Markup (May 4, 2021, 8:00 PM), https://themarkup.org/citizen-browser/2021/05/04/facebook-pledges-to-remove-discriminatory-credit-and-loan-ads-discovered-by-the-markup.

[128] Office of General Counsel, Department of Housing and Urban Development, *Guidance on Application of Fair Housing Act Standards to the Use of Criminal Records by Providers of Housing and Real Estate-Related Transactions* (2016), https://www.hud.gov/sites/documents/HUD_OGCGUIDAPPFHASTANDCR.PDF.

[129] Office of General Counsel, Department of Housing and Urban Development, *Guidance on Application of Fair Housing Act Standards to the Enforcement of Local Nuisance and Crime-Free Housing Ordinances Against Victims of Domestic Violence, Other Crime Victims, and Others Who Require Police or Emergency Services* (2016) https://www.hud.gov/sites/documents/FINALNUISANCEORDGDNCE.PDF.

[130] Brown, *Tenant Screening Algorithms*, *supra* n. 118.

[131] 15 U.S.C. §1691(a).

[132] Consumer Financial Protection Bureau, *Circular 2022-03: Adverse Action Notification Requirements in Conenction With Credit Decisions Based on Complex Algorithms*, https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/.

[133] *Id.*; 15 U.S.C. §1691(d)(2).

supplement that data.[134] The ECOA also requires correction of inaccuracies in credit records upon request, which places responsibility on consumers to detect such errors, without clarity about which data contributed to the ultimate decision. Further, the ECOA offers limited recourse for targeted advertising – it protects people who actually apply for credit, extending to prospective applicants only insofar as it prohibits creditors from stating discriminatory preferences in advertising.[135]

ii. Employment

Algorithmic tools play a driving role in decisions including hiring, promotion, and termination. Vendors develop hiring technologies that aim to distinguish candidates in an applicant pool based on attributes they appear to have in common with other successful candidates and employees – in other words, attributes of people who have historically been hired more often.[136] These tools include resume screeners, personality and aptitude assessments, and recorded video interviews. Reliance on these tools can perpetuate discrimination against jobseekers with a range of disabilities:[137]

- Ideal's resume screening software analyzes language and details in resumes, from candidates' names to affiliations to employment gaps, to identify whether the resumes reflect qualities the tools are designed to look for.[138] Taleo assigns bonus points for keywords in resumes that reflect attributes that are desired but not required.[139] Disabled people who have previously experienced discrimination in their education, employment, or access to healthcare (especially if they face multiple forms of discrimination) might not get past screening tools that downgrade or screen out resumes before human reviewers can consider them. For instance, a disabled person may previously have had

[134] Samir Jain & Ridhi Shetty, *Taking a Hard Line on AI Bias in Consumer Finance*, Center for Democracy & Technology, https://cdt.org/insights/taking-a-hard-line-on-ai-bias-in-consumer-finance/.
[135] 12 C.F.R. Supplement I to Part 1002, Paragraph 4(b).
[136] Miranda Bogen & Aaron Rieke, Upturn, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias* (2018), https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf.
[137] Center for Democracy & Technology, *Algorithm-Driven Hiring Tools: Innovative Recruitment or Expedited Disability Discrimination?* (2020), https://cdt.org/wp-content/uploads/2020/12/Full-Text-Algorithm-driven-Hiring-Tools-Innovative-Recruitment-or-Expedited-Disability-Discrimination.pdf.
[138] Ideal, *Screening*, https://ideal.com/product/screening/. *See also* Avi-Asher Schapiro, *AI is Taking Over Job Hiring, But Can it Be Racist?*, Thomson Reuters (Jun. 7, 2021, 7:04 AM), https://www.reuters.com/article/global-tech-ai-hiring/analysis-ai-is-taking-over-job-hiring-but-can-it-be-racist-idUSL5N2NF5ZC.
[139] James Hu, *Taleo: 4 Ways the Most Popular ATS Ranks Your Job Application*, Jobscan (Mar. 8, 2018), https://www.jobscan.co/blog/taleo-popular-ats-ranks-job-applications/.

difficulty getting full-time employment, thus leading to gaps in their resume that will be flagged by such systems.[140]

- Personality and aptitude assessments can vary in how they assess candidates, ranging from simulation to psychometric tests.[141] Paradox Traitify provides candidates with a series of images, requiring them to indicate whether they identify with what is depicted in each image to determine their alignment with a pseudoscientific personality model.[142] Pymetrics analyzes data collected while candidates complete a set of games to predict "cognitive and emotional attributes," which it claims to be "fairness-optimized" but has not been examined for disability bias.[143] Pymetrics was recently acquired by Harver, which implements "behavioral-based AI methodology" in soft skills assessments and automates matching of "high-potential" candidates.[144] Cappfinity's Koru uses a survey that requires candidates to select the responses with which they feel they align most, to assess soft skills.[145] Blind people and people with mobility impairments might not be able to adequately interface with a gamified assessment, while people with mental health disabilities or cognitive disabilities might have difficulty processing the information quickly enough to score well. Similarly, autistic and other neurodivergent people may fail to answer correctly on personality tests that score candidates on characteristics unrelated to core competencies or essential functions of the job at hand.
- HireVue has used video interview assessments that process data about how candidates physically appear, move, emote, and sound as they respond to interview questions. This treats candidates' eye contact, facial expressions, fidgeting, tics, vocabulary, and speech patterns as data points to infer personality traits such as confidence and trustworthiness.[146] HireVue has stated that it does not use video analysis or audio

---

[140] Jim Fruchterman & Joan Mellea, Benetech, *Expanding Employment Success for People With Disabilities* (2018), https://benetech.org/about/resources/expanding-employment-success-for-people-with-disabilities-2/.

[141] *Algorithm-Driven Hiring Tools*, *supra* n. 137, at 11-12; Aaron Rieke, Urmila Janardan, Mingwei Hsu, and Natasha Duarte, Upturn, *Essential Work* (2021), https://www.upturn.org/work/essential-work/.

[142] Paradox, *Assessments*, https://www.paradox.ai/products/assessments; Olivia Goldhill, *We Took the World's Most Scientific Personality Test – and Discovered Unexpectedly Sexist Results* (Feb. 11, 2018), https://qz.com/1201773/we-took-the-worlds-most-scientific-personality-test-and-discovered-unexpectedly-sexist-results/.

[143] Pymetrics, *Assessments*, https://www.pymetrics.ai/assessments; Christo Wilson, Avijit Ghosh, Shan Jiang, Alan Mislove, Lewis Baker, Janelle Szary, Kelly Trindel, and Frida Polli, *Building and Auditing Fair Algorithms: a Case Study in Candidate Screening* (2021), https://evijit.github.io/docs/pymetrics_audit_FAccT.pdf.

[144] Harver, *Harver Acquires Pymetrics, Further Enhancing Talent Decision Capabilities Across the Employee Lifecycle* (Aug. 11, 2022), https://harver.com/press/harver-acquires-pymetrics/; Harver, *Assessments*, https://harver.com/software/assessments/; Harver, *Hiring Process Optimization*, https://harver.com/software/hiring-process-optimization/.

[145] Cappfinity, *Skills Identification*, https://www.cappfinity.com/cappfinity-product-page/assessment-cognitive-3/.

[146] Drew Harwell, *A Face-Scanning Algorithm Increasing Decides Whether You Deserve the Job*, Wash. Post (Nov. 6, 2019, 12:21 PM), https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

characteristics, but it analyzes personality traits and aptitudes by applying natural language processing to a transcription developed through an AI-driven speech-to-text service.[147] Disabled candidates who possess the traits that are necessary for successful job performance can nonetheless be scored unfairly by this type of tool, because their disabilities can cause them to demonstrate examined traits in ways that cannot be accurately captured through the analyzed data points.[148] HireVue also claims its product has been audited for fairness, but does not make its audit report available unless one provides their name, email address, and professional affiliation and agrees not to use any part of the audit report without HireVue's written authorization.[149] HireVue is now facing a class action lawsuit over its collection and use of biometric data.[150]

Vendors market many of these tools as bias audited or less biased, without showing how (or even whether) the tools have been examined for disability bias.[151] Meanwhile, the tools collect and analyze data about candidates that is not relevant to candidates' ability to perform job functions, causing workers to be rejected over irrelevant data related to disability or other marginalized identities.[152]

Companies are also increasingly developing and deploying sophisticated electronic surveillance to automate the monitoring and management of workers, whether they are in a warehouse, out making deliveries, at an office, or working remotely from home. Companies can use such automated systems, commonly referred to as "bossware," to perform a wide variety of monitoring tasks, such as tracking workers' location and movements, productivity and downtime, computer use, facial expressions, biometric markers, and frequency and length of

---

[147] HireVue, *Explainability Statement* (2022), https://webapi.hirevue.com/wp-content/uploads/2022/03/HV_AI_Short-Form_Explainability_3152022.pdf.
[148] Matthew Scherer, *HireVue "AI Explainability Statement" Mostly Fails to Explain what it Does*, Center for Democracy & Technology (Sept. 8, 2022), https://cdt.org/insights/hirevue-ai-explainability-statement-mostly-fails-to-explain-what-it-does/.
[149] HireVue, *Download IO Psychology Audit Description by Landers Workforce Science LLC*, https://www.hirevue.com/resources/template/hirevue-io-psychology-audit-report.
[150] Samantha Hawkins, *HireVue Attempts to Escape Biometrics Suit Over AI Interviews*, Bloomberg (June 22, 2022, 1:16 PM), https://news.bloomberglaw.com/privacy-and-data-security/hirevue-attempts-to-escape-biometrics-suit-over-ai-interviews.
[151] *See* Manish Raghavan, Solon Barocas, Jon Kleinberg, & Karen Levy, *Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices*, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency 469 (2020), https://arxiv.org/pdf/1906.09208.pdf.
[152] *See* Hilke Schellmann, *Finding it Hard to Get a New Job? Robot Recruiters Might Be to Blame*, The Guardian (May 11, 2022, 4:30 PM), https://www.theguardian.com/us-news/2022/may/11/artitifical-intelligence-job-applications-screen-robot-recruiters (discussing how automated hiring technologies exhibit gender biases and use criteria such as names and data about non-professional activities).

bathroom and other breaks.[153] One system, Crossover's WorkSmart productivity tool, takes periodic screenshots and images of workstations to monitor what workers are doing.[154] Another company, Time Doctor, prevents workers from deleting screenshots to protect their privacy by deducting time worked during the period when screenshots were taken.[155] Some programs use workers' phones or computers to listen, watch, or monitor other sensors in their device, and can penalize workers for moving away from their workstation or slowing productivity.

Companies often use these technologies to optimize tasks for their own profit, but they put workers' health and safety at risk and threaten their privacy, autonomy, and dignity.[156] For example, Amazon has used productivity monitoring to monitor "time off task," which triggers warnings to workers for resting when needed, putting them at risk of termination if they do not work at a pace that is dangerously fast.[157] Productivity monitoring also fails to capture work that is being performed offline or that cannot be accurately quantified through surveillance measures, and can punish and deter worker organizing.[158]

Many low-wage and hourly workers endure constant surveillance, often combined with algorithmic management systems that can discipline or even terminate them.[159] This exacerbates the already-wide gaps in information and bargaining power that low-wage workers face. In a recent policy statement, the FTC recognizes that algorithmic tools further diminish gig workers' bargaining power.[160] The policy statement advises that the FTC's authority against unfair or deceptive practices may apply to the use of data-driven or algorithmic methods to

---

[153] Jodi Kantor, Arya Sundaram, Aliza Aufrichtig, & Rumsey Taylor, *Workplace Productivity: Are You Being Tracked?*, N.Y. Times (Aug. 16, 2022, 10:03 AM), https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html; Spencer Soper, *Fired by Bot at Amazon: 'It's You Against the Machine'*, Bloomberg (June 28, 2021, 6:00 AM), https://www.bloomberg.com/news/features/2021-06-28/fired-by-bot-amazon-turns-to-machine-managers-and-workers-are-losing-out.

