COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

Disrupting Data Abuse:
Protecting Consumers from Commercial Surveillance in the Online Ecosystem

Federal Trade Commission
Proposed Trade Regulation Rule on
Commercial Surveillance & Data Security
Commercial Surveillance ANPR, R111004

epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

NOVEMBER 2022

About EPIC

The Electronic Privacy Information Center (EPIC) is a 501(c)(3) non-profit public interest research and advocacy center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC advocates for privacy, algorithmic fairness, and government accountability. Learn more at epic.org.

Authors

Chris Baumohl, Law Fellow
Suzanne Bernstein, Law Fellow
Alan Butler, Executive Director
John Davisson, Senior Counsel
Caitriona Fitzgerald, Deputy Director
Grant Fergusson, Law Fellow
Christopher Frascella, Law Fellow
Sara Geoghegan, Counsel
Calli Schroeder, Global Privacy Counsel
Ben Winters, Counsel

With Special Thanks

EPIC is deeply grateful for the extensive drafting contributions to Section 3 (Discrimination) by Fordham University School of Law students Clara Abramson, James Garvey, Cameron Kasanzew, Chelsea Lim, Lauren Park, Katherine Pfingsten, and Carly Weisen, as well as the editing and organizational support of Catherine Powell, Professor of Law, Fordham University School of Law, and Ari Ezra Waldman, Professor of Law and Computer Science, Northeastern University School of Law.

Table of Contents

INTRODUCTION

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Federal Trade Commission's Advanced Notice of Proposed Rulemaking regarding a Trade Regulation Rule on Commercial Surveillance and Data Security. The unchecked spread of commercial surveillance over the last two decades has led to a data privacy crisis for consumers in the United States. Without any comprehensive privacy laws or regulations, abusive data practices have flourished. The ability to monitor, profile, and target consumers at a mass scale has created a persistent power imbalance that robs individuals of their autonomy and privacy, stifles competition, and undermines democratic systems. It is far past time to disrupt this data abuse, set rules of the road for our online ecosystem, and ensure that companies cannot extract private value from personal data in ways that undermine the public good.

Section 5 of the Federal Trade Commission Act provides that unfair and deceptive trade practices are unlawful and empowers the Commission to prevent and protect consumers from such practices. Under section 18 of the FTC Act, the Commission can issue a trade regulation rule defining those unfair and deceptive surveillance practices and establishing strong privacy and data security standards for all.

In these comments, EPIC provides an overview of the systems that facilitate commercial surveillance and the injuries they inflict on consumers. A business's collection, use, retention, or transfer of a consumer's personal information beyond what is reasonably necessary and proportionate to achieve the primary purpose for which it was collected (consistent with consumer expectations and the context in which the data was collected) is an unfair trade practice. These out-of-context secondary uses of data—including its sale to and use by data brokers, surveillance advertising firms, and other entities trafficking in consumer profiles—and the overcollection that feeds them are inconsistent with the reasonable expectations of online consumers. These unfair commercial surveillance practices lead to invasive, discriminatory targeting that violates the privacy and autonomy of consumers. EPIC argues that the FTC should establish a data minimization rule to ensure that

businesses only collect the data that they need to provide the goods and services that consumers request, and that they don't use or transfer data in ways that defy reasonable consumer expectations.

EPIC further argues that the Commission should issue a rule declaring it an unfair and deceptive practice to use an automated decision-making system without first demonstrating that it is effective, accurate, and free from impermissible bias. Commercial entities frequently use automated decision-making systems without substantiating the claims made about the systems, verifying their accuracy, or evaluating them for disparate impact. These automated systems—which can encompass a broad range of statistical or machine-learning tools that perform operations on data to aid or replace human decision-making—cause substantial injury to consumers when used without proper disclosure and oversight.

The Commission should also find that it is an unfair and deceptive practice to use an automated decision-making system implicating the interests of consumers without providing adequate notice of such use, including meaningful, readable, and understandable disclosure of the logic, factors, inputs, and training data on which the system relies. Companies should be required to publicly substantiate their claims about automated decision-making systems implicating the interests of consumers, articulate the purposes of those systems, evaluate the accuracy of those systems, and analyze potential disparate impacts of those systems.

The Commission should also categorically ban algorithmic systems that have been shown to cause serious and systemic harms. Specifically, systems that enable one-to-many facial recognition and systems that purport to provide "emotion recognition" capabilities have been shown to exacerbate biases and produce harmful outcomes. There is mounting evidence that such systems cannot be operated in a way that is fair to consumers or in a way that serves the public interest.

Throughout these comments, EPIC highlights the ways that commercial surveillance and algorithmic decision-making systems disproportionately harm marginalized communities. Targeting and profiling systems are designed to divide, segment, and score individuals based on their characteristics, their demographics, and their behaviors. In many cases, this means that consumers are sorted and scored

in ways that reflect and entrench systematic biases. EPIC believes the FTC should issue a rule that prohibits discrimination as an unfair trade practice.

In response to the Commission's questions regarding notice, transparency, and consent, EPIC argues that the agency should issue a rule declaring it an unfair and deceptive practice to collect, use, retain, or transfer personal data without first assessing, justifying, and providing adequate notice of such collection, use, retention, or transfer. EPIC further argues that the Commission should require businesses to promptly honor an individual's request to access all data the business maintains on them; to have such data corrected if it is in error; or to secure the deletion of all such data. EPIC notes, however, that even the most effective notice and transparency requirements cannot, by themselves, fully protect against the abuse of personal data. Commercial surveillance practices are simply too complex and numerous for even the most sophisticated consumer to understand. Transparency and user rights are only valuable in conjunction with substantive limits on data collection and use.

It is clear that children and teens require heightened protections when it comes to the collection and use of their personal data. Minors are uniquely vulnerable to profiling and the outputs of commercial surveillance systems, which are necessarily designed to suggest and shape preferences and beliefs. Therefore, the Commission should issue a rule declaring it an unfair practice to collect, process, retain, or transfer the personal data of minors under the age of 18 unless *strictly* necessary to achieve the minor's specific purpose for interacting with the business or to achieve certain essential purposes. The Commission should also ban targeted advertising to minors and issue a rule declaring it to be an unfair and deceptive practice for companies to make intentional design choices in order to facilitate the commercial surveillance of minors.

Data security and privacy go hand in hand. The Commission's rule should declare that a business's failure to implement reasonable security measures is an unfair trade practice, and that any entity which represents that it protects the security of consumer data but fails to adopt reasonable data security measures has engaged in a deceptive trade practice. Consumers are facing an epidemic of data breaches and resulting identity theft due to a lack of investment in and commitment

to data security. For over two decades, the FTC has tried to remedy the situation through case-by-case enforcement and the encouragement of industry self-regulation, but it is clear those approaches are not sufficient.

Lastly, the Commission should issue a rule affirming that is an unfair practice for a business to use manipulative design or dark patterns to nudge consumers to "accept" terms or options that broaden the scope of personal data that the business collects, uses, or discloses. Dark patterns are especially harmful in the data protection context. Companies have pushed for decades to frame data collection and processing as an issue of consumer "choice" while deploying manipulative choice architecture to ensure that consumers always "choose" to permit more data collection, broader uses of data, and loose or non-existent data sale and transfer restrictions. The Commission has already taken steps to crack down on manipulative design techniques and dark patterns and should take this opportunity to declare them an unfair trade practice.

INTEREST OF EPIC

By notice published on August 22, 2022, the Federal Trade Commission has requested comment on the prevalence of harmful commercial surveillance and data security practices in anticipation of a possible trade regulation rule addressing these subjects.[1] The Commission's advance notice of proposed rulemaking (ANPR) "invites comment on whether [the Commission] should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive."[2]

[1] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (advanced notice issued Aug. 22, 2022) [hereinafter ANPR].
[2] Press Release, FTC, *FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices* (Aug. 11, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

The Electronic Privacy Information Center submits these comments in support of the Commission's contemplated rulemaking and to share additional recommendations and expertise with the Commission. EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC has long defended the rights of consumers and has played a leading role in developing the Commission's authority to address emerging privacy and cybersecurity issues.[3] EPIC routinely files comments in response to proposed FTC rules and consent orders,[4] complaints concerning enforcement of Commission consent orders,[5] and complaints concerning business practices that violate privacy rights and otherwise harm consumers.[6]

EPIC has a particular interest in mitigating the harmful effects commercial surveillance and inadequate data security practices. EPIC believes that the Commission should promulgate a trade regulation rule that will promote data

---

[3] *See, e.g.*, Consumer Reps. & EPIC, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (2022), https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking/; EPIC, *What the FTC Could Be Doing (But Isn't) To Protect Privacy: The FTC's Unused Authorities* (2021), https://epic.org/privacy/consumer/EPIC-FTC-Unused-Authorities-Report-June2021.pdf.