[154] Sean Captain, *In 20 Years, Your Boss May Track Your Every Glance, Keystroke, and HeartBeat*, Fast Company (Jan. 27, 2020), https://www.fastcompany.com/90450122/in-20-years-your-boss-may-track-your-every-glance-keystroke-and-heartbeat.

[155] Matt Scherer, Center for Democracy & Technology, *Warning: Bossware May Be Hazardous to Your Health* 9 (2021), https://cdt.org/insights/report-warning-bossware-may-be-hazardous-to-your-health/.

[156] *Id.* at 36.

[157] Deborah Berkowitz, *Packaging Pain: Workplace Injuries in Amazon's Empire*, Nat'l Emp. Law Project, https://www.nelp.org/publication/packaging-pain-workplace-injuries-amazons-empire/; Colin Lecher, *How Amazon Automatically Tracks and Fires Warehouse Workers for 'Productivity'*, The Verge (Apr. 25, 2019, 12:06 PM))https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations.

[158] Kantor, *supra* n. 153.

[159] Aiha Nguyen, *The Constant Boss: Labor Under Digital Surveillance*, Data & Society (2021), https://datasociety.net/library/the-constant-boss/.

[160] Federal Trade Commission, Policy Statement on Enforcement Related to Gig Work (Sept. 15, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Matter%20No.%20P227600%20Gig%20Policy%20Statement.pdf.

determine compensation and availability and termination of jobs. The FTC's authority would better protect gig workers than existing civil rights laws and the Occupational Health and Safety Act, which do not classify all workers as covered "employees."[161]

Low-wage workers marginalized on the basis of disability, race, ethnicity, and gender identity are at an even greater disadvantage. As many as 100,000 disabled workers are paid subminimum wages due to a provision in the Fair Labor Standards Act that allows employers to pay disabled workers commensurate with wages paid to non-disabled workers for "the same type, quality, and quantity of work" – effectively limiting disabled workers' wages based on their challenges in meeting productivity expectations.[162] In other words, this provision allows an employer to pay a disabled worker only for the hours a non-disabled worker would take to complete the same work rather than the hours of labor the disabled worker has actually put in. Productivity monitoring systems can discriminate against disabled workers, pregnant or breastfeeding workers, older workers, and workers requiring religious prayer breaks by flagging breaks or slower pace of work, increasing the risk of injury to physical or mental health.[163] These effects are especially worse for people with physical, mental health, developmental, or cognitive disabilities.

Relatedly, more employers are relying on workplace wellness programs to increase worker productivity while reducing the cost of benefits claims for employers, even turning to gamified approaches to influence employees' behavior and personal health decisions.[164] Studies have shown that these programs do not deliver the intended positive effects on healthcare expenses or productivity.[165] Meanwhile, the programs impose expectations for physical exercise and diet that disabled workers may not be able to meet, and reinforce the higher societal value assigned

[161] Scherer, *supra* n. 155, at 16.
[162] Rebecca Vallas, Kim Knackstedt, Hayley Brown, Julie Cai, Shawn Fremstad, & Andrew Stettner, The Century Fdn. and Disability Econ. Just. Collaborative, *Economic Justice is Disability Justice* (2022), https://tcf.org/content/report/economic-justice-disability-justice/. Section 14(c) of the Fair Labor Standards Act allows employers to apply for special certificates to employ disabled workers at subminimum wages. 29 U.S.C. §214(c).
[163] *The Future of Work: Protecting Workers' Civil Rights in the Digital Age, Before House Comm. on Ed. & Labor, Civil & Human Serv. Subcomm.* (2020) (testimony of Jenny Yang, Senior Fellow, Urban Institute), https://edlabor.house.gov/imo/media/doc/YangTestimony02052020.pdf.
[164] *See* Joseph Sanford & Kevin Sexton, *Opinion: Improve Employee Health Using Behavioral Economics*, CFO (Feb. 3, 2022), https://www.cfo.com/human-capital/health-benefits/2022/02/employee-health-wellness-medical-claims-behavorial-economics/.
[165] Sally Wadyka, *Are Workplace Wellness Programs a Privacy Problem?*, Consumer Reports (Jan. 16, 2020), https://www.consumerreports.org/health-privacy/are-workplace-wellness-programs-a-privacy-problem-a2586134220/.

to being "healthy."[166] To make matters worse, these programs pressure employees to provide health data that might make its way to third parties.[167]

While the discriminatory outcomes of hiring and algorithmic management technologies run afoul of federal employment discrimination laws, enforcement has not kept up with these technologies. For instance, Title I of the ADA prohibits adverse employment decisions based on workers' disability, and it requires employers to provide reasonable accommodations when doing so would not pose an undue hardship on employers.[168] Hiring and algorithmic management technologies provided by private companies can make or influence adverse decisions using disability-related data, without informing workers about how the technologies are collecting and analyzing their data, how this will influence employment decisions, and how workers might access accommodations that enable fairer evaluation.[169] Thus, workers may not have enough detail to pursue disability discrimination claims arising from these technologies' use. Similar issues plague enforcement of Title VII of the Civil Rights Act. As Commissioner Bedoya stated, Title VII "does not directly address hiring technology vendors, digital sourcing platforms, and other companies that intermediate people's access to employment opportunity."[170]

Beyond civil rights protections, there are few other laws or rules governing employers' use of surveillance technologies or safeguarding workers from their harmful effects. Workers have no concrete privacy rights under either federal law or the laws of most states. The Occupational Safety and Health Act prohibits practices that pose a risk of death or serious injury to workers, but the Occupational Safety and Health Administration's regulations do not cover many of the harms to workers' health that these technologies can impose, such as repetitive motion injuries and threats to workers' mental health. In addition, a new fact sheet from the Department of Labor regarding reporting requirements under the Labor-Management Reporting and Disclosure Act states that employers must report expenditures made for surveillance of employees and unfair labor practices, but only when the surveillance is used to obtain information connected to a labor dispute or the labor practices are intended to undermine the right to organize.[171]

---

[166] Brown, *Surveillance Technologies*, *supra* n. 12, at 54-55; Ifeoma Ajunwa, Kate Crawford, & Jason Schultz, *Limitless Worker Surveillance*, 129-30, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746211.
[167] *Id.*
[168] 42 U.S.C. §12112.
[169] *Algorithm-Driven Hiring Tools*, *supra* n. 137.
[170] Federal Trade Commission, Statement of Commissioner Alvaro M. Bedoya Regarding the Commercial Surveillance Data Security Advance Notice of Proposed Rulemaking (Aug. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Bedoya%20ANPR%20Statement%2008112022.pdf.
[171] Jeffrey Freund, *How We're Ramping Up Enforcement of Surveillance Reporting*, Department of Labor Blog (Sept. 15, 2022), https://blog.dol.gov/2022/09/15/how-were-ramping-up-our-enforcement-of-surveillance-reporting; Office of Labor-Management Standards, U.S. Department of Labor, *OLMS Fact Sheet on Form LM-10 Employer*

Note on Public Sector Uses: Data- and algorithm-driven decision-making is increasingly used in numerous sectors, and its effects in one sector can flow to other sectors. The harms described above are focused on private entities, such as private housing sales or private employers. Schools and other governmental entities regularly work with private contractors to provide critical services to schools and families, some of which may be data-intensive. Because services provided by private contractors to governmental entities require special considerations, they are discussed separately in Part 2, Sections II and III of our comments.

The processing of consumer data to make adverse decisions about consumers' access to housing, credit, and employment based on protected traits constitutes an unfair practice:

- *Substantial injury:* Discriminatory data-driven decision-making denies critical opportunities to marginalized communities, whether by rejecting applicants from these opportunities outright or by imposing unfavorable conditions for people to maintain access to these opportunities. This practice also causes psychological and physical harm to marginalized communities when it subjects them to conditions that harm physical or mental health.
- *Not reasonably avoidable:* Consumers do not have control over how the data-driven decision-making systems that evaluate them are designed or developed. They also are not properly informed prior to a decision-making process about how their data will be analyzed and whether alternative methods of evaluation are available, nor are they informed about how the processing of their data compares to how data of other consumers outside of their protected class is analyzed.
- *Not outweighed by countervailing benefits to consumers or competition:* Consumers do not benefit when they receive adverse decisions due to discriminatory decision-making practices. The processing of consumer data related to protected characteristics is not a reliable way to determine whether consumers are eligible or qualified for the opportunity in question. Nor do these practices promote competition; indeed, they undermine it by disadvantaging companies that respect consumer privacy interests.

E. Companies utilize dark patterns designed to nudge consumers to enable access to their data.

Reporting: Transparency Concerning Persuader, Surveillance, and Unfair Labor Practices Expenditures, https://www.dol.gov/sites/dolgov/files/OLMS/regs/compliance/LM10_FactSheet.pdf.

The ANPR states that the dark pattern practices the FTC has targeted include misrepresentations of how account holders' selected privacy settings are implemented,[172] and misrepresentations that trick or trap consumers into subscriptions.[173] Dark patterns that do not require consumers to make accounts or cause them to make purchases can be similarly troublesome. Certain practices involve deploying user interface and design elements that consumers would be expected to overlook, misunderstand, or be manipulated by, inducing consumers to provide data or agree to certain uses of their data when they may not otherwise.[174]

Dark patterns come in a variety of options. One prominent type of dark pattern is hidden information, where a company provides consumers' options or the information needed to compare those options in fine print text or in faded text.[175] In the same situation, misdirection, or aesthetic manipulation, can be used to distract consumers to pay attention to the company's preferred options, for example by providing their preferred options or information about those options in contrasting, more eye-catching colors.[176] This is further exacerbated by preselection, another type of dark pattern where a choice is already selected by default – for instance, an already checked box indicating acceptance of terms of service or opt-in to a mailing list – which increases the likelihood that consumers will proceed with the selected option instead of looking at others.[177] There are several other dark pattern types as well,[178] including privacy zuckering in which privacy-invasive defaults are in place and privacy settings are intentionally made difficult for consumers to navigate, leaving these defaults in place.[179]

---

[172] Federal Trade Commission, *Facebook Settles FTC Charges That it Deceived Consumers by Failing to Keep Privacy Promises* (Nov. 29, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep-privacy-promises.

[173] Federal Trade Commission, *Children's Online Learning Program ABCmouse to Pay $10 Million to Settle FTC Charges of Illegal Marketing and Billing Practices* (Sept. 2, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/09/childrens-online-learning-program-abcmouse-pay-10-million-settle-ftc-charges-illegal-marketing.

[174] *See generally* Jamie Luguiri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. Legal Analysis 43 (2021), https://academic.oup.com/jla/article/13/1/43/6180579; Alfred Ng & Sam Morris, *Dark Patterns That Mislead Are All Over the Internet*, The Markup (June 3, 2021, 10:00 AM), https://themarkup.org/2021/06/03/dark-patterns-that-mislead-consumers-are-all-over-the-internet.

[175] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, & Austin L. Toombs, *The Dark (Patterns) Side of UX Design*, 7 (2018) https://dl.acm.org/doi/pdf/10.1145/3173574.3174108.

[176] *Id.*; Luguiri, *supra* n. 174 at 51; Deceptive Design, *Misdirection*, https://www.deceptive.design/types/misdirection.

[177] *Id.*

[178] Deceptive Design, *Types of Deceptive Design*, https://www.deceptive.design/types.

[179] Deceptive Design, *Privacy Zuckering*, https://www.deceptive.design/types/privacy-zuckering; Luisa Jarovsky, *Dark Patterns in Personal Data Collection: Definition, Taxonomy, and Lawfulness* 30-31 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4048582.

Dark patterns can affect consumers differently depending on the devices they are using and barriers they may experience with respect to digital literacy. User experiences with dark patterns can differ between mobile and web modalities, so a company might use dark patterns only in one modality, treating consumers differently according to the devices on which they are accessing the company's service.[180] Therefore, the company's potential uses of dark patterns would need to be scrutinized across all modalities through which it provides the service. Further, on top of the information asymmetry that consumers in general face when it comes to data collection and processing, education level is shown to affect susceptibility to more subtle dark patterns, indicating that communities with inequitable access to education may be more likely to be manipulated.[181] With the emergence of new media types such as augmented and virtual reality, dark patterns may become even more difficult for consumers to recognize.[182]

The ANPR points to the FTC's recent policy statement on negative option arrangements as an example of the FTC's guidance on dark patterns.[183] The policy statement applies to companies that treat consumers' silence or failure to take an affirmative action to reject or stop a purchased service as acceptance of the service or its continuation. This policy statement affirms notice and consent requirements for companies before executing a transaction. The policy statement is limited to practices where payment is collected – it does not apply to consumers not taking affirmative steps to stop the collection or use of their data in exchange for goods and services that they need not purchase to access. As the FTC's new report on dark patterns recognizes, dark patterns can force consumers to give up data by steering them into taking specific actions online, denying consumers the ability to navigate websites and apps freely by making them responsible for avoiding manipulative elements they may not even recognize.[184]

Companies' use of dark patterns constitutes a deceptive practice because dark patterns rely on misleading design elements that have been shown to obscure consumers' choices or limit their ability to exercise their choices. **Dark patterns also constitute an unfair practice:**

---

[180] *See* Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, & Christo Wilson, *A Comparative Study of Dark Patterns Across Mobile and Web Modalities*, 5 Proceedings of the ACM on Human-Computer Interaction 22 (2022), https://cbw.sh/static/pdf/gunawan-2021-pacmhci.pdf.
[181] *See* Luguiri, *supra* n. 174, at 70-71.
[182] *See* Michal Turjeman, *Designing the Metaverse: Challenges and Questions*, VentureBeat (July 24, 2022, 1:10 PM), https://venturebeat.com/datadecisionmakers/designing-the-metaverse-challenges-and-questions/.
[183] Federal Trade Commission, *Enforcement Policy Statement Regarding negative Option Marketing* (Oct. 22, 2021), https://www.ftc.gov/system/files/documents/public_statements/1598063/negative_option_policy_statement-10-22-2021-tobureau.pdf.
[184] Lauren E. Willis, *Deception by Design*, 34 Harvard J. L. Tech. 133-34 (2020), https://jolt.law.harvard.edu/assets/articlePDFs/v34/3.-Willis-Images-In-Color.pdf; Federal Trade Commission, *Bringing Dark Patterns to Light* 23-27 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

- *Substantial injury:* Dark patterns enable companies to overcollect consumers' data by manipulating consumers about what they are consenting to or what an action they take would allow companies to do. Companies can then treat consumers' manipulated actions as "consensual" actions granting them permission to utilize consumer data.
- *Not reasonably avoidable:* Because dark patterns are inherently designed to be difficult for consumers to avoid while creating a false sense of choice, consumers are induced to take actions they may not want to take or even recognize they are taking.
- *Not outweighed by countervailing benefits to consumers or competition:* Dark patterns enable companies to obtain consumers' data without providing any benefit to consumers in return, or any benefit to competition.

II. Recommendations for privacy-protective measures in FTC rulemaking

Moving forward, the FTC should create data management obligations that include minimizing data collected and requiring purpose/use limitations; requiring consumer controls; and imposing strong transparency measures.

A. Require data minimization and use and purpose limitations in how companies handle consumer data.

The responsibility for preventing data misuse should not be left to consumers. The Commission should focus on rebalancing the burden for who is responsible for keeping people's data private. In many cases, the burden properly belongs with the entities collecting and using the data, rather than with individuals. The FTC can and should place meaningful limits on how companies handle data in the first place to address harms that are cross-cutting, sector-specific, and specific to particular classes of underserved people.[185] FTC rules should restrict data collection, retention, processing, and sharing to only as much as is necessary to fulfill the purpose for which consumers are choosing to engage with the company that deploys the data practices in question.[186]

FTC rules should impose data minimization requirements against overcollection and secondary use of sensitive data by generally restricting companies from:

[185] *See generally* Consumer Reports & Electronic Privacy Information Center, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.
[186] *See* Pre-rulemaking Stakeholder Session before the Cal. Privacy Protection Agency (2022) (testimony of Eric Null, Director of Privacy & Data Project, Center for Democracy & Technology), https://cdt.org/wp-content/uploads/2022/05/CA-Testimony-Eric-Null-Data-Minimization-Letterhead.pdf.

- Collecting sensitive data unless it is strictly necessary to provide the service requested by the consumer.
- Engaging in secondary uses or repurposing of sensitive data.[187]
- Retaining sensitive data after the purpose for which the data was collected, used, and stored has been fulfilled.
- Continuing any use, processing, or sharing of sensitive data after it has been shown to pose unmitigated risks to consumers.
- Using consumers' sensitive data to target advertisements to consumers.[188]
- Using settings or interfaces or making other representations that are likely to mislead consumers as to how their personal data is handled, or to induce consumers' disclosure of data, so as to affect reasonable consumers' conduct with respect to the product or service.[189]

The FTC should note that while properly de-identified data can be used in privacy-protecting ways, de-identified and aggregated data sets should not be viewed as absolute privacy protections – they can often be reidentified.[190] Even when appropriate steps are taken to protect individual privacy, people can still be re-identified and harms can still result. Aggregated and de-identified data sets can still mischaracterize underrepresented groups and thus result in disparate impacts. Therefore, other measures such as selective redaction of sensitive data from amassed data should also be incorporated.[191]

---

[187] *See* Pre-rulemaking Stakeholder Session before the Cal. Privacy Protection Agency (2022), (testimony of Andrew Crawford, Senior Policy Counsel, Center for Democracy & Technology) https://cdt.org/wp-content/uploads/2022/05/Andrew-Crawford-5-6-22-CPPA-Statement.pdf; Andrew Crawford & Michelle Richardson, *CDT & EHI's Proposed Consumer Privacy Framework for Health Data* 15, 23-27, Center for Democracy & Technology (2021), https://cdt.org/insights/cdt-ehis-proposed-consumer-privacy-framework-for-health-data/.

[188] There may be some limited instances where this is allowed, like if a consumer specifically opts into behaviorally targeted advertising.

[189] *See* Center for Democracy & Technology, *CDT's Federal Baseline Privacy Legislation Discussion Draft* 9 (2018), https://cdt.org/wp-content/uploads/2018/12/2018-12-12-CDT-Privacy-Discussion-Draft-Final.pdf.

[190] *See e.g.,* Thompson, *supra* n. 68. European researchers "have published a method they say is able to correctly re-identify 99.98% of individuals in anonymized data sets with just 15 demographic attributes." Natasha Lomas, *Researchers Spotlight the Lie of 'Anonymous' Data,* TechCrunch (Jul 24, 2019, 6:30 AM), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/; Justin Sherman explains how "[r]eidentification has become horrifyingly easy." Justin Sherman, *Big Data Might Not Know Your Name. But It Knows Everything Else,* Wired (Dec. 19, 2021, 8:00 AM), https://www.wired.com/story/big-data-may-not-know-your-name-but-it-knows-everything-else/.

[191] Nick Doty, *Selectively Redacting Sensitive Places from Location Data to Protect Reproductive Health Privacy*, Center for Democracy & Technology (Aug. 25, 2022), https://cdt.org/insights/selectively-redacting-sensitive-places-from-location-data-to-protect-reproductive-health-privacy/.

These considerations would help reduce harms arising from certain uses or categories of data that present heightened risks. The Commission can look to existing work to help shape its approach to protecting sensitive data. For example, when formulating rules to address health data that falls outside of HIPAA and its associated Privacy Rule, the Commission should look to the AMA's Privacy Principles,[192] and consider the protections contemplated and outlined in the CDT/EHI Proposed Consumer Privacy Framework for Health Data[193] along with CDT's associated report, "Placing Equity at the Center of Health Care & Technology."[194] These include the following:

- Moving beyond outdated privacy models that place too much emphasis on notice and consent, which put unreasonable burdens on consumers to read and understand each company's voluminous and dense privacy policy statements, and that fail to articulate data use limits;
- Covering all information that can be used to make inferences or judgments about, or otherwise misuse, a person's sensitive characteristics; and
- Covering all entities that collect, disclose, or use consumer sensitive information, regardless of the size or business model of the covered entity.

If the FTC were to determine that certain data practices can have demonstrable benefits to consumers, rules should be scoped to ensure consumers receive those benefits. For example, not all sensitive data uses, including those that utilize health and location data, are harmful. There are examples where health and location data can be utilized in a manner that both recognizes and protects individual user privacy, while also offering insights that can benefit public health and allow for dramatic improvements in health outcomes.[195] However, as detailed in Part 1, Section I, current laws and regulations do not prevent harmful uses. The Commission should act and promulgate new privacy rules that are rooted in fair and equitable principles and balance the benefits to consumers with risks.

FTC rules should restrict data brokers' misappropriation and misuse of data by:

---

[192] American Medical Association, *AMA Privacy Principles* (2020), https://www.ama-assn.org/system/files/2020-05/privacy-principles.pdf.

[193] The privacy principles embodied in the framework are not limited to only apply to self-regulatory regimes. Indeed, the principles were drafted to help both the public and private sectors better protect the privacy of people's health data. Crawford & Richardson, *supra* n. 187.

[194] Crawford, *Placing Equity*, *supra* n. 53.

[195] *See e.g.,* Mana Azarmi & Andrew Crawford, Center for Democracy & Technology, *Use of Aggregated Location Information and COVID-19: What We've Learned, Cautions about Data Use, and Guidance for Companies* 5-6 (2020), https://cdt.org/wp-content/uploads/2020/05/2020-05-29-Use-of-Aggregated-Location-Information-and-Covid-19.pdf.

- Prohibiting the sharing or sale to third parties of any data of consumers whose consent is not meaningfully informed and freely given in a way that specifies the context and scope for which they consent.
- Failing to provide effective opt-out mechanisms for consumers such as those described in Section II(B) below.
- Repurposing consumer data provided to another entity in ways that are inconsistent with consumers' reasonable expectations of the entity to whom the data was originally provided.[196]
- Misrepresenting to consumers the network of third parties with whom data will be shared.

The FTC should also apply data minimization requirements to the processing of data that is likely to produce discriminatory decisions. Specifically, FTC rules should prohibit companies from

- Using decision-making systems that evaluate data related to protected characteristics, or are heavily influenced by data that tend to disproportionately disadvantage marginalized communities, when
    - The data is unrelated to consumers' ability to fulfill the obligations they would incur if approved for the prospective opportunity, or
    - There are effective, less discriminatory alternatives to such decision-making systems.
- Continuing to use or analyze consumer data through a method that has been shown to disproportionately harm marginalized people.

B. Require companies to provide easily accessible consumer controls.

Meaningful, direct limitations and data minimization requirements put the least burden on consumers. But effective consumer controls can be an additional complement, allowing consumers to select the data use practices that work for them. For control requirements to be effective, controls must be, wherever feasible, universal preferences. Forcing consumers to opt out of data collection, sharing or re-use on every interaction in an online environment with widespread commercial surveillance is unreasonably burdensome, and would be equivalent to no genuine controls at all.