[4] *See, e.g.*, EPIC, Comments on Proposed Consent Order, *In re Support King, LLC (SpyFone.com)*, FTC File No. 192-3003 (Oct. 8, 2021), https://archive.epic.org/apa/comments/In-re-SpyFone-Order-EPIC-comment-100821.pdf; EPIC et al., Comments on Proposed Consent Order, *In re Zoom Video Communications, Inc.* FTC File No. 192-3167 (Dec. 14, 2020), https://epic.org/apa/comments/EPIC-FTC-Zoom-Dec2020.pdf.

[5] Complaint for Injunctive Relief, *EPIC v. FTC*, No. 1:18-cv-00942 (Apr. 20, 2018), https://epic.org/wp-content/uploads/foia/ftc/facebook/EPIC-v-FTC-Complaint.pdf (concerning the Commission's failure to make a timely decision regarding EPIC's request for Facebook's assessments as required by the 2012 FTC Consent Order); *See EPIC v. FTC (Enforcement of the Google Consent Order)*, EPIC (2012), https://epic.org/documents/epic-v-ftc-enforcement-of-the-google-consent-order/.

[6] Complaint and Request for Investigation, Injunction, and Other Relief, *In re Online Test Proctoring Companies* (Dec. 9, 2020), https://epic.org/privacy/dccppa/online-test-proctoring/EPIC-complaint-in-re-online-test-proctoring-companies-12-09-20.pdf; Complaint and Request for Investigation, Injunction, and Other Relief *In re Airbnb* (Feb. 26, 2020), https://epic.org/privacy/ftc/airbnb/EPIC_FTC_Airbnb_Complaint_Feb2020.pdf; Complaint and Request for Investigation, Injunction, and Other Relief, *In re HireVue* (Nov. 6, 2019), https://epic.org/wp-content/uploads/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf [hereinafter EPIC HireVue Complaint]; EPIC, Comments on Proposed Consent Order, *In re Unrollme, Inc.*, FTC File No. 172-3139 (Sept. 19, 2019), https://epic.org/apa/comments/EPIC-FTC-Unrollme-Sept2019.pdf; Complaint, Request for Investigation, Injunction, and Other Relief, *In re Zoom Video Commc'ns, Inc.* (July 11, 2019), https://epic.org/privacy/ftc/zoomEPIC-FTC-Complaint-In-re-Zoom-7-19.pdf.

minimization;[7] establish fairness and transparency for automated decision-making systems;[8] address systemic discrimination online;[9] ensure that businesses meet their notice and transparency obligations;[10] protect the privacy of minors;[11] enforce data security standards;[12] and prohibit manipulative designs that thwart consumer choice ("dark patterns").[13]

EPIC,[14] alongside other consumer protection and civil rights organizations,[15] has previously urged the Commission to undertake a trade regulation rulemaking that would define unfair and deceptive commercial data practices and unlock the FTC's dormant enforcement power. EPIC is heartened to see the Commission considering such a rule now, and we are eager to work with the FTC to ensure that this process yields the strongest possible privacy and civil rights protections for consumers.

---

[7] Consumer Reps. & EPIC, *supra* note 3.
[8] EPIC, *In re Petition for Rulemaking Concerning Use of Artificial Intelligence in Commerce* (Feb. 3, 2020), https://epic.org/wp-content/uploads/privacy/ftc/ai/EPIC-FTC-AI-Petition.pdf [hereinafter EPIC FTC AI Petition].
[9] EPIC HireVue Complaint, *supra* note 6; *see* Press Release, EPIC, *EPIC Urges DC Council to Pass Algorithmic Discrimination Bill* (Sept. 23, 2022), https://epic.org/epic-urges-dc-council-to-pass-algorithmic-discrimination-bill/.
[10] EPIC, Comments on Notice of Proposed Rulemaking, *In re Empowering Broadband Consumers Through Transparency*, CG Docket No. 22-2 (Mar. 9, 2022), https://epic.org/documents/in-the-matter-of-empowering-broadband-consumers-through-transparency/.
[11] Letter from EPIC to U.S. Senate Committee on Commerce, Science, and Transportation (July 26, 2022), https://epic.org/wp-content/uploads/2022/07/EPIC-SCOM-privacy-July2022.pdf (concerning the Kids Online Safety Act).
[12] EPIC, Comments on Notice of Proposed Supplemental Rulemaking, *In re Standards for Safeguarding Customer Information ("Safeguards Rule")*, 86 Fed. Reg. 70,062 (Feb. 7, 2022), https://epic.org/wp-content/uploads/2022/02/EPIC-FTC-Safeguards-Reporting-EPIC-comments-22-02-07.pdf; EPIC, Comments on Proposed Consent Order, *In re CafePress*, File No.1923209 (Apr. 21, 2022), https://epic.org/wp-content/uploads/2022/04/EPIC-comments-in-re-cafepress.pdf.
[13] Letter from EPIC et al. to FTC (June 30, 2022), https://www.documentcloud.org/documents/22075421-tacd-ftc-google-account-letter.
[14] EPIC FTC AI Petition, *supra* note 8; EPIC, *supra* note 3.
[15] Consumer Reps. & EPIC, *supra* note 3; Letter from Access Now et al., to Lina M. Khan, Chair, FTC (Oct. 27, 2021), https://www.freepress.net/sites/default/files/2021-10/Letter-to-FTC-on-Privacy-Rulemaking-10-27-2021.pdf.

THE FTC AND THE DATA PROTECTION CRISIS

The United States faces a data privacy crisis. The lack of comprehensive privacy laws and regulations has allowed abusive data practices to flourish, creating a persistent power imbalance that threatens both individual rights and competition. Due to the failure of policymakers in the U.S. to establish adequate data protection standards, online firms have been allowed to deploy commercial surveillance systems that collect and commodify every bit of our personal data.[16] The platforms and data brokers that track us across the internet and build detailed profiles to target us with ads also expose us to ever-increasing risk of breaches, data misuse, manipulation, and discrimination.[17] The impacts of these commercial surveillance systems are especially acute for marginalized communities, where they foster discrimination and inequities in employment, government services, healthcare, education, and other life necessities.[18]

The notice and choice approach that has dominated the United States' response to this uncontrolled data collection over the last several decades simply does not work. The focus on notice has led to longer and more complicated privacy policies that users do not read and could not change even if they did. And modern surveillance systems, including the schemes used to track our digital and physical activities across the web and across devices, are too complex and opaque for the vast majority of internet users to understand or control. Robust data protection standards

---

[16] *See generally* Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (2019).

[17] *See Factsheet: Surveillance Advertising: How Does the Tracking Work?*, Consumer Fed. of America (Aug. 26, 2021), https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-how-tracking-works/.

[18] *See* Anita Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 131 Yale L.J.F. 907, 913-28 (Feb. 20, 2022), https://www.yalelawjournal.org/forum/dismantling-the-black-opticon; Safiya Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (2018); *Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security: Hearing before the Subcomm. Consumer Prot. of the H. Comm. on Energy & Com.*, 117th Cong. (2022) (testimony of David Brody), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony_Brody_CPC_2022.06.14.pdf [hereinafter David Brody Testimony]; Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U.L. Rev. Online 793, 855–59 (2021), https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf (discussing discrimination harm as a privacy harm).

are essential to restore the balance of power between individuals and technology companies and to ensure the preservation of our privacy and civil rights.

In the absence of a comprehensive privacy law or dedicated privacy regulator in the U.S., the task of safeguarding personal data has been divided among federal and state entities. For general online privacy enforcement, that responsibility has fallen chiefly to the Federal Trade Commission. The FTC was established in 1914 to prevent unfair methods of competition in commerce.[19] In 1938, Congress expanded the Commission's mandate to include a broad prohibition against unfair and deceptive acts or practices, and the FTC has since been charged with enforcing a variety of consumer protection laws.[20] The Commission's overarching mission is to "[p]rotect[] consumers and competition by preventing anticompetitive, deceptive, and unfair business practices through law enforcement, advocacy, and education without unduly burdening legitimate business activity."[21] The Commission is tasked with using these broad and flexible authorities to address emerging and evolving injuries.

Though some statutes enforced by the Commission authorize the FTC to impose civil penalties for first-time violations, the FTC Act generally does not. But trade regulation rules present a notable exception. If the Commission were to promulgate a commercial surveillance and data security rule, the FTC would be empowered to pursue civil penalties against violators without having to bring each company under a consent decree first.[22]

The Commission has considerable rulemaking authority.[23] The most notable example of this authority is section 18 of the FTC Act, which authorizes the Commission to promulgate trade regulation rules "defin[ing] with specificity . . . unfair or deceptive acts or practices in or affecting commerce" (a procedure commonly known as Magnuson-Moss rulemaking).[24] The statute requires that the

[19] *About the FTC*, FTC, https://www.ftc.gov/about-ftc (last visited Nov. 20, 2022).
[20] *A Brief Overview of the Federal Trade Comm'n's Investigative, Law Enforcement, and Rulemaking Authority*, FTC (Oct. 2019), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [hereinafter FTC Authority Overview].
[21] *Mission*, FTC, https://www.ftc.gov/about-ftc/mission (last visited Nov. 21, 2022).19
[22] 15 U.S.C. § 45(m)(1)(A).
[23] *See* Consumer Reps. & EPIC, *supra* note 3, at 4–5.
[24] 15 U.S.C. § 57a; *see also* FTC Authority Overview, *supra* note 20.

Commission have reason to believe the practices addressed by the rulemaking are "prevalent"[25] and provides for a hearing with an opportunity for cross-examination, among other steps.[26] After the Commission has established a trade regulation rule, any party who violates the rule "with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule" is liable for civil penalties for each violation.[27] Further, any party who violates a rule, regardless of their state of knowledge, may be held liable for consumer injuries caused by the violation.[28]

This rulemaking authority is key to protecting consumers from unfair and deceptive practices. Rulemaking is also important for businesses, as the process gives market participants clear guidance about what constitutes an unfair or deceptive data practice.[29]

The Commission has taken some steps to protect privacy over the past two decades, but the Commission's enforcement and regulatory strategies have been critically flawed. Too often, the FTC has neglected to use the authority Congress has already given it. The Commission's repeated failure to take meaningful enforcement action and to block harmful mergers has allowed abusive data practices by Facebook, Google, and other industry giants to flourish. Some statutory authorities, including the FTC's power to promulgate trade rules, have simply never been used to advance the Commission's data protection mission.

Beginning in 1951 and running through a "series of cases in the 1970s, [the Commission] recognized the general consumer preference against commercialization of personal data."[30] In the mid-1990s, the Commission took an interest in the emerging issue of online privacy and held a series of workshops that led, in part, to the passage of the Children's Online Privacy Protection Act (COPPA); the issuance of reports critical of the data practices of early internet companies; and

[25] 15 U.S.C. § 57a(b)(3).
[26] 15 U.S.C. § 57b; 5 U.S.C. § 57c(2)(B).
[27] 15 U.S.C. § 45(m)(1)(A).
[28] FTC Authority Overview, *supra* note 20.
[29] *See Rules*, FTC, https://www.ftc.gov/enforcement/rules (last visited Nov. 20, 2022).
[30] Chris Jay Hoofnagle et al., *The FTC Can Rise to the Privacy Challenge, but Not Without Help From Congress*, Lawfare (Aug. 9, 2019), https://www.lawfareblog.com/ftc-can-rise-privacy-challenge-not-without-help-congress.

calls for additional regulatory authority. In 1998, the Commission brought its first internet-related privacy case.[31] Unfortunately, the Commission's early data protection work led to a framing of privacy law in the United States as being a matter of "notice and choice" and deference to industry-backed "self-regulation."[32] Both notice and choice and self-regulation have failed to meaningfully protect consumer privacy online. These approaches have helped produce a "privacy paradox," wherein consumers say they want online privacy but behave differently because the information ecosystem is so complicated and cumbersome that is impossible to access online services without exposing personal information.[33] Notice and choice mechanisms are particularly ineffective, as consumer privacy increasingly involves surveillance platforms and third parties. "When monitoring is built into services and presented as necessary for the provision of the service, it constrains the relevance and utility of the notice-and-choice regime."[34] Moreover, notice and choice completely fails to address the threat from data brokers and other third parties that have no direct interaction with the consumer.[35]

Although the Commission has gradually embraced its role as a regulator of commercial data practices, the FTC's impact has been regrettably limited. In the 2000s, the Commission began to expand the scope of its privacy investigations and eventually formed a Division of Privacy and Identity Protection within the Bureau of Consumer Protection. But the Commission's enforcement actions did not lead to substantial changes in business practices or sufficient monetary penalties, and it became clear that companies under consent decrees would have no incentive to protect consumer data if they did not expect real consequences for violating those decrees. The Commission's failure to take meaningful action to curb privacy violations has come at great cost to American consumers and businesses.

There are signs that the Commission is beginning to take its role as a privacy regulator more seriously, as the agency takes steps to improve the

[31] *In re GeoCities*, FTC File No. 982-3015 (1998).
[32] EPIC, *supra* note 3, at 1.
[33] *See* Chris Jay Hoofnagle, *Federal Trade Commission Privacy Law and Policy* 169 (2016).
[34] *Id.* at 333.
[35] *Id.* at 173.

effectiveness of its consumer privacy enforcement. As Chair Khan stated in a speech earlier this year:

> Going forward, I believe we should approach data privacy and security protections by considering substantive limits rather than just procedural protections, which tend to create process requirements while sidestepping more fundamental questions about whether certain types of data collection and processing should be permitted in the first place.[36]

This shift builds on years of work by Commissioners Slaughter and Wilson, as well as former Commissioner Chopra, to focus the FTC's attention on privacy and to ensure changes to harmful data practices.[37] The Commission has begun to impose new remedies in its enforcement actions, including algorithmic disgorgement requirements that prevent companies from benefitting from illegally obtained data.[38] The Commission has also started holding executives directly accountable when appropriate,[39] as well as requiring companies to minimize the amount of data they collect and retain.[40] These remedies mark a critical shift in the Commission's privacy enforcement and reflect a recognition that modest monetary settlements are not enough to safeguard consumer privacy—particularly where the largest tech giants are concerned.

---

[36] Lina M. Khan, Chair, FTC, Remarks of Chair Lina M. Khan As Prepared for Delivery at the IAPP Global Privacy Summit 2022 (Apr. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks%20of%20Chair%20Lina%20M.%20Khan%20at%20IAPP%20Global%20Privacy%20Summit%202022%20-%20Final%20Version.pdf.

[37] *See, e.g.*, Rebecca Kelly Slaughter, Comm'r, FTC, *The Near Future of U.S. Privacy Law* (Sept. 6, 2019), https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf; Christine Wilson, Comm'r, FTC, *A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation* (Feb. 6, 2020), https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf; Rohit Chopra, Former Comm'r, FTC, Statement of Comm'r Rohit Chopra Regarding the Report to Congress on the FTC's Use of Its Authorities to Protect Consumer Privacy and Security (June 17, 2020), https://www.ftc.gov/system/files/documents/public_statements/1577067/p065404dpipchoprastatement.pdf.

[38] *See, e.g.*, *In re Everalbum, Inc.*, FTC File No. 192-3172 (2021).

[39] *In re Drizly, LLC*, FTC File No. 202-3185 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Complaint.pdf (naming CEO James Cory Rellas in complaint).

[40] *In re Residual Pumpkin Entity, LLC, formally d/b/a Cafepress*, FTC File No. 192-3209 (2022).

Rules that define unfair and deceptive commercial data practices will enhance the Commission's ability to protect privacy online. A commercial surveillance and data security rule would provide clear notice to companies of their obligations with respect to personal data and level the playing field by requiring all companies to play by the same rules. Critically, it would also unlock the full potential of first-time civil penalties, giving companies a strong financial incentive to comply, deterring harmful commercial surveillance practices, promoting the development of privacy enhancing techniques, and protecting individual privacy.