Opt-out control mechanisms should also be standardized, to ease adoption by industry and to facilitate effective choices by consumers. The Commission can provide guidance in regulation about consolidating on and respecting existing opt-out and consumer preference mechanisms,

[196] *See* Testimony of Andrew Crawford, *supra* n. 187; Crawford & Richardson, *supra* n. 193.

including the Global Privacy Control.[197] Clear regulatory guidance and enforcement of expressed preferences have been identified as needs for the successful standardization and widespread adoption of this class of consumer-controlled preference mechanism.[198]

Additional privacy-preserving advertising techniques are also possible, and could see further investment in response to signals from new regulatory requirements to provide consumers with more effective controls and context-based limits on the use of their personal information. Proposals deployed by browser vendors or proposed in technical standard-setting bodies include on-device auctions based on selected audiences or cohorts of interest topics. To the extent that many consumers see a benefit in personally targeted advertising, there are alternative techniques that can provide greater control, satisfaction, and data quality from consumers who choose to opt in and list their specific interests. The greatest impediment to progress on any of this class of proposals today is the lack of uptake from advertising firms who rely on and benefit from a status quo where consumers can be ubiquitously tracked and targeted with little transparency or effective control. Absent effective rules that promote consumer-controlled advertising, we do not expect the requisite work on development and adoption of these alternative advertising practices.

The Commission should anticipate that some companies will turn to practices that specifically undermine user control and consumer privacy once rules are in place and once increased technical mitigations are deployed. Privacy protections developed by online platforms – including web browsers and mobile operating systems – have led to similar kinds of industry workarounds that can maintain pervasive cross-context tracking of user behavior while circumventing user controls. Browser or device fingerprinting is one notable example, where a website or app will collect many different observable characteristics about the configuration of a device or browser to create a unique fingerprint that can track activity across multiple contexts without the user's knowledge or consent.[199] But there are many additional novel tracking techniques, including bounce tracking, and, more recently, direct solicitation of personally identifiable information that can be used for the secondary purpose of combining the user's data across many different contexts.

FTC rules should foresee and prohibit the use of techniques that circumvent technical privacy protections, as in the 2012 settlement of the Commission's complaint against Google for

---

[197] Global Privacy Control, https://globalprivacycontrol.org/. *See also* Cal. Civ. Code §1798.135(a)-(b); Colo. Rev. Stat §6-1-1313.

[198] Nick Doty, *Enacting Privacy in Internet Standards* 74-75 (University of California, Berkeley 2020), https://npdoty.name/writing/enacting-privacy/drafts/enacting-privacy-20201219.pdf.

[199] *See* Peter Eckersley, Electronic Frontier Found., *How Unique Is Your Web Browser?*, Proceedings of the 10th Int'l Symp. on Privacy Enhancing Technologies 4 (2010), https://coveryourtracks.eff.org/static/browser-uniqueness.pdf.

violating a previous consent decree and working around the Safari browser's cookie blocking mechanism.[200] The technical community has recognized that for some of these technical circumventions of privacy protections, technical protections will likely always be incomplete or insufficient, and that there is a specific need for regulation, investigation, and enforcement from authorities, including the Commission, to both protect privacy and provide a level playing field to companies that do not circumvent consumers' choices.[201]

C. Require companies to abide by meaningful transparency measures.

If the FTC establishes self-certification standards for companies' data practices, false or inaccurate certifications could trigger claims that the relevant practice is deceptive, but this might only incentivize companies to narrow their disclosures.[202] More effective transparency measures would (subject to any applicable First Amendment limits):

- Require companies to perform algorithmic impact assessments that proactively examine the practice's fitness for purpose, potential risks of disparate impact affecting all marginalized identities that may be subjected to the practice, and mitigating measures, and making assessment results or their summaries publicly available. Companies should not be permitted to use, sell, or provide a technology, online platform, or software that they claim to be nondiscriminatory if they do not provide pertinent information about the tool's impacts on all marginalized identities that may be subject to the tool, or if they obligate consumers to provide personal data to access the results or summaries of impact assessments.
- Establish that the information companies must disclose about their data practices should be provided in two forms: a shorter, easy-to- understand form with enough detail to enable consumers to interact with companies' platforms without being harmed, and a more thorough form with enough detail to enable regulators' enforcement. Companies must provide meaningful information to consumers before and after collecting, processing, or sharing consumer data, explaining the purpose for which the practice is used, reasons for possible and actual adverse decisions, factors that contribute to such decisions, and consumers' available alternatives to the data practice.

---

[200] Federal Trade Commission, *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser* (Aug. 9, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented-privacy-assurances-users-apples

[201] *See e.g.,* World Wide Web Consortium (W3C) Technical Architecture Group, *Unsanctioned Web Tracking* (2015) https://www.w3.org/2001/tag/doc/unsanctioned-tracking/.

[202] Inioluwa Deborah Raji, I. Elizabeth Kumar, Aaron Horowitz, and Andrew D. Selbst, *The Fallacy of AI Functionality*, Proceedings of the 2022 ACM Conf. on Fairness, Accountability & Transparency 959, 966, https://dl.acm.org/doi/pdf/10.1145/3531146.3533158.

- Require disclosures to be available in multiple commonly spoken languages and in plain language to ensure that all consumers are actually informed about how their data is handled. Companies must recognize that non-English-speaking consumers, consumers with disabilities – including blindness and disabilities affecting cognitive processing – and communities who experience barriers to education are entitled to this information.
- Enable comparison and easy understanding through standardized, short-form notice that is relevant to the context and medium. In other sectoral privacy laws and in other areas where consumers are expected to quickly comprehend product information,[203] standardized labels have been successful in enabling consumers to compare and make informed choices.

III. The FTC should consider several competition issues

(This section addresses Questions 26, 27, and 52.)

Rules to protect the security of sensitive personal information and to appropriately limit its use need not, and should not, interfere with the promotion and preservation of an open marketplace in which competition can grow and thrive, providing better choices to consumers and spurring innovation, higher quality, and more affordability. Indeed, as the Commission recognizes, lack of effective and enforceable privacy protections can put companies that do want to implement stronger privacy protections at a competitive disadvantage, both in terms of resources expended, and in terms of profit-making opportunities foregone. Thus, a properly crafted privacy rule would be pro-competitive.

Importantly, a new rule should allow for a platform to independently undertake continued innovation and improvements in privacy protection, as long as they do not undermine the protections required by the new rule. In this regard, there are some signs of competitive market incentives already at work. In response to growing consumer awareness, some online companies are strengthening their commitment to protecting personal data, including:

---

[203] *See e.g.*, 15 U.S.C. §6801 et seq; Lorrie Faith Cranor, Pedro Giovanni Leon, & Blase Ur, *A Large-Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices*, 10 ACM Transactions on the Web, no. 3 (Aug. 26, 2016): 17:1-17:33. https://doi.org/10.1145/2911988; Brian X. Chen, *What We Learned From Apple's New Privacy Labels*, N.Y. Times, (Jan. 27, 2021), https://www.nytimes.com/2021/01/27/technology/personaltech/apple-privacy-labels.html; Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor, *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, *in* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1573–82 (2010), https://doi.org/10.1145/1753326.1753561. Note that research has also shown challenges with comprehensibility of existing labels and recommended improvements. *See* Yucheng Li, Deyuan Chen, Tianshi Li, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I. Hong, *Understanding IOS Privacy Nutrition Labels: An Exploratory Large-Scale Analysis of App Store Data*, *in* Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems, 1–7 (2022), https://doi.org/10.1145/3491101.3519739.

- investing additional resources in data security infrastructure;
- limiting their own retention and use of personal data;
- developing technologies to minimize the data collected to provide new services;
- providing tools to protect against commercial surveillance;
- encrypting more communications to protect personal data from hackers and foreign governments;
- enabling simpler and more understandable consumer choices;
- making commercial data practices more transparent and easier to understand.

These market-driven motivations should be enabled and encouraged. The focus of a new rule should be on setting an appropriate floor for privacy that reins in anti-consumer incentives for online companies to exploit data in harmful ways, or to cut corners on protecting data – or to simply fail to invest sufficient effort and resources commensurate with making data protection a priority.

The Commission has extensive experience in assessing legislative and regulatory proposals to ensure that they do not unnecessarily interfere with the competitive process. It has on many occasions, over many years, rendered such "competition advocacy" advice to Congress, to other federal agencies, and to state legislatures and regulators. Such assessments are second nature to the Commission. And it will no doubt be mindful of that goal here in its own rulemaking.

Crafting appropriate privacy rules for online commerce will implicate sensitive technological issues that must be addressed with expert attention and care. CDT has previously emphasized the importance of the relevant regulatory agencies having their own technological expertise.[204] In this regard, it was encouraging to hear Chair Khan testify at the Senate Judiciary Committee's September 20 oversight hearing that the Commission has already significantly increased the number of technologists on its staff. Further increases will likely be warranted.

One challenge will be ensuring that any new rule appropriately protects privacy while not unduly preventing companies that are competing, or seeking to compete, from having fair access to information they need to offer their products and services. Mandating access could jeopardize key privacy and security safeguards the platform has constructed. On the other hand, requiring, or allowing, the creation of closed silos around data that an online platform has collected has the potential to interfere with competition – a potential that increases with the

[204] Center for Democracy & Technology, Comments to National Telecommunications and information Administration on Report on Competition in the Mobile App Ecosystem (May 23, 2022), https://cdt.org/insights/cdt-comments-to-ntia-on-mobile-app-ecosystem-competition/.

amounts of data that platform has collected. The Commission should endeavor to ensure that neither of these important objectives is compromised.

At one extreme, a blanket mandate of equal access to a platform's data risks undermining key privacy and security safeguards. But at the other extreme, blanket latitude for a platform to impose whatever restrictions it chooses under the pretext of protecting privacy and security risks unduly impairing competition and entrenching a platform's market power. The platform's selective use of blocking might, whether intentional or not, render competing online service providers unviable. The result could be anticompetitive effects that could be reasonably prevented, which the Commission's rules should not facilitate.

Another challenge will be taking into account the potential differential effects of a rule's requirements on small vs. large companies, and on established enterprises vs. new entrants. Protecting privacy should not have the side effect of making it too difficult for new competitors to enter the market and grow. Some differentiation in the requirements may be warranted to accommodate those differential effects. Any such differentiation should not, however, undermine the effectiveness of the requirements in protecting privacy.

Any new rules should be written so they can be adapted to take new insights into account – and, as the Commission notes, new changes in technology and new business models. And the Commission will still need to continue pursuing case-by-case enforcement as it learns, through investigatory experience, to distinguish restrictions that companies impose to protect the security of systems and data, and restrictions imposed to increase and entrench market power.

Providing choices to users through competition is one important spur for companies to innovate and provide better quality products and services, including better privacy protections. While these competitive incentives cannot take the place of effective rules, they should be encouraged and certainly not impeded.

Part 2: A privacy rule should be appropriately scoped to address impacts of commercial surveillance and lax data security practices in education and other government services

I. The FTC should adopt measures to mitigate unintended consequences for educational and governmental entities

Although the private sector data practices addressed throughout these comments should largely apply to all companies, private companies acting on behalf of public agencies require additional attention and nuance. As a result, the FTC should consider the data practices of private contractors for public sector entities in promulgating regulations. Public sector services, from education to governmental benefits, can be data intensive practices, and regularly involve the collection of personal data. Often, these services are provided in part or entirely by private contractors or vendors, and the FTC should proceed intentionally with respect to private contractors for public schools and other governmental entities.

The FTC should ensure that its new regulations do not hinder, but instead protect, the privacy-forward provision of governmental services. This section will discuss potential unintended consequences from overbroad regulations and how the FTC could potentially mitigate them.

A. Potential unintended consequences from overbroad regulations

Governments regularly contract out services to private companies, and many of those services involve data collection and use. Schools and school districts may contract with private contractors to provide systems for online lessons, communications services, or managing students' personal information. Other governmental entities may contract with private entities for a variety of services such as identity verification (discussed below in section III). A broadly applicable data-related rule may not apply as easily to entities providing government services and may even interfere with those services.

In recognition of that issue, for more than twenty years, agencies tasked with formulating and enforcing legal rules aimed at regulating the collection, use, maintenance, and disclosure of personal information have worked to avoid unintended consequences for schools and government contractors. For example:

- In its initial rulemaking under the Children's Online Privacy Protection Act (COPPA), the FTC acknowledged that strict application of COPPA to private contractors providing services to schools "would interfere with classroom activities, especially if parental

consent were not received for only one or two children."[205] In response, the FTC provided schools with flexibility to engage with contractors on behalf of parents "in the school setting."[206]

- In promulgating rules under the California Consumer Privacy Act (CCPA), the California Attorney General and the California Privacy Protection Agency have interpreted the CCPA to include carve outs for entities that provide services to schools and other governmental entities.[207] According to the California Attorney General, that carve-out was "necessary to address the unintended consequences that would result from allowing consumers to access and delete personal information held on behalf of public and nonprofit entities and that would otherwise not be subject to the CCPA."[208] For example, "a public school district may use a service provider to secure student information, including each student's grades and disciplinary record. Without this regulation, service providers used by public and nonprofit entities may be required to disclose or delete records in response to consumer requests."[209]

Lawmakers have also recognized the need to treat government service providers differently. For example, the House Commerce Committee amended the pending American Data Privacy and Protection Act (ADPPA)[210] to ensure that the bill would not have unintended consequences for government contractors. Amendments to the ADPPA ensured that governmental entities are not "covered entities" under the bill and that their contractors would be treated as "service providers" — and not directly subject to the bill's requirements for "covered entities."[211]

Those efforts have recognized that well-meaning — and much-needed — regulation of data processing could adversely impact schools and governmental entities in at least two ways:

- **Interfering with basic functions:** Overbroad applications of regulations may impede the ability of schools and other governmental entities to provide services to the public, as recognized in the promulgation of rules under COPPA and the CCPA.[212]

---

[205] 64 Fed. Reg. 59888, 59903 (Nov. 3, 1999).
[206] *Id.*; *accord* Federal Trade Commission, Complying with COPPA: Frequently Asked Questions sec. N (2020), https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.
[207] Cal. Code Regs. tit. 11, § 7051(a) (West 2022); Cal. Code Regs. tit. 11, § 999.314(a) (West 2021).
[208] Office of the California Attorney General, Final Statement of Reasons at 30 (2020), https://www.oag.ca.gov/privacy/ccpa/regs.
[209] *Id.*
[210] H.R. 8152, 117th Cong. (2022).
[211] H.R. 8152, Amendment in the Nature of a Substitute #1 (H8152_ANS_FC_02) sec. 2(9)(B)(i)-(ii), (29)(A)(ii), 117th Cong. (2002), https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=115041 (including entities that provide services to governmental entities as "service providers" but excluding them from the scope of "covered entities").
[212] 64 Fed. Reg. 59888, 59903 (Nov. 3, 1999); Office of the California Attorney General, Summary and Response to Comments Submitted during 45-Day Period, resp. 53 (2020), https://oag.ca.gov/privacy/ccpa/regs; Office of the California Attorney General, Final Statement of Reasons at 30 (2020), https://www.oag.ca.gov/privacy/ccpa/regs.

- **Creating legal confusion:** The collection, use, and disclosure of personal information by schools, governmental entities, and their contractors are already governed by laws such as the Family Educational Rights and Privacy Act (FERPA),[213] the Privacy Act of 1974,[214] and their state equivalents, which contain detailed rules. Any potential regulations should take into account those requirements and the circumstances of private contractors for public agencies. For example, even two closely related laws such as COPPA and FERPA have sometimes dissonant requirements, and the FTC has long recognized the need to harmonize their provisions.[215]

B. To mitigate unintended consequences, the FTC should build on existing legal requirements, ensure that new regulations are harmonized with existing laws, and supplement existing civil rights enforcement

As it considers regulations to address commercial surveillance and data security, the FTC should specifically consider the regulations' application to contractors for schools and other governmental entities. Possible strategies to mitigate unintended consequences in the education and governmental sectors include:

- **Reinforcing and building on existing legal requirements:** Existing federal laws such as COPPA, FERPA, the Privacy Act, and the e-Government Act[216] already address many of the issues discussed by the ANPR with regard to public agencies and their contractors, including use and purpose restrictions on personal information, data security requirements, data rights, and impact assessments. These existing rules have been shaped to avoid unintended consequences, and any regulations promulgated by the FTC could begin with those existing requirements and, if necessary, expand them to cover currently unaddressed harms.
- **Harmonizing with existing legal requirements, especially at the federal level:** The FTC has previously noted the tension between COPPA and FERPA — the statutes have similar overall scope and coverage, but different definitions of personal information, notice and consent requirements, and sets of data rights. That tension has only grown as technology has taken on an increasingly important role in education and government. CDT has called for the FTC to harmonize COPPA and FERPA in its pending COPPA rulemaking and renews that call here.
- **Supplementing existing civil rights enforcement:** Some uses of data and technology in the education and governmental sectors may have discriminatory effects, such as

[213] 20 U.S.C § 1232g; 34 C.F.R. §§ 99.1–.67.
[214] 5 U.S.C. § 552a.
[215] 84 Fed. Reg. 35842, 35845 (2019).
[216] E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (2002); *see also* Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435, 132 Stat. 5529 (2019).

through student activity monitoring software or premising access to governmental benefits on the use of facial recognition technology. For example, CDT has called on the Office for Civil Rights in the U.S. Department of Education to address harms from some uses of data and technology on students of color, students with disabilities, and LGBTQ+ students.[217]

Where the use of data and technology discriminates against legally protected classes, the FTC should coordinate with the appropriate enforcement authorities such as the U.S. Department of Education's Office for Civil Rights, the Equal Employment Opportunity Commission, the Federal Housing Administration, and the Department of Justice. Coordination could identify which agencies would address which harms, based on their respective experience, resources, and enforcement priorities, as well as conducting joint investigations. Such coordination could be memorialized in a memorandum of understanding or other documentation.

Although existing laws address many of the impacts of the uses of data and technology on civil rights, they do not cover all harms to historically marginalized groups of people. Where those harms are unaddressed, the FTC should promulgate regulations to provide a supplemental basis for protecting marginalized groups, including those that are not currently legally protected classes. The FTC's authority to protect marginalized groups is discussed below.

II. The FTC should address harms of commercial surveillance and lax data security practices in education

The FTC should consider commercial surveillance and lax data security by contractors in the education sector. Private contractors often provide data-intensive services to schools and other educational agencies, including IT infrastructure, online learning, and applications that monitor

[217] Center for Democracy & Technology, *Comment on Nondiscrimination on the Basis of Sex in Education Programs or Activities Receiving Federal Financial Assistance*, Docket No. ED-2021-OCR-0166 (filed Sept. 12, 2022), https://cdt.org/insights/cdt-urges-us-department-of-education-to-protect-lgbtqi-students-from-discrimination-in-proposed-title-ix-rules; Letter to Catherine Lhamon, Assistant Secretary for Civil Rights, U.S. Department of Education, from Coalition of Civil, Digital, and Education Rights Organizations (filed Aug. 2, 2022), https://cdt.org/insights/letter-to-ed-office-for-civil-rights-on-discriminatory-effects-of-online-monitoring-of-students/; Center for Democracy & Technology, *Comment on Request for Information Regarding the Nondiscriminatory Administration of School Discipline*, Docket No. ED-2021-OCR-0068 (filed July 23, 2022), https://cdt.org/insights/cdt-comments-to-us-dept-of-ed-urging-the-protection-of-students-of-color-and-students-with-disabilities-and-their-data; Center for Democracy & Technology, *Comment on Announcement of Public Hearing; Title IX of the Education Amendments of 1972*, 86 Fed. Reg. 27429 (filed June 11, 2021), https://cdt.org/insights/cdt-comments-on-protecting-privacy-rights-and-ensuring-equitable-algorithmic-systems-for-transgender-and-gender-non-conforming-students/.

students' online activity. Because schools and students are required to exchange data in return for those services provided by private, for-profit entities, the services fit within the FTC's definition of "commercial surveillance."[218] Although some laws already govern private contractors' use of student data, they often have limited reach and may not curtail commercial use of students' data, invasive surveillance, or lax data security practices.

A. The FTC should address commercial surveillance in education by enforcing existing limitations, extending those limitations to all students, and utilizing its Section 5 authority to protect marginalized groups

Commercial surveillance in the education sector can cause discriminatory harm to students, as CDT research shows. To mitigate these harms, the FTC should:

- Redouble efforts to enforce existing limitations already in COPPA for students and schools.
- Extend COPPA's existing limitations and security requirements in a limited manner under Section 5 to ed tech companies and other contractors providing services in the education context to all students, regardless of their age.
- Address discriminatory uses of data and technology in education by utilizing its Section 5 authority to combat unaddressed civil rights harms.

i. Commercial Surveillance in Education Causes Discriminatory Harms to Students (Q53, 65)

Students and families may be subjected to commercial surveillance throughout the education context, from the use of cameras equipped with computer vision on campus, to algorithms that make critical decisions about students' lives, to software that monitors everything students do online — often through technology sold by private contractors. Those uses of data and technology surveil students often without meaningful consent or opportunity to opt out

[218] We use the term "surveillance" only in the sense used in the ANPR, and not necessarily in the ordinary sense. Student activity monitoring and other practices in the education sector described in these comments likely constitute "commercial surveillance" as defined in the ANPR. The ANPR defines "commercial surveillance" broadly as "the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and [its] direct derivatives." 87 Fed. Reg. 51273, 51277 (Aug. 22, 2022). The term "consumer" includes not only individuals but also "small businesses and . . . not-for-profit organizations," FTC v. IFC Credit Corp., 543 F. Supp. 2d 925, 934-41 (N.D. Ill. 2008), and the FTC has previously found that harms to students constitute harms to consumers, *see* Complaint ¶¶ 2-6, In the Matter of MacMillan, Inc., 96 F.T.C. 208 (1980), https://www.ftc.gov/sites/default/files/documents/commission_decision_volumes/volume-96/ftc_volume_decision_96_july_-_december_1980pages_208-331.pdf; Federal Trade Commission, Notice of Penalty Offenses Concerning Deceptive or Unfair Conduct in the Education Marketplace (2021), https://www.ftc.gov/enforcement/penalty-offenses/education. Because students and schools receive services from private contractors, including systems for online lessons, communications services, or managing students' personal information, often in exchange for data, those services constitute "commercial surveillance" under the ANPR.

because they are a condition for students' ability to access a fundamental service — their education.