THE FTC'S AUTHORITY

Section 5 of the Federal Trade Commission Act provides that unfair and deceptive trade practices are unlawful and empowers the Commission to prevent and protect consumers from those unfair and deceptive practices.[41] "[Section 5] cannot be defined in terms of constants. More broadly, it is a recognition of an ever-evolving commercial dexterity and the personal impact of economic power as important dimensions of trade. Its underlying proposition is that a free competitive society must have some means of preventing that very freedom to compete from destroying our economic system."[42] It is under this authority that the Commission published its Advance Notice of Proposed Rulemaking, which opens the door to a trade regulation rule addressing unfair and deceptive commercial surveillance practices.[43]

Unfair and Deceptive Trade Practices

An unfair practice "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."[44] The FTC has generally

[41] 15 U.S.C. § 45(a).
[42] Hoofnagle, *supra* note 33, at 120.
[43] ANPR, *supra* note 1; 15 U.S.C. § 57a(b)(3).
[44] 15 U.S.C. § 45(n).

used this authority to maintain the "free exercise of consumer decision-making."[45] In the 1980s, the FTC clarified in a policy statement that it would use its unfairness authority to stop commercial practices that (1) cause substantial injury, (2) are not outweighed by any countervailing benefits to consumers or competition, and (3) consumers cannot reasonably avoid.[46] In 1993, Congress incorporated aspects of the FTC's unfairness policy statement into the FTC Act.[47] Notably, Congress decided that "[i]n determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence."[48] However, Congress did not adopt the Commission's more restrictive rubric in the 1980 policy statement for determining which harms constitute "substantial injury."

Substantial Injury

Courts typically defer to the Commission's findings and guidance on the substantial injury prong of the unfairness standard. Courts have upheld the Commission's determination that a practice can cause substantial injury by doing "a small harm to a large number of people" or by raising "a significant risk of concrete harm."[49] Moreover, a substantial injury can result when consumers are "injured by a practice for which they did not bargain."[50] In other words, a trade practice may cause substantial injury if it effectively thwarts a consumer's ability to make a decision. Unfair trade practices may be caused by or involve multiple entities,

---

[45] FTC, *Policy Statement on Unfairness* (1980), https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness [hereinafter FTC Unfairness Statement]; *see* Calli Schroeder & Cobun Keegan, *Unpacking Unfairness: The FTC's Evolving Measures of Privacy Harms*, 15 J. L. Econ. & Pol'y 1, 27 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4204208.

[46] *Id.*

[47] 15 U.S.C. § 45(n).

[48] *Id.*

[49] *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 972 (D.C. Cir. 1985).

[50] *FTC v. Windward Mktg. Inc.*, 1997 WL 33642380, at *11 (N.D. Ga. Sept. 30, 1997) (citing *Orkin Exterminating Co., Inc. v. FTC*, 849 F.2d 1354, 1364–65 (11th Cir. 1988)). The FTC brings these types of cases "not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decision making." Citron & Solove, *supra* note 18, at 848.

including platforms or facilitators, whose actions together inflict substantial injury.[51] The Commission "is not required to show intent, merely that customers were substantially injured."[52]

A wide range of harms can constitute substantial injuries, including intangible harms, economic harms, and non-economic harms that are otherwise quantifiable.[53] A substantial injury often entails economic or monetary harms to consumers. For example, the Commission has found that billing customers without a mechanism for consent,[54] debiting consumers' accounts without authorization,[55] and charging erroneous or unexpected fees cause substantial injury.[56] In *FTC v. Neovi*, the Ninth Circuit held that the FTC met its burden to establish substantial injury where a business's "profound lack of diligence" enabled fraud on its platform.[57]

Reputational and economic harms also constitute substantial injuries where the unfair practice exposes consumers to "embarrassment and risk of adverse action, such as job loss."[58] In *FTC v. LoanPointe*, a substantial injury was caused not by the wage assignment clause in a payday loan, but by the lender's practice of "disclosing debts and the amount of the debts to consumers' employer[s]" without prior approval from the consumers.[59] While the economic harms from this breach of privacy spanned from job loss to a disruption of personal finances, the reputational

---

[51] *FTC v. Inc21.com Corp.*, 745 F. Supp. 2d 975, 1003 (N.D. Cal. 2010) ("It is not a bar to liability if a violation is caused by more than one perpetrator. Rather, liability under the Act may be found if a business facilitated or provided substantial assistance to a deceptive scheme resulting in substantial injury to customers.").
[52] *FTC v. Fleetcor Techs., Inc.*, 2022 WL 3273286, at *29 (N.D. Ga. Aug. 9, 2022) (citing *Orkin Exterminating Co.*, 849 F.2d at 1364–65).
[53] *See In re DesignerWare, LLC*, FTC File No. 1123151 (Apr. 25, 2013) (unfair practice to install monitoring software on rented computers to potentially gather sensitive personal information from consumers).
[54] *FTC v. Amazon.com, Inc.*, 2016 WL 10654030, at *8 (W.D. Wash. July 22, 2016).
[55] *Windward*, 1997 WL 33642380, at *15–16.
[56] *Fleetcor*, 2022 WL 3273286, at *28.
[57] *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1153 (9th Cir. 2010).
[58] *FTC v. LoanPointe, LLC*, 2011 WL 4348304, at *3 (D. Utah Sept. 16, 2011).
[59] *Id.* at *6 ("The Circuit Court for the District of Columbia has noted that the FTC "found wage assignments particularly harmful to consumers because they can be invoked without the due process safeguards of a hearing and opportunity to present defenses.") (citing *Am. Fin. Servs. Ass'n v. FTC,* 767 F.2d at 974).

harms to consumers also contributed to establishing substantial injury.[60] Courts at common law have long recognized that intangible injuries, including those protected by privacy torts, can support an award of damages.[61] Many privacy statutes have simplified this process by assigning a default or minimum damages value.[62]

Modern commercial surveillance practices, defined in the ANPR as "the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information,"[63] produce harms that constitute substantial injury. In addition to economic harms, consumer surveillance can work non-economic harms sufficient for a finding of unfairness. For example, many privacy unfairness cases "involve consumer data that was actually sold for value or sensitive data that was shared with third parties."[64] Where these harms are not strictly economic, their impact can still be measured "based on (1) the sensitivity of the data, (2) the lack of a direct relationship with consumers, (3) consumers' lack of knowledge of and of agency over the sharing."[65] The Commission has recognized in prior privacy enforcement actions that both financial and non-financial harms can constitute substantial injury.[66]

The Commission's reluctance to pursue a wider range of unfairness cases is attributable, in part, to its excessively narrow construction of "substantial injury" in the 1980 policy statement. The Commission is not bound by the limitations of that statement, and it should not feel compelled to follow them. Even under the 1980 policy statement, the Commission can act to prevent non-economic harms. Yet the statement's categorial exclusion of "emotional" and "subjective" harms impermissibly and artificially narrows the meaning of "substantial injury" and may

---

[60] *FTC v. LoanPointe, LLC*, 525 F. App'x 696, 701 (10th Cir. 2013).
[61] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 Tex. L. Rev. 737, 769–73 (2018) ("The privacy torts readily allow for emotional distress damages alone.").
[62] *See, e.g.*, Federal Wiretap Act, 18 U.S.C. § 2520.
[63] ANPR, *supra* note 1, at 51277.
[64] Schroeder & Keegan, *supra* note 45, at 32.
[65] *Id.*
[66] *Id.* at 31–38 (injuries include unauthorized sale of data, unauthorized data sharing, unfair collection of data, breach of consumer privacy expectations, high risk of emotional and reputational injury from sexual privacy exposure).

exclude a wide range of privacy and data-driven harms caused by modern commercial surveillance practices.[67]

Instead, the Commission should understand the term "substantial injury" to describe any nontrivial harm, setback, loss, risk to health or safety, or other impairment to well-being, whether discrete or cumulative, that affects one or more individuals. This definition is consistent with the plain meaning of "substantial injury"; incorporates a wider range of non-economic and intangible (yet real) harms, including many recognized at common law; allows that multiple small injuries can add up to a substantial one; and emphasizes that a substantial injury can be suffered both by individuals and groups of individuals. It is well within the Commission's authority to broadly define the scope of substantial injury under the unfairness authority, as "Congress delegated broad discretionary authority to the [FTC] to define unfair trade practices on a flexible, incremental basis."[68]

The harms of commercial surveillance have a substantial impact in part because these practices affect every person who uses the internet and connected services. "Many privacy violations involve broken promises or thwarted expectations about how people's data will be collected, used, and disclosed."[69] Some of these harms "may appear small when viewed in isolation, such as the inconvenience of receiving an unwanted email or advertisement or the failure to honor people's expectations that their data will not be shared with third parties. But when done by hundreds or thousands of companies, the harms add up. Moreover, these harms are dispersed among millions—and sometimes billions—of people and can be hard to combat absent the Commission's intervention; the overall societal