Student monitoring is pervasive, as is the discriminatory impacts of commercial surveillance in schools.[219] CDT recently researched student activity monitoring software, a type of school surveillance technology that allows schools to view students' screens, record their browsing and search histories, and scan their messages and documents stored online or on school devices. The resulting surveillance is pervasive: 89 percent of teachers report that their school uses student activity monitoring software,[220] and monitoring often occurs even outside of school hours. CDT's research — attached to these comments — reveals how online monitoring violates rights traditionally protected by civil rights laws:[221]

- **Title VI: Exacerbating disproportionate discipline and law enforcement interactions for students of color.** As a result of student activity monitoring, students of color are experiencing increased interactions with law enforcement, as well as being disciplined at disproportionate rates. **44 percent** of teachers report that students were contacted by law enforcement as a result of behaviors flagged by student activity monitoring.[222] Moreover, **78 percent** of teachers report that student activity monitoring flagged students for violations of disciplinary policy, and **59 percent** report that a student was actually disciplined following those alerts.[223] That discipline falls disproportionately along racial lines, with **48 percent of Black students and 55 percent of Hispanic students** reporting that they or someone they know got into trouble as a result of student activity monitoring — compared to 41 percent of white students.[224]
- **Title IX: Targeting LGBTQ+ students for "outing," discipline, and criminal investigations.** LGBTQ+ students are disproportionately targeted as a result of student activity monitoring. **29 percent** of LGBTQ+ students report that they or another student they know has had their sexual orientation or gender identity disclosed without their consent (i.e., was "outed") due to student activity monitoring.[225] Additionally, **56 percent** of LGBTQ+ students reported that they or someone they know was disciplined as a result of student activity monitoring, and **31 percent** reported they were contacted by law

[219] Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke, & Hannah Quay-de la Vallee, Center for Democracy & Technology, *Hidden Harms: The Misleading Promise of Monitoring Students Online* (2022), https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of- monitoring-students-online [hereinafter *Hidden Harms*].
[220] *Id.* at 8.
[221] *Id.* at 19-24.
[222] *Id.* at 20.
[223] *Id.* at 24.
[224] *Id.*
[225] *Id.* at 21.

enforcement regarding a crime flagged by the software — compared to 44 percent and 19 percent, respectively, for their non-LGBTQ+ peers.[226]

- **Americans with Disabilities Act and Section 504 of the Rehabilitation Act: Harming students' expression and mental health.** Research also suggests that students with disabilities are experiencing disproportionate harm as a result of student activity monitoring, including through behavioral threat assessments.[227] Approximately **five in ten** students agree with the statement: "I do not share my true thoughts or ideas because I know what I do online may be monitored."[228] This chilling effect is compounded for students with learning differences and physical disabilities, with **60 percent and 67 percent**, respectively, reporting that they do not share their true thoughts or feelings due to monitoring.[229] Moreover, **66 percent** of teachers are concerned that students are less likely to access resources or visit websites that might provide help to them, such as how to share their sexual orientation or gender identities with their families or how to access mental health supports.[230]

Finally, previous CDT research showed that students experiencing poverty and students of color rely more heavily on school-issued devices, which are more likely to be subject to monitoring than personal devices.[231] As a result, these groups of students are similarly subject to increased risks of discrimination.

National reporting has also underscored the harms caused by commercial surveillance in education. Students with disabilities are at higher risk of generating false positives and false negatives when surveilled by student monitoring tools that are designed to identify atypical sounds, text, speech, or movements as potential indicators that students may be engaging in violent or prohibited conduct, making threats, or cheating on tests. For instance, a ProPublica investigation found that aggression-detection microphones were so unreliable that they flagged

---

[226] *Id.* at 21.
[227] Brown, *Surveillance Technologies*, *supra* n. 12, at 16, 17-21; Jazmyne Owens, New America, *Threat Assessment Systems as a School Safety Strategy* (2021), https://www.newamerica.org/education-policy/briefs/threat-assessment-systems-as-a-school-discipline-safety-strategy/.
[228] *Hidden Harms*, *supra* n. 219, at 22.
[229] *Id.* at 23.
[230] *Id.*
[231] DeVan L. Hankerson Madrigal, Cody Venzke, Elizabeth Laird, Hugh Grant-Chapman, & Dhanaraj Thakur, Center for Democracy & Technology, *Online and Observed: Student Privacy Implications of School-Issued Devices and Student Activity Monitoring Software* 10 (Sept. 21, 2021), https://cdt.org/insights/report-online-and-observed-student-privacy-implications-of-school-issued-devices-and-student-activity-monitoring-software/; Hugh Grant-Chapman & Elizabeth Laird, Center for Democracy & Technology, *Research Slides: Key Views Toward Ed Tech, School Data, and Student Privacy* 48 (Nov. 15, 2021), https://cdt.org/insights/report-navigating-the-new-normal-ensuring-equitable-and-trustworthy-edtech-for-the-future.

loud laughter and locker doors slamming as indicators of violence.[232] Those false positives raise concerns for students whose disabilities affect their speech and movement, such as students with cerebral palsy who might not be able to modulate voice volume or students with Tourette's who have loud vocal tics.

Meanwhile, student advocacy organizations such as the National Disabled Law Students Association have documented the discriminatory barriers that students with a wide range of disabilities, including ADD, blindness, and Crohn's disease, experience when required to use automated proctoring software.[233] Students reported not being permitted to take enough bathroom breaks, worrying about false positives from needing to move or pace, or not moving their eyes or hands the right way. For disabled students of color or LGBTQ+ students with disabilities, who also face additional discrimination and prejudice, the risks of student monitoring and commercial surveillance programs are further compounded by their intersected identities.

ii. Emphasize Existing Limitations under COPPA (Q34)

To address these harms, the FTC should first continue to emphasize existing requirements under COPPA[234] that address commercial surveillance in education.[235] The FTC has already taken a strong step in this direction, when it released a policy statement this past spring,[236] making clear that it expected ed tech providers in particular to adhere to COPPA's limitations. In the policy statement, the FTC said, "[g]oing forward, the Commission will closely scrutinize the providers of these services and will not hesitate to act where providers fail to meet their legal obligations with respect to children's privacy."[237]

The policy statement emphasized that "operators of ed tech that collect personal information pursuant to school authorization may use such information only to provide the requested online education service,"[238] and that "ed tech companies are prohibited from using such information for any commercial purpose."[239] Use limitations may help mitigate the impacts of commercial

[232] Jack Gillum & Jeff Kao, *Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students*, ProPublica (June 25, 2019), https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/.
[233] National Disabled Law Students Association, *Report on Concerns Regarding Online Administration of Bar Exams* (2020), https://ndlsa.org/wp-content/uploads/2020/08/NDLSA_Online-Exam-Concerns-Report1.pdf.
[234] 64 Fed. Reg. 59888, 59903 (Nov. 3, 1999).
[235] COPPA also addresses lax data security practices in education, which are addressed below. *See* Part 2, Sec. II.B.
[236] Federal Trade Commission, Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act 3 (2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-crack-down-companies-illegally-surveil-children-learning-online.
[237] *Id.* at 4.
[238] *Id.* at 3.
[239] *Id.* at 3.

surveillance in education by ensuring that data is collected and used only for a specified educational purpose.[240]

The FTC should continue to emphasize and enforce those existing protections.

iii. Extend Certain COPPA Privacy Protections to Ed Tech Companies and Other Contractors that Provide Services in the Education Context to All Students (Q47)

Second, the FTC should consider using its authority under Section 5 to extend the specific privacy protections of COPPA set forth in its policy statement to all data collected and maintained by ed tech providers and other private third parties during the course of providing service for schools — regardless of whether the student is under 13. Namely, the FTC should utilize its Section 5 authority to ensure that all contractors providing services to schools abide by limitations that prohibit private companies from exploiting student data gathered through commercial surveillance.

One of the chief extensions that could bring substantial benefit with minimal costs is extending COPPA's existing use limitations to ed tech providers that provide services to students over 13 in the education context. Evidence is increasingly demonstrating that commercial surveillance in education harms students; privacy limitations will help limit the use (and potentially then the collection) of student data to only specified educational purposes.[241]

Extending COPPA's limitations in this limited way is within the FTC's authority under Section 5 because commercial surveillance in education constitutes an unfair and deceptive practice when it results in discrimination or other harms:

- **Commercial Surveillance in Education Is an Unfair Practice:** Students and families entrust schools and their contractors with their students' wellbeing, including responsible stewardship of their data, and overbroad commercial surveillance in education constitutes an unfair practice:
    - *Substantial injury:* Commercial surveillance in education, such as student activity monitoring online, injures students, families, and students. As CDT research shows, commercial surveillance in education results in discriminatory harms by outing LGBTQ+ students, subjecting them and students of color to disparate discipline, and chilling the access of students with disabilities to resources supporting their mental health.[242]

[240] Complying with COPPA: Frequently Asked Questions, Federal Trade Commission § N, https://www.ftc.gov/businessguidance/resources/complying-coppa-frequently-asked-questions (last visited Sept. 28, 2022).
[241] *Id.*
[242] *Hidden Harms*, *supra* n. 219.

- *Not reasonably avoidable:* Students and families are likely unable to avoid those injuries, because they do not have a meaningful choice in whether to consent to the surveillance. Students are often required or encouraged to use school-issued devices that are subject to monitoring,[243] or they may rely on school-issued devices because of their families' socioeconomic status.[244] Further, students and families are often not provided accurate, complete disclosures around commercial surveillance in education. For example, in recent CDT research, 47 percent of parents reported they were not informed about how their schools' contractors collect data about students' activity online; only 39% reported they were asked for input on those practices.[245] Even if students and families are provided adequate disclosures, they are typically not given a choice (whether opt-in or opt-out) with respect to whether and how schools or their contractors monitor student online activity. Moreover, families are often obstructed in asserting legal rights under COPPA or FERPA, with schools and contractors failing to implement clear procedures for exercising legal rights for data held by those contractors.[246] Moreover, it may be impractical or even impossible for students and families to switch schools to avoid their commercial surveillance practices.

- *Not outweighed by countervailing benefits to consumers or competition:* The discriminatory harms of commercial surveillance in educaton outweigh its purported benefits to consumers or competition — especially to students. Although vendors claim that student activity monitoring and other forms of commercial surveillance benefit students, those claims are largely

[243] Hankerson Madrigal, *supra* n. 231, at 10.
[244] *Id.*
[245] Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke, & Hannah Quay-de la Vallee, Center for Democracy & Technology, *Hidden Harms: Research Slide Deck* 30–32 (2022), https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of-monitoring-students-online.
[246] Cody Venzke, *What Is an Education Record? That is the Question that the Department of Education Should Answer*, Center for Democracy & Technology (Mar. 16, 2022), https://cdt.org/insights/what-is-an-education-record-that-is-the-question-that-the-department-of-education-should-answer/ ("[C]onfusion over the scope of 'education records' has caused parents to receive conflicting instructions from schools and the company, as each directed parents to submit their requests to the other. Consequently, parents' requests often languished for months.").

unsubstantiated.[247] Unproven benefits cannot outweigh documented discrimination and other harms, particularly when those harms could themselves be mitigated by data minimization, use restrictions, and similar practices.

- **Commercial Surveillance in Education Is a Deceptive Practice:** Commercial surveillance in education constitutes a deceptive practice for schools, students, and families if ed tech providers and other contractors collect more student data than necessary or use it in ways that are not disclosed:
    - *Misleading to consumers acting reasonably under the circumstances:* Schools have very little ability to gain insight into contractors' data practices, no matter how reasonable their precautions, and this prevents them from providing parents with adequate notice. Schools, families, and students are consequently dependent on contractors' representations regarding data use, and any misrepresentation or omission about collections or uses of student data would be misleading.

      For example, in CDT interviews, school district IT leaders stated that they had very little insight into contractors' practices. One IT leader commented, "One of the biggest challenges…[is that our students' data is] not on our servers like it used to be in the old on-[premises] days. We have language in place to protect the data [such] that they don't share it while they have it on their servers."[248] Another described the difficulty of verifying contractors' data usage and security practices, stating, "We have a tough enough problem right now, trying to prove to outsiders that we are protecting their data."[249] This precludes families from receiving adequate notice; in CDT research, only 39 percent of students and 47 percent of parents stated they had been informed about certain commercial surveillance used in schools.[250]

    - *Materiality:* Schools value transparency regarding contractors' collection and use of student data. In interviews, school IT leaders stated they took strides through contractual measures to hold contractors accountable for their uses of student

[247] Center for Democracy & Technology & Brennan Center for Justice, Social Media Monitoring in K-12 Schools: Civil and Human Rights Concerns (2019), https://cdt.org/insights/social-media-monitoring-in-k-12-schools-civil-and-human-rights-concerns; *see also* Rebecca Heilweil, *The Problem with Schools Turning to Surveillance After Mass Shootings*, Vox (June 2, 2022, 7:30 AM), https://www.vox.com/recode/23150863/school-surveillance-mass-shooting- texas-uvalde; Lucas Ropek, *Surveillance Tech Didn't Stop the Uvalde Massacre*, Gizmodo (May 27, 2022), https://gizmodo.com/surveillance-tech-uvalde-robb-elementary-school-shootin-1848977283; Jolie McCollough & Kate McGee, *Texas Already "Hardened" Schools. It Didn't Save Uvalde.*, Texas Tribune (May 26, 2022), https://www.texastribune.org/2022/05/26/texas-uvalde-shooting-harden-schools;
[248] Hankerson Madrigal et al., *supra* n. 231, at 17.
[249] *Id.* at 18.
[250] *Hidden Harms*, *supra* n. 219, at 17.

data, and expressed frustration with "what they describe as a lack of distinguishable options for privacy-forward devices."[251] Similarly, 94 percent of parents and 88 percent of students stated it was "important" for schools to engage them on the uses of student data.[252] Transparency around contractors' collection and use of student data consequently "would likely affect the consumer's conduct or decisions with regard to a product or service."

Because overbroad commercial surveillance in schools is an unfair practice, particularly when it results in discriminatory harms, and the lack of accurate and adequate disclosures around such surveillance is deceptive, the Commission has authority under Section 5 to extend the privacy protections under COPPA described in its policy statement to ed tech providers and other contractors that provide services to all students, not just those under 13. The privacy protections under COPPA will help mitigate the significant harms that many teen students are experiencing today as a result of overbroad surveillance in the educational setting, and the Commission should accordingly extend those protections to all students as part of this proceeding.

iv. Utilize FTC Authority to Protect Historically Marginalized Groups (Q67-69, 72)

The FTC can utilize its experience with data and technology and authority under section 5 to help supplement existing civil rights protections and mitigate currently unaddressed harms to historically marginalized groups. The FTC's efforts will be particularly critical where historically marginalized groups are not recognized as a legally protected class, such as unhoused students, low-income students, foster care students, and rural students.

These comments previously detailed gaps in existing civil rights law for private sector entities,[253] and those gaps exist in education as well:

- Title VI[254] and Title IX[255] prohibit discrimination on the basis of race, sex, and related classes by entities receiving certain federal funds, including in the education sector. However, when discrimination is caused by technology distributed by private contractors for schools, students and families may not be aware of the discriminatory impact, due to a lack of transparency around the implementation and utilization of technological systems. For example, an algorithmic system used to assign students to schools may rely

[251] Hankerson Madrigal et al., *supra* n. 231, at 17.
[252] *Hidden Harms*, *supra* n. 219, at 18.
[253] *See* Part 1, Sec. I.
[254] 42 U.S. Code § 2000d.
[255] 20 U.S.C. §§ 1681–1688.

on a variety of factors, not all of which may be known to students and families;[256] this information asymmetry may make it difficult or impossible to challenge discriminatory practices caused by data or technology use.

- Title VI[257] and Title IX[258] similarly prohibit entities receiving certain federal funds from acquiring discriminatory technology, but would not preclude private vendors from selling it in the first place.
- Further, certain uses of data and technology may not intentionally discriminate against consumers based on race, sex, disability status, or other protected classes, but nonetheless cause disparate impact. Courts, however, have curtailed consumers' ability to challenge disparate impact under critical civil rights laws in court,[259] limiting their ability to seek redress.

The FTC's Section 5 authority can help fill in gaps in existing civil rights laws in education by deeming certain discriminatory uses of data and technology to be an unfair or deceptive practice:

- **Discriminatory uses of data and technology are an unfair practice:** As noted throughout these comments, families and students entrust their data to schools and their contractors on the premise that the data will be used for beneficial purposes while minimizing harms.[260] Discriminatory uses of data and technology in the education context violate that trust and meet the requirements for an unfair practice:
    - *Substantial injury:* As demonstrated by CDT's research described above, discriminatory uses of data and technology can place students at risk. Student activity monitoring in particular threatens to out LGBTQ+ students, places LGBTQ+, Black, and Hispanic students at risk of disproportionate discipline and contact with law enforcement, and chills disabled students' access to resources online. These incursions on students' fundamental rights constitute a substantial injury and are a betrayal of schools' role as "the nurseries of democracy."[261]
    - *Not reasonably avoidable:* As noted above, schools, families, and students have little insight into or control over contractors' practices, including discriminatory

[256] Hannah Quay-de la Vallee & Natasha Duarte, Center for Democracy & Technology, *Algorithmic Systems in Education* 8-9 (2019), https://cdt.org/insights/algorithmic-systems-in-education-incorporating-equity-and-fairness-when-using-student-data/.
[257] 42 U.S. Code § 2000d.
[258] 20 U.S.C. §§ 1681–1688.
[259] *E.g.*, Jackson v. Birmingham Bd. of Educ., 544 U.S. 167, 178, 178 n.2 (2005) (Title IX); Alexander v. Sandoval, 532 U.S. 275 (2001) (Title VI); Doe v. BlueCross BlueShield of Tenn., Inc., 926 F.3d 235, 240-42 (6th Cir. 2019).
[260] Elizabeth Laird & Hannah Quay-de la Vallee, Center for Democracy & Technology, *Data Ethics in Education & the Social Sector* (2021), https://cdt.org/insights/report-data-ethics-in-education-and-the-social-sector-what-does-it-mean-and-why-does-it-matter.
[261] Mahanoy Area Sch. Dist. v. B.L., 141 S. Ct. 2038, 2046 (2021).

uses of data and technology, and often lack a choice about whether to use ed tech that uses surveillance. With limited insight and control, schools, families, and students cannot reasonably avoid contractors' discriminatory uses of data and technology.

- *Not outweighed by countervailing benefits to consumers or competition:* Finally, as described above, the harms from discriminatory uses of data and technology outweigh any unproven benefits to students.

- **Discriminatory uses of data and technology are a deceptive practice:** As with commercial surveillance, schools have very little insight into contractors' practices,[262] including for discriminatory uses of data and technology, and are consequently dependent on contractors' representations regarding data use when selecting education technology products. Any misrepresentations or omissions regarding the discriminatory impact of contactors' use or collection of student data would constitute a deceptive practice.

The FTC accordingly should issue rules as part of this proceeding that would prohibit collection or use of data in school settings that discriminates or has a disparate impact on students in protected classes or those in marginalized groups such as unhoused students, low-income students, and foster care students.

B. The FTC should address lax data security practices in education by extending existing data security requirements to ed tech providers and other contractors in the education setting

To mitigate harms from lax data security practices by contractors in the education sector, the FTC should enforce existing requirements under COPPA and extend COPPA's security requirements to ed tech companies and other contractors providing services to all students in the education context, regardless of their age, under Section 5.

i. Lax Data Security Practices Harm Students and Schools

Lax data security practices by private contractors in the education sector harm students, families, and schools. Lax data security practices can result in breaches and other data security incidents, which have substantially increased in both number and scope since 2016.[263] For example, one recent incident involved a contractor serving schools in six states, affecting over three million current and former students.[264] Similarly, a recent ransomware attack on Los

[262] Hankerson Madrigal et al., *supra* n. 231, at 17–18.
[263] K12 SIX, State of K-12 Cybersecurity 3 (2022), https://www.k12six.org/the-report.
[264] Mark Keierleber, *After Huge Illuminate Data Breach, Ed Tech's 'Student Privacy Pledge' Under Fire*, The 74 (July 24, 2022),

Angeles Unified School District resulted in the release of students' personal information, and parents and students have questioned the district's preparation and transparency.[265]

Those breaches not only undermine students' and families' trust in schools and contractors, but can put their financial and physical wellbeing at risk. As the Government Accountability Office has described, student data "can be sold on the black market and can cause significant financial harm to students who typically have clean credit histories and often do not inquire about their financial status until adulthood."[266] One breach included the personal information of students who completed surveys on bullying, and another included students' phone numbers, which "were used to send text messages that threatened physical violence."[267]

Lax data practices strain the resources of schools and place students and families at risk. For example, a ransomware attack on a Texas school district cost more than a half million dollars to mitigate, and attacks in Baltimore and Buffalo cost in excess of $9 million each.[268]

ii. Emphasize Existing Security Requirements under COPPA (Q34)

In addition to emphasizing existing privacy limitations under COPPA, the FTC should continue to emphasize COPPA's existing security requirements in the education context.[269] The FTC's policy statement released this past spring[270] made it clear that it expected ed tech providers in particular to adhere to COPPA's data security requirements. In the policy statement, the FTC stated, "COPPA-covered companies, including ed tech providers, must have procedures to maintain the confidentiality, security, and integrity of children's personal information. For example, even absent a breach, COPPA-covered ed tech providers violate COPPA if they lack reasonable security."[271]

---

https://www.the74million.org/article/after-huge-illuminate-data-breach-ed-techs-student-privacy-pledge-under-fire/.

[265] Howard Blume & Alejandra Reyes-Velarde, *Student Information Remains at Risk After Massive Cyberattack on Los Angeles Unified*, Los Angeles Times (Sept. 7, 2022), https://www.latimes.com/california/story/2022-09-07/los-angeles-unified- schools-cyberattack; Joshua Bay, *LA Parents Sound Off After Cyberattack Leaves Students Vulnerable*, The 74 (Oct. 7, 2022), *https://www.the74million.org/article/la-parents-sound-off-after-cyberattack-leaves-students-vulnerable*.

[266] Government Accountability Office, Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm 13 (2021), https://www.gao.gov/products/gao-20-644.

[267] *Id.*

[268] K12 SIX, *supra* n. 263, at 8; *see also* McKenna Oxenden, *Baltimore County Schools Suffered a Ransomware Attack. Here's What You Need to Know*, Baltimore Sun (Nov. 30, 2020, 8:33 PM), https://www.baltimoresun.com/maryland/baltimore-county/bs-md-co-what-to-know-schools-ransomware-attack-20201130-2j3ws6yffzcrrkfzzf3m43zxma-story.html.

[269] 16 C.F.R. §§ 312.3(e), 312.8.

[270] Federal Trade Commission, Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act 3 (2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-crack-down-companies-illegally-surveil-children-learning-online.

[271] *Id.* at 3 (citing 15 U.S.C. § 6502(b)(1)(D); 16 C.F.R. § 312.8; 16 C.F.R. § 312.10).

The FTC should continue to emphasize and enforce those existing protections.

iii. Extend COPPA Data Security Requirements to Ed Tech Companies and Other Contractors Providing Services in the Education Context to All Students (Q47)

The FTC should use its authority under Section 5 to extend COPPA's Data Security requirements to all data collected and maintained by ed tech companies and other private third parties during the course of providing service for public schools, regardless of whether the student is under 13.