[67] *See generally* Info. Comm'r's Off., *Overview of Data Protection Harms and the ICO's Taxonomy* (2022), https://ico.org.uk/media/about-the-ico/documents/4020144/overview-of-data-protection-harms-and-the-ico-taxonomy-v1-202204.pdf (UK ICO's broad framework, evidence, and taxonomy of data protection harms) [hereinafter ICO].
[68] Consumer Reps. & EPIC, *supra* note 3, at 11.
[69] Citron & Solove, *supra* note 18, at 797 (citing Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. Rev. 477, 508 (2010) (noting "the greatest harms in the present age often come from unauthorized uses of private information online" including the improper collection, aggregation, processing, and dissemination of information)).

impact is significant."[70] The extent of these harms can depend on "how the data is used, what data is involved, and how the data might be combined with other data. Sharing an innocuous piece of data with another company might provide a key link to other data or allow for certain inferences to be made."[71] Privacy violations can cause psychological harms, relationship harms, discrimination harms, and autonomy harms, including lack of control and chilling effects.[72]

The Commission's understanding of substantial injury should encompass harms that consumers suffer as a result of commercial surveillance. The Commission's unfairness authority is well suited to these types of privacy and data security violations "because incremental injuries that affect many people can be substantial and because their negative impacts can materialize over time[.]"[73]

Not Reasonably Avoidable

Another prong of the unfairness test considers whether consumers can reasonably avoid the harms caused by business practices. It is clear that consumers cannot reasonably avoid the substantial injuries caused by widespread commercial surveillance, which routinely occurs without their knowledge and in ways that are too convoluted for even the most determined consumer to understand. In the same way that the "substantial injury" prong assesses whether a consumer has been "injured by a practice for which they did not bargain,"[74] the "reasonably avoidable"

---

[70] *Id.* at 797 (citing Brian Fung, *T-Mobile Says Data Breach Affects More than 40 Million People*, CNN Bus. (Aug. 18, 2021), https://www.cnn.com/2021/08/18/tech/t-mobile-data- breach/index.html [https://perma.cc/L6XV-6PUN] (reporting that one data breach "affect[ed] as many as 7.8 million postpaid subscribers, 850,000 prepaid customers and 'just over' 40 million past or prospective customers who have applied for credit with T-Mobile")).

[71] *Id.* at 818.

[72] *See generally* Citron & Solove, *supra* note 18, at 841–59 (expanding on typology of privacy harms).

[73] Consumer Reps. & EPIC, *supra* note 3, at 13.

[74] *Windward*, 1997 WL 33642380, at *11 (citing *Orkin Exterminating Co.*, 849 F.2d at 1364–65). The FTC brings these types of cases "not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decision making." Citron & Solove, *supra* note 18, at 848.

prong examines the relative bargaining power of the consumer and the seller and the consumer's freedom of choice.[75]

The 1980 policy statement asks whether the consumer could have reasonably avoided the injury in a broader context of a self-correcting marketplace. But a focus on consumer choice only works if individuals have meaningful decisions to make that can impact the harmful business practices at issue.[76] When the Commission brings an unfairness claim, it is typically because a commercial pattern or practice has hindered the nominally free-market decision-making power of consumers. Examples in the 1980 policy statement include leaving buyers with insufficient information for informed choices, overt coercion, and exercising undue influence over susceptible purchasers. The Commission's unfairness actions are brought "not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decision making."[77]

Courts have identified two different paradigms that satisfy the "not reasonably avoidable" element: cases in which market forces left consumers without a reasonable choice, and cases in which consumers could not have anticipated or avoided the harm. As to the first category, the D.C. Circuit has explained that "the requirement that the injury cannot be reasonably avoided by the consumers stems from the Commission's general reliance on free and informed consumer choice as the best regulator of the market."[78] The Commission has intervened where a business has either affirmatively distorted consumers' choices or has taken advantage of an existing obstacle to free consumer choice.[79] Similarly, harm is unavoidable where there is a faulty assumption that the consumers had a choice.[80]

---

[75] *See* ICO, *supra* note 67, at 6 ("economic circumstances such as market power or barriers to switching can mean that harms are hard to avoid even if informed and unbiased consumers are unable to discipline providers by switching to alternatives.").
[76] FTC Unfairness Statement, *supra* note 45.
[77] *Id.*
[78] *Am. Fin. Servs. Ass'n*, 767 F.2d at 976.
[79] *Id.* at 981.
[80] *Pa. Funeral Dirs. Ass'n, Inc. v. FTC*, 41 F.3d 81, 91 (3d Cir. 1994).

The Third Circuit has held that a consumer does not truly have the ability to exercise their choice if they are *forced* to make a certain choice or pay a fee.[81]

In the second category of cases, courts have looked at whether consumers could have anticipated the harm of a commercial practice at all. Consumers may avoid injury before it occurs if they anticipate the harm.[82] However, where consumers have no reason to anticipate the harm, as with fraud, "there [i]s no occasion for the consumers even to consider taking steps to avoid it."[83] This happens commonly, though not only, when unfair practices dovetail with deceptive practices. For example, in *FTC v. Wyndham*, consumers could not have reasonably avoided harm from the hotel chain's poor security practices where the privacy policy overstated the efficacy of those practices.[84] Finally, consumers cannot reasonably avoid harms caused by practices that they never actually consented to, like unauthorized charges.[85]

In the context of commercial surveillance, the average consumer does not have the knowledge, understanding, or ability to avoid invasive and harmful data collection; the average consumer does not choose to be subject to commercial surveillance online. There is a fundamental power imbalance between consumers and the entities that design and operate online services to maximize the collection and extraction of their data for targeting, profiling, and other harmful uses.[86] Data collection methods and data flows are so opaque that it is not reasonable to expect an average consumer to understand how their data is being used (or even when it is being collected in many cases).[87] This relationship reflects an asymmetry of information—a fundamental power imbalance between consumers and the online

---

[81] *Id.* at 92–93.
[82] *FTC v. IFC Credit Corp.*, 543 F. Supp. 2d 925, 941 (N.D. Ill. 2008).
[83] *Orkin Exterminating Co.*, 849 F.2d at 1365.
[84] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 245–46 (3d Cir. 2015).
[85] *Inc21.com*, 745 F. Supp. 2d at 1004–05.
[86] Roomy Khan, *Google, Facebook and Others: Are They Offering Enough For Using the Consumer Created Content?*, Forbes (May 3, 2018), https://www.forbes.com/sites/roomykhan/2018/05/03/google-facebook-and-others-are-they-offering-enough-for-using-the-consumer-created-content/?sh=6aecc86c76c9.
[87] *See, e.g.*, Surya Mattu et al., *How We Built A Meta Pixel Inspector*, Markup (Apr. 28, 2022), https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector (study on Meta Pixel).

platforms that collect and process their personal data.[88] It is understood in other contexts that power imbalances can lead to unavoidable injury. For example, patients are not expected to avoid harms caused by a proposed course of medication or treatment.

The Commission has made clear that for a consumer to have the ability to reasonably avoid harm, they must be able to anticipate it. But in the online ecosystem, the average consumer is only aware of the direct interactions they have with businesses, such as browsing a website, using a mobile app, or posting on social media. They are typically not aware of, and have little control over, how their data is collected or what happens to it in the background.

The Meaning of 'Consumer'

The FTC rightly acknowledges in the ANPR that the term "consumer" is an expansive one.[89] The ANPR defines consumers to include businesses and workers, "not just individuals who buy or exchange data for retail goods and services."[90] Courts have also acknowledged the FTC's authority to interpret the term "consumer" broadly. "The text and the legislative history of the 1994 Amendment to the FTCA demonstrate that Congress's intent was to limit the Commission's authority to proscribe *unfair* acts and practices *not* through a restrictive definition of 'consumer,' but rather through subsection (n)'s requirement that an unfair practice must cause substantial harm that is not reasonably avoidable or outweighed by countervailing benefits to consumers or competition."[91] Notably, the term consumer should be understood to describe a *reasonable* consumer—not a superuser or

[88] Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. Info. Tech. 83 (2015) ("[U]sers have few meaningful options for privacy self-management[.] These asymmetries in knowledge are sustained by asymmetries of power.").
[89] ANPR, *supra* note 1, at 51277.
[90] *Id.* ("This approach is consistent with the Commission's longstanding practice of bringing enforcement actions against firms that harm companies as well as workers of all kinds."). *See generally Orkin Exterminating Co.*, 849 F.2d at 1364–65 (companies as consumers); Press Release, FTC, *FTC Settles Charges Against Two Companies That Allegedly Failed to Protect Sensitive Employee Data* (May 3, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/05/ftc-settles-charges-against-two-companies-allegedly-failed-protect-sensitive-employee-data (employees as consumers).
[91] *IFC Credit Corp.*, 543 F. Supp. 2d at 941.

otherwise exceptional consumer—as "the sophistication of the [consumer] is not a factor in determining the applicability of the Act."[92]

Not Outweighed by Countervailing Benefits

Once the Commission determines that a business practice causes substantial injury, it must consider whether that harm is outweighed by countervailing benefits to consumers or competition.[93] A practice is unfair if it is"injurious in its net effects."[94] The FTC must "assure that consumers will not ultimately be worse off after the Commission acts."[95]

Invasive commercial surveillance practices routinely cause substantial injury that is not outweighed by benefits to consumers or competition. One of the principles broadly recognized in global privacy frameworks is that the processing of personal data should be limited to the minimum amount necessary and proportionate to the specific purposes for which it was collected (the data minimization principle).[96] An unfairness rule prohibiting commercial surveillance practices that violate the data minimization principle will satisfy the countervailing benefits test because those surveillance practices infringe on consumers' privacy in a way that is not proportionate to the benefit they provide to the public. Indeed, many commercial surveillance practices have been shown to provide no benefit to consumers at all.

To take one notable example, targeted advertising routinely fails to benefit consumers or competition. Consumers enjoy few benefits because the ads targeted at them are rarely relevant.[97] Targeted advertising can also hurt advertisers

---

[92] *Id.* at 936.
[93] J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, FTC (May 30, 2003), https://www.ftc.gov/news-events/news/speeches/ftcs-use-unfairness-authority-its-rise-fall-resurrection (internal citations omitted).
[94] FTC Unfairness Statement, *supra* note 45.
[95] Beales, *supra* note 93.
[96] *See, e.g.*, Org. of Am. States, *Updated Principles on Privacy and Data Protection* 37 (2022), https://www.oas.org/en/sla/iajc/docs/Publication_Updated_Principles_on_Privacy_and_Protection_of_Personal_Data_2021.pdf.
[97] Dr. Augustine Fou, *Why Is Ad Tech Targeting So Bad?*, Forbes (May 5, 2021), https://www.forbes.com/sites/augustinefou/2021/05/05/why-is-ad-tech-targeting-so-bad/?sh=458b2dbe7212; *How many relevant ads do we see each day?*, Adalytics, https://adalytics.io/blog/how-many-relevant-ads-do-we-see-each-day (last visited Nov. 21, 2022).

themselves, as it tends to be much less effective than companies anticipate.[98] Moreover, targeted advertising has isolating and divisive social impacts.[99] There are better, less privacy invasive ways to serve digital advertisements. "'The seduction of these consumer products is so powerful that it blinds us to the possibility that there is another way to get the benefits of the technology without the invasion of privacy. But there is[.]"[100] Contextual advertising provides largely the same benefits of traditional advertising without the privacy harms inherent in commercial surveillance.[101]

Surveillance-based targeting and profiling systems also harm competition because they concentrate power in the hands of a small number of firms with access to the bulk of the data used for targeting. It is both "foundationally and cyclically anticompetitive: It allows dominant firms to continuously extract more data and profit from trapped used, while raising barriers to entry that serve to further deprive those users of viable alternatives."[102] Privacy protective measures that distribute market power are beneficial to competition and improve data-driven markets.[103]

---

[98] Shoshana Wodinsky, *Facebook Knowingly Profited Off Junk Ad Efficacy Estimates, Lawsuit Claims*, Gizmodo (Feb. 18, 2021), https://gizmodo.com/facebook-knowingly-profited-off-junk-ad-efficacy-estima-1846297561; Matt Shipman et al., *New Study Reveals Why Facebook Ads Can Miss Target*, NC State University (Mar. 28, 2022), https://news.ncsu.edu/2022/03/new-study-reveals-why-facebook-ads-can-miss-target/.

[99] Silvia Milano et al., *Targeted Ads Isolate and Divide Us Even When They're Not Political – New Research*, The Conversation (July 13, 2021), https://theconversation.com/targeted-ads-isolate-and-divide-us-even-when-theyre-not-political-new-research-163669.

[100] 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; *see also* Shoshana Zuboff, *You Are Now Remotely Controlled*, N.Y. Times (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html.

[101] Beware of Contextual Advertising 2.0, which uses A.I. and machine learning to serve contextual advertisements. *See* Jeff Chester, *Contextual Advertising – Now Driven by AI and Machine Learning Requires Regulatory Review for Privacy and Marketing Fairness*, Ctr. Dig. Democracy (Mar. 11, 2021), https://www.democraticmedia.org/article/contextual-advertising-now-driven-ai-and-machine-learning-requires-regulatory-review-privacy.

[102] Accountable Tech, *Petition for Rulemaking to Prohibit Surveillance Advertising* 20 (Sept. 28, 2021), https://accountabletech.org/wp-content/uploads/Rulemaking-Petition-to-Prohibit-Surveillance-Advertising.pdf.

[103] Robin Berjon, *Competition & Privacy: It's Both or Nothing*, Robin Berjon (Dec. 13, 2021), https://berjon.com/competition-privacy/.

Deceptive Trade Practices

In addition to its unfairness authority, the Commission also has the authority to prohibit deceptive trade practices. Deception includes a "representation, omission or practices that is likely to mislead the consumer."[104] Under the FTC's 1983 policy statement on deception, the practice must be evaluated from the perspective of a reasonable consumer, and it must be material.[105] A deceptive practice occurs when a business makes representation to consumers but "lacks a 'reasonable basis' to support the claims made."[106] Most of the Commission's privacy cases have relied on the FTC's deception authority. Examples of deceptive trade practices include broken promises to consumers related to data security and actions taken to encourage or induce disclosure of personal information from consumers or financial institutions.[107] Insufficient notice to consumers concerning commercial data practices has been "one of the most central aspects of the FTC's privacy jurisprudence[.]"[108] The Commission has brought deception actions where companies have failed to provide sufficient notice concerning data use policies, the storage of personal information, default software settings, and the collection of personal data.[109]

Prevalence

The Commission has the authority to issue a proposed trade regulation rule where the unfair or deceptive acts or practices at issue are "prevalent."[110] Two categories of evidence can be used to demonstrate prevalence: (1) past cease-and-desist orders by the Commission concerning the practices at issue and (2) "any other information available to the Commission indicat[ing] a widespread pattern of unfair

---

[104] FTC, *Policy Statement on Deception* (1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf [hereinafter FTC Deception Statement].
[105] *Id.*
[106] *Daniel Chapter One v. FTC*, 405 F. App'x 505, 506 (D.C. Cir. 2010) (quoting *Thompson Med. Co., Inc., v. FTC*, 791 F.2d 189, 193 (D.C. Cir. 1986)).
[107] Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 628–33 (2014).
[108] *Id.* at 634–36.
[109] *Id.*
[110] 15 U.S.C. § 57a(b)(3).

or deceptive practices."[111] Here, prior enforcement actions, academic research, market data, news reports, and numerous other sources—many of which are cited in the Commission's ANPR[112]—demonstrate "that harmful commercial surveillance and lax data security practices may be prevalent and increasingly unavoidable."[113]

OVERARCHING CONSIDERATIONS FOR A RULE

1. THE SCOPE OF COVERED DATA

Responsive to question 10.

As the Commission determines what types of data should be covered by a potential rule, we urge it to define personal data broadly, with special attention to sensitive data and inferences. A good definition recognizes that personal data includes both data that is explicitly associated with a particular individual and also data from which it is possible to infer the identity of a particular individual. The Definitions of personal data vary slightly between existing regulations,[114] but the most comprehensive definitions describe personal data as any information that "identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or [to] a device that identifies or is linked or reasonably linkable to an individual, and may include derived data and unique persistent identifiers."[115] This includes sensitive data (though sensitive data should

---

[111] *Id.*
[112] ANPR, *supra* note 1, at 51273–76.
[113] *Id.* at 51276.
[114] *See, e.g.*, Commission Regulation (EU) 2016/679, art. 4(1), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR] (personal data includes "any information relating to an identified or identifiable natural person," including both direct and indirect identifiers); American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 2(8)(A) (2022) [hereinafter ADPPA] (covered data is "information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual and may include derived data and unique identifiers"); California Consumer Privacy Act, Cal. Civ. Code § 1798.140(o)(1) (2018) [hereinafter CCPA] (personal information is "information that identifies, relates to, describes, is reasonably associated with, or could reasonably be linked, directly or indirectly, with a particular consumer" – this includes identifiers that could be linked with a particular household); Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1303(17)(a) (2021) [hereinafter Colorado Privacy Act] (personal data is "information that is linked or reasonably linkable to an identified or identifiable individual").
[115] ADPPA § 2(8)(A).

be subject to additional protections), data linkable to an individual device, and non-aggregated data, as all of these could be used to identify an individual.

Several existing regulations do not consider de-identified data to be personal data.[116] However, this exclusion is only workable when de-identified data is clearly differentiated from personal data such that it is impossible to connect de-identified data to an individual.[117] This standard is much higher than merely requiring that names or exact birthdates be removed, that a simple cipher be applied to data, or that data be pseudonymized. In fact, the standard should be much closer to true anonymization. Without clear restrictions on what may be considered de-identified data, there is a potential overlap between de-identified data and personal data, creating confusion for companies, consumers, and enforcement bodies. EPIC suggests the following definition of de-identified data, adapted from the proposed American Data Privacy and Protection Act (ADPPA):

> DE-IDENTIFIED DATA.—The term ''de-identified data'' means information that does not identify and is not linked or reasonably linkable to a distinct individual or a device, regardless of whether the information is aggregated, and if the covered entity or service provider—
>
> (A) takes technical measures to ensure that the information cannot, at any point, be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual;
>
> (B) publicly commits in a clear and conspicuous manner—
>
> (i) to process and transfer the information solely in a de-identified form without any reasonable means for re-identification; and

[116] *See, e.g.*, *id.* at § 2(8)(B)(i); CCPA § 1798.140(o)(3); Colorado Privacy Act § 6-1-1303(17)(b).
[117] *See, e.g.*, Colorado Privacy Act § 6-1-1303(11) (only data that cannot reasonably be used to infer information about or otherwise be linked to an identified or identifiable individual or device linked to that individual may be considered de-identified data and parties using de-identified data must make commitments to use and maintain the data solely in de-identified form); CCPA § 1798.148(c) (requires a contract in place for any sale or licensing of deidentified information that includes specific provisions prohibiting reidentification); ADPPA § 2(10) (2022) (mandates that de-identified data cannot identify or be linked or reasonably linkable to an individual or individual's device, regardless of whether information is aggregated).

> (ii) to not attempt to re-identify the information with any individual or device that identifies or is linked or reasonably linkable to an individual; and
>
> (C) contractually obligates any person or entity that receives the information from the covered entity or service provider—
>
> (i) to comply with all of the provisions of this paragraph with respect to the information; and
>
> (ii) to require that such contractual obligations be included contractually in all subsequent instances for which the data may be received.[118]

Several regulations also make distinctions between personal data and sensitive data, which is subject to heightened protections. The use of sensitive data (also called sensitive covered data,[119] sensitive personal information,[120] or special categories of personal data)[121] carries with it higher risk to the data subject, whether that be from breach, misuse, targeting, or other processing. While definitions vary, sensitive data typically includes data related to government-issued identifiers (such as social security number, passport number, etc.), health information, biometric and genetic data, financial information, sexual orientation and behavior, religious or philosophical belief, union membership, race and national origin, and children's information.[122] Some statutes have also included geolocation data, the contents of

[118] ADPPA § 2(10).
[119] ADPPA § 2(24).
[120] CCPA § 1798.140(ae).
[121] GDPR art. 9.
[122] ADPPA § 2(24) (sensitive covered data includes government-issued identifiers (social security number, passport number, or driver's license number); information describing or revealing past, present, or future physical health, mental health, disability, diagnosis, healthcare condition, or treatment of an individual; financial account number, debit card number, credit card number, or information about income level or bank account balances; biometric information; genetic information; precise geolocation information; private communications; account or device log-in credentials or security/access codes; information identifying sexual orientation or sexual behavior; calendar, address book, phone/text logs, photos, audio recordings, videos, etc. stored on a private device; photo, film, video recording, or similar showing naked or underwear-clad private area; info revealing video content or services requested/selected by an individual; information about an individual known to be under 17; any other covered data processed for the purpose of identifying the above data types); CCPA § 1798.140(ae) (sensitive personal information includes personal information that reveals social security, driver's license, state ID card, or passport number; account

communications, and images of private areas. In order to properly protect consumers, sensitive data must be identified as distinct from ordinary personal data and must be subject to heightened protections, particularly when it comes to collection, access, data transfers, and permissible uses.

Recently, there has been growing recognition in privacy laws that certain "inferences" made about individuals also fall under the definition of personal data, as the use of consumer profiling increases.[123] For example, the proposed ADPPA includes within its scope of protected personal data "derived data," which includes data created "by the derivation of information, data, assumptions, correlations, inferences, predictions, or conclusions from facts, evidence, or other sources" about an individual or the individual's device.[124] The California Attorney General has also confirmed that inferences (including internally generated inferences) used to create a profile about a consumer or "predict a salient consumer characteristic" are personal information about the individual, subject to all required protections and data rights under California law.[125] And the most recent draft regulations issued under the Colorado Privacy Act include a new category of data, "sensitive data inferences," which are defined as "inferences made by a Controller based on Personal Data, alone or in combination with other data, which indicate an

log-in, financial account, debit or credit card number along with security/access code, password, or credentials allowing account access; precise geolocation; racial or ethnic origin, religious or philosophical belief, or union membership; contents of communications; genetic data; processing of biometric data for identification purposes; health data; and sex life or sexual orientation); Colorado Privacy Act § 6-1-1303(24) (Sensitive data is personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation, citizenship or citizenship status, genetic or biometric data used to identify an individual, or personal data from a known child); GDPR art. 9 (special categories of personal data include "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation").

[123] *See, e.g.*, Privacy International, *Examples of Data Points Used in Profiling* (2018), https://privacyinternational.org/sites/default/files/2018-04/data%20points%20used%20in%20tracking_0.pdf;

[124] ADPPA § 2(11).

[125] 105 Ops. Cal. Atty. Gen. at 5, 10–13 (2022), https://oag.ca.gov/system/files/opinions/pdfs/20-303.pdf (referencing CCPA § 1798.140(o)(1)(K), which specifically includes in the definition of personal information "[i]nferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes").

individual's racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status."[126]

To ensure that the Commission's commercial surveillance rule is flexible enough to adapt to future changes in technology, the FTC should adopt a broad definition of covered personal data, with special attention to sensitive data and inferences.

2. OBSOLESCENCE

Responsive to question 95.

The regulations that emerge from the Commission's commercial surveillance rulemaking process must stand the test of time. Both the technologies used by commercial actors to exploit personal data and the business models that incentivize such exploitation are constantly evolving, presenting new threats to privacy and civil rights. But as the Commission is well aware, section 18 rulemaking is a lengthy and resource-intensive process—one the FTC is unlikely to return to quickly after its initial commercial surveillance and data security rules are in place. It is therefore essential that the Commission adopt regulations which, while "specific[]"[127] are sufficiently inclusive to capture unforeseen instantiations of practices already known to be unfair and deceptive.

To this end, we make two recommendations. First, the practices that the Commission declares unfair or deceptive should, with limited exceptions, be defined in platform- and technology-neutral terms. Trade rules focused narrowly on the commercial use of dial-up internet, LaserDiscs, or carbon copy credit card imprinters would be of little or no value today. The same fate likely awaits rules that are restricted to the technological particulars of today's commercial data practices.[128]

---

[126] 45 Colo. Reg. 19 (Oct. 2022), https://www.sos.state.co.us/CCR/RegisterHome.do.
[127] 15 U.S.C. § 57a(a)(1)(B).
[128] *Cf. Electronic Communications Privacy Act (ECPA)*, EPIC (2022), https://epic.org/ecpa/ ("ECPA embodies many important and useful protections, but much has changed since ECPA was passed in 1986; from personal computing to the Internet and now the ubiquity of mobile devices, much of today's technology (and even much of yesterday's) was not conceived when the law was first

Instead, the Commission's definitions of unfair and deceptive practices should draw on well-established terminology from privacy and civil rights law: principles such as transparency, necessity, disparate impact, accountability, and purpose limitation. Rules framed in these terms are far more likely to remain relevant well into the future.

Second, in establishing "requirements . . . for the purpose of preventing such acts or practices,"[129] the Commission should take every opportunity to emphasize that the requirements it establishes are non-exhaustive. Compliance with the prophylactic provisions established by the Commission should not be understood as a safe harbor if a business practice still meets the elements of unfairness or deception. For example, we recommend below that the Commission require businesses to conduct and disclose the results of a privacy impact assessment before collecting or processing personal data, and we set out categories of information that we believe each assessment must include. But we recommend that this list be "non-exhaustive" to allow for the possibility that additional disclosures may become necessary in the future to give individuals adequate notice of how their personal data is being used. The Commission should consider using this strategy throughout the text of its rule.

drafted."); Letter from EPIC to Rep. Jim Sensenbrenner et al. (Mar. 18, 2013), https://archive.epic.org/privacy/ecpa/EPIC-to-HJC-re-ECPA-3-18-2013.pdf ("It is our view the key terms in ECPA will continue to present interpretive problems until Congress takes action to update the law.").

[129] 15 U.S.C. § 57a(a)(1)(B).

WHAT THE TRADE REGULATION RULE SHOULD COVER

1. DATA MINIMIZATION

1.1. It is an unfair trade practice to collect, use, transfer, or retain personal data beyond what is reasonably necessary and proportionate to the primary purpose for which it was collected, consistent with consumer expectations and the context in which the data was collected.

Responsive to questions 26, 27, 29, 40, 41, 43–47, 86.

A business's collection, use, retention, or transfer of a consumer's personal information beyond what is reasonably necessary and proportionate to achieve the primary purpose for which it was collected (consistent with consumer expectations and the context in which the data was collected) is an unfair business practice that has, unfortunately, become widespread in the online ecosystem in the absence of clear prohibitions. The overcollection and out-of-context secondary uses of personal data, including the sale to and use by data brokers, surveillance advertising firms, and other entities trafficking in consumer profiles, are inconsistent with the reasonable expectations of online consumers. These unfair commercial surveillance practices lead to invasive, discriminatory targeting that violates the privacy and autonomy of consumers while fueling division, misinformation, and harassment that undermine democratic institutions.

The Commission has recognized that the overcollection and misuse of personal information is a widespread problem that harms millions of consumers every day and has identified that data minimization is the key to addressing these unfair business practices. As it stated in a recent report:

> Data minimization measures should be inherent in any business plan—this makes sense not only from a consumer privacy perspective, but also from a business perspective because it reduces the risk of liability due to potential data exposure. Businesses should collect the data necessary to provide the service the consumer requested, and nothing more.[130]

[130] FTC, *Bringing Dark Patterns to Light* 17–18 (2022), https://www.ftc.gov/reports/bringing-dark-patterns-light [hereinafter FTC Dark Patterns Report].

The Commission and individual Commissioners have made numerous similar statements in support of requiring data minimization.[131]

Most online transactions and interactions between businesses and consumers can be carried out without the customer's personal data being sold, transferred, or stored to be used for an unrelated secondary purpose. Consumers reasonably expect that when they interact with a business online, that business will collect and use their personal data for the limited purpose and duration necessary to provide the goods or services they have requested. For example:

[131] *See* Statement of Commissioner Christine Wilson, *In re Drizly*, FTC (Oct. 24, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023185WilsonDrizlyStatement.pdf ("I agree that data minimization plays an important role in a healthy data security program."); *see* Statement of Commissioner Rebecca Slaughter, *In re Drizly*, FTC (Oct. 21, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Statement-of-Commissioner-Slaughter-Regarding-Drizly-FINAL.pdf ("There are many ways to approach data collection guardrails. As the FTC further develops a minimization framework, one framework I hope we consider is centering a consumer's reasonable expectation that there should be limits on the collection and use of their information based on the service they've actually requested. I believe the agency is in a better position to effectuate this expectation than it is to anticipate, understand, and police every claim of reasonable business necessity."); Press Release, FTC, *FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks* (Jan. 27, 2015), https://www.ftc.gov/news-events/news/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices-address-consumer-privacy-security ("Commission staff also recommend that companies consider data minimization – that is, limiting the collection of consumer data, and retaining that information only for a set period of time, and not indefinitely. The report notes that data minimization addresses two key privacy risks: first, the risk that a company with a large store of consumer data will become a more enticing target for data thieves or hackers, and second, that consumer data will be used in ways contrary to consumers' expectations."); Leslie Fair, *Data Breach Prevention and Response: Lessons from the CafePress Case*, FTC Bus. Blog (Mar. 15, 2022), https://www.ftc.gov/business-guidance/blog/2022/03/data-breach-prevention-and-response-lessons-cafepress-case ("The order also mandates that the company put in place and maintain an Information Security Program that includes (among other things) policies and procedures for data minimization and data deletion."); Stipulated Order, *United States v. Kurbo, Inc.*, No. 3:22-cv-00946-TSH, 7 (N.D. Cal. Mar 3, 2020) (The Commission permanently restrained Kurbo f/k/a WeightWatchers from "retaining personal information collected online from a child for longer than reasonably necessary to fulfill the purpose for which the information was collected[.]").

COMMERCIAL SURVEILLANCE AT WORK

When a person uses a map application to get directions to a restaurant from their current location, the consumer reasonably expects that their precise location data will be collected and used by the app to provide them with turn-by-turn directions they have requested, and perhaps display advertisements for nearby businesses. The consumer may also reasonably expect that the app will store a record of the most recent destinations they have searched for the limited purpose of suggesting the same or similar search again. And if the app uses the consumer's location data to identify and compare nearby traffic patterns to find an optimal route, that is within the scope of the original purpose and consumer's expectations. The consumer does not expect that their precise location data will be disclosed to third parties they have no relationship with and combined with other data about them to profile them.

But businesses operating websites and mobile apps now engage in commercial surveillance practices that violate the privacy of consumer data by collecting and using it to track and profile individuals in ways that defy reasonable consumer expectations. These unfair business practices have been so widely adopted that they happen seamlessly and beyond the visibility or control of the consumer. And the result is that nearly every website we visit, every link we click, and everything we see on a screen can be tracked and cataloged to feed detailed profiles that are later used to target us in myriad ways. For example:

COMMERCIAL SURVEILLANCE AT WORK

A social media app will necessarily collect, store, and process a range of data from its users including texts and images, profile information, and potentially metadata like location or other tags. The app may also collect certain data for diagnostics, testing, or debugging of its systems (though most of this data need not be individually linkable). But the app should not process or transfer the precise location data of its users for unrelated commercial purposes. If a third-party company seeks to purchase or analyze consumer location records from the app to "know when users leave their house, their commute to work, and everywhere they go throughout the day," that would violate the privacy of the apps' users and clearly go far beyond what an average consumer expects the app to be doing with their data.[132] The social media company would also be violating their users privacy and expectations if they combine data about an individual's use of the social media app with unrelated app usage and website browsing data to build a profile of that user's behaviors.[133]

The most widespread injuries to privacy online today are the sweeping collection and use of personal data to profile and then target consumers based on what they read, where they go, who they interact with, and how likely they are to click or buy. [134] These invasive practices violate the reasonable expectations of consumers and cause substantial injury. Consumers have a strong interest in the privacy and integrity of their personal data, including in who is collecting it, how much they are collecting, how they are using it, whether and to whom they are disclosing it, and how it is protected. Commercial surveillance systems rob consumers of their autonomy and also fuel other substantial harmful effects including reputational harms, discrimination, threats to physical safety, psychological harms, and economic loss.

---

[132] Steve Krenzel (@stevekrenzel), Twitter (Nov. 7, 2022, 2:26 PM), https://twitter.com/stevekrenzel/status/1589700736207949824.

[133] A recent report by Congress found that "Google's internal reports show that Google was tracking in real-time the average number of days users were active on any particular app, as well as their total time spent in first- and third-party apps." Majority Staff of H. Subcomm. On Antitrust, Com. & Admin. L. of the H. Comm. on the Judiciary, 116th Cong., *Investigation of Competition in Digital Markets* 13 (2020), https://fm.cnbc.com/applications/cnbc.com/resources/editorialfiles/2020/10/06/investigation_of_competition_in_dig ital_markets_majority_staff_report_and_recommendations.pdf (internal citations omitted) [hereinafter Investigation of Competition in Digital Markets].

[134] Consumer Reps. & EPIC, *supra* note 3 at 6.

This section first provides an overview of the systems that facilitate commercial surveillance online. Next, it addresses the substantial injuries that consumers suffer when businesses fail to limit the collection and use of their personal data to what is reasonably necessary to provide the goods or services that the consumer has requested, and describes how consumers cannot reasonably avoid the overcollection and misuse of their personal information. This section further explains how prevalent commercial surveillance practices do not provide benefits to consumers or competition that outweigh the substantial injuries to consumers' privacy