The FTC has authority to address lax data security practices by edtech providers as an unfair and deceptive practice under Section 5:

- **Lax Data Security In the Educational Context Is an Unfair Practice:**
    - *Substantial injury:* Lax data security practices can result in breaches and other data security incidents, which have substantially increased in both number and scope since 2016.[272] Those breaches not only undermine students' and families' trust in schools and contractors, but can put their financial and physical wellbeing at risk, as described above. One breach included the personal information of students who completed surveys on bullying, and another includes students' phone numbers, which "were used to send text messages that threatened physical violence."[273]
    - *Not reasonably avoidable:* Students and families have no ability to avoid the consequences of contractors' lax security practices. Moreover, laws governing data in this space provide almost no relief for students and parents directly: FERPA provides families with no private right of action,[274] gives the U.S. Department of Education little oversight authority over private contractors,[275] and does not even require schools to notify parents of data breaches.[276] Similarly, COPPA provides no private right of action[277] and only protects children under

[272] K12 SIX, *supra* n. 263, at 3.
[273] *Id.*
[274] *Gonzaga University* v. *Doe,* 536 U.S. 273, 288 (2002).
[275] The "five-year rule" under FERPA permits the Department of Education to prohibit a particular educational institution or agency from disclosing students' personal information to a particular third party that has violated certain provisions of the law. 34 C.F.R. § 99.67. However, "the five-year rule does not prohibit *all* educational agencies and institutions from disclosing PII from education records to the offending third party; as made clear by the statute, the prohibition only applies to the educational agency or institution *that originally disclosed* PII from education records to that third party." 76 Fed. Reg. 75603, 75635 (Dec. 2, 2011) (emphasis added).
[276] 73 Fed. Reg. 74805, 74843 (2008) ("The Department does not have the authority under FERPA to require that agencies or institutions issue a direct notice to a parent or student upon an unauthorized disclosure of education records. FERPA only requires that the agency or institution record the disclosure" in the student's education record.).
[277] *Cf.* 15 U.S.C. §§ 6504–05; *N.M. ex rel. Balderas v. Tiny Lab Prods.*, 457 F. Supp. 3d 1103, 1120-21 (D.N.M. 2020).

13.[278] Contractors alone have the knowledge and capacity to identify cybersecurity threats,[279] and the responsibility for establishing reasonable security measures should lie with them.

- *Not outweighed by countervailing benefits to consumers or competition:* Lax data practices do not benefit consumers or competition, but instead strain the resources of schools and place students and families at risk, with the costs of responding to a single breach sometimes reaching millions of dollars,[280] and undermine competitive incentives to provide greater care in data security.

- **Lax Data Security Practices Are a Deceptive Practice:** Lax data security in education also constitutes a deceptive practice if contractors' representations regarding their security practices are materially misleading to students, families, or schools. As described above, schools have very little insight into contractors' practices, including for data security,[281] and are consequently dependent on contractors' representations regarding data use when selecting education technology products.

For these reasons, the FTC should utilize its Section 5 authority to extend COPPA's data security requirements to ed tech companies and other private contractors that provide services in the education context to all students, including those 13 or older.

III. The FTC should regulate private vendors that provide identity verification for government service delivery

In its definition of marginalized populations that might be affected by data surveillance, the FTC included both recipients of government services and victims of identity theft. Both groups of individuals face risks from the use of private vendors by state and federal agencies providing benefits and services.[282] However, regulation of private vendors assisting with government service delivery presents a further challenge: just as with private providers of educational services, improperly considered rules may hamper the ability of government agencies to effectively deliver essential services.

On the other hand, rules are clearly needed: the use and collection of citizen data by private companies poses risks to privacy that could result in material harm, such as identity theft; and government outsourcing of key benefits determinations to private companies can result in

[278] 15 U.S.C. §§ 6501–02.
[279] Hankerson Madrigal et al., *supra* n. 231, at 7.
[280] K12 SIX, *supra* n. 263, at 8.
[281] Hankerson Madrigal et al., *supra* n. 231, at 17–18.
[282] Here, we focus on practices that involve passing data to private technology vendors and exclude services that are provided solely by governmental entities or primarily involve in-person verification.

preventing some individuals from getting essential benefits. General privacy practices for consumer data similar to those discussed above should apply to the use of third-party private vendors for government services. These requirements include the following:

- data use limitations that prohibit the usage of user data for secondary services like selling other products;[283]
- data minimization limitations that restrict private vendors to collecting only to what is required to provide the contracted services;
- data retention limitations under which data is stored only as long as needed to perform services; and
- adoption of up-to-date data security practices to protect any data that must be stored.

The FTC should consider promulgating rules imposing these requirements on private vendors who work in government service delivery.

Identity verification – a government service that often utilizes private vendors – poses heightened risks and would benefit from more specific requirements that build on general data privacy and security practices.

The starting point for delivery of governmental benefits is identity verification, where the government agency checks that an applicant is who they say they are. As public agencies seek to modernize identity verification through data and technology use, they are increasingly considering incorporating assistance from private companies. Examples of vendor assistance include: attribute validation, where the vendor confirms that the information provided by an applicant matches that in other identity databases (such as driver's license data, health records, or financial records); and biometric verification, where the vendor confirms through the use of physical or biological information that the applicant matches any submitted identity documents (1:1 matching) or other biometric information in the vendor's database (1:many matching). Most recently, the use of facial recognition as a kind of biometric verification has garnered widespread scrutiny.[284]

The two main risks in the provision and use of such identification verification services on which the FTC should focus are inadequate privacy protections and biased algorithms.[285]

---

[283] Joseph Cox, *LexisNexis to Pay $5 Million Class Action Settlement for Selling DMV Data*, Vice (Nov. 5, 2020, 9:30 AM), https://www.vice.com/en/article/epddy4/lexisnexis-dmv-data-class-action-settlement.
[284] Brian Naylor, *IRS Has Second Thoughts About Selfie Requirement*, NPR (Feb. 7, 2022, 3:29 PM), https://www.npr.org/2022/02/07/1078024597/want-information-from-the-irs-for-some-the-agency-wants-a-selfie.
[285] Hannah Quay-de la Vallee, *Public Agencies' Use of Biometrics to Prevent Fraud and Abuse: Risks and Alternatives*, Center for Democracy & Technology (Jun. 7, 2022), https://cdt.org/insights/public-agencies-use-of-biometrics-to-prevent-fraud-and-abuse-risks-and-alternatives/.

A. The FTC should protect privacy in identity verification services

Private third-party processing of sensitive information for purposes of identity verification poses threats to privacy and equitable access to governmental services. Without adequate protections, sensitive data could end up in the hands of bad actors and lead to identity fraud. Some examples include the following:

- ID.me, a facial recognition identity verification company, allowed employees to bring home devices that carried U.S. citizens' identity data and retained biometric data longer than necessary.[286] Such practices increase the chances of data being leaked onto the internet and later used for identity theft.
- Equifax, a credit agency that also provides attribute validation for identity verification, exposed personal information of 147 million people in a 2017 data leak, over which they settled with the FTC in 2017.[287]

The Equifax leak and other leaks of data allowed both domestic and foreign criminals to defraud state governments of pandemic unemployment assistance by using false or stolen identities.[288] Victims of identity theft face significant obstacles in re-asserting their identity and regaining access to government services. As supporting victims of identity theft is already one of FTC's functions, the FTC should consider how best to prevent identity theft in addition to seeking to remedy it.

The FTC already regulates the data security practices of financial institutions under the Gramm-Leach-Bliley Act. This is crucial because some financial institutions may also provide identity services, including certain credit agencies.[289] However, these rules do not apply to

---

[286] Caroline Haskins, *Inside ID.me's Torrid Pandemic Growth Spurt, Which Led to Frantic Hiring, Ill-Equipped Staff, and Data-Security Lapses as Tte Company Closed Lucrative Deals With Unemployment Agencies and the IRS*, Bus. Insider (Jun. 7, 2022, 5:00 AM), https://www.businessinsider.com/id-me-customer-service-workers-hiring-secuirty-privacy-stress-data-2022-6. Jessy Edwards, *ID.me Lawsuit Claims Company Violates Data Storage Requirements*, Top Class Actions (Aug. 22, 2022), https://topclassactions.com/lawsuit-settlements/privacy/bipa/id-me-lawsuit-claims-company-violates-data-storage-requirements/.

[287] *Equifax Data Breach Settlement*, Federal Trade Commission (Sep. 2022), https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement.

[288] Cezary Podkul, *How Unemployment Insurance Fraud Exploded During the Pandemic*, ProPublica (July 26, 2021, 5:00 AM), https://www.propublica.org/article/how-unemployment-insurance-fraud-exploded-during-the-pandemic.

[289] *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches,* Federal Trade Commission (Oct. 27 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data.

non-financial vendors of identity verification. The FTC should consider how to expand these rules to include non-financial vendors of identity verification. An expansion of data security rules would be especially relevant for vendors that maintain a large database of personal information, such as some credit agencies and providers that offer 1:many biometric services.

Moreover, vendors of identity services may engage in deceptive claims that pose additional risks to data privacy (Q33). For example, when a vendor claims to only use 1:1 biometric matching but in fact uses 1:many matching, they mislead government agencies and users about the amount of data that they are collecting and retaining.[290] Because 1:many matching requires more data collection, it poses higher risks for data privacy and security. The FTC should prioritize investigating and punishing deceptive claims from private vendors of identity verification services.[291]

B. The FTC should reduce algorithmic bias in identity verification services

Secondly, biometric analysis for identity verification may be less accurate for individuals from some racial backgrounds.[292] That bias harms members of those groups because they face increased barriers in accessing government services that require biometrics as part of identity verification. For this reason, the General Services Administration (GSA) committed in January 2022 not to use facial recognition, from private companies or otherwise, for identity verification in government service delivery until facial recognition is sufficiently free of biases.[293] However, the GSA does not set rules for all government agencies considering using facial recognition from private companies. The GSA's new rule is limited to the products that it deploys (namely, Login.gov, the single sign-on authentication solution it provides to other federal, state, and local agencies). Furthermore, the GSA's rule is limited to facial recognition and does not address bias in other forms of biometrics, like voice recognition.[294] Other government agencies at every level may still use biometrics from private vendors, regardless of levels of bias, for identity verification.

---

[290] Kris Holt, *ID.me Says it Uses More Powerful Facial Recognition Than Previously Claimed*, Engadget (Jan. 26, 2022), https://www.engadget.com/idme-ceo-facial-recognition-one-to-many-backtrack-205046356.html.
[291] *Senators Urge FTC to Investigate ID.me's Facial Recognition Claims*, Electronic Privacy Information Center (May 19, 2022), https://epic.org/senators-urge-ftc-to-investigate-id-mes-facial-recognition-claims/.
[292] Nicol Turner Lee, *Mitigating Bias and Equity in Use of Facial Recognition Technology by the U.S. Customs and Border Protection*, Brookings Institution (July 27, 2022), https://www.brookings.edu/testimonies/mitigating-bias-and-equity-in-use-of-facial-recognition-technology-by-the-u-s-customs-and-border-protection/.
[293] *Executive Order 13985 – Equity Action Plan*, General Services Administration (Jan. 20, 2022), https://www.gsa.gov/cdnstatic/GSAEquityPlan_EO13985_2022.pdf.
[294] Claudia Lopez Lloreda, *Speech Recognition Tech Is Yet Another Example of Bias*, Scientific American (July 5, 2020), https://www.scientificamerican.com/article/speech-recognition-tech-is-yet-another-example-of-bias/.

Thus, as the FTC considers rulemaking for algorithmic bias more generally (Q68), it should follow the GSA's lead by considering the appropriate level of accuracy and fairness for biometrics to be used safely. One possible action for the FTC would be to establish rules that enshrine a particular standard for accuracy and fairness for all private vendors providing biometric verification to government services on the ground that use of services that fail to meet that standard would constitute an unfair practice.

Conclusion

As the data-driven and algorithmic practices discussed in our comments continue to proliferate, new protections are urgently needed to protect consumers' rights. The FTC has authority under section 5 to address these practices, and FTC rules can help fill enforcement gaps related to other existing protections. CDT appreciates the FTC's attention to these harms and urges the FTC to move forward with rulemaking that restricts companies from collecting, using, and sharing consumer data in exploitative and discriminatory ways. We look forward to supporting the FTC's work to advance data privacy rules that protect all consumers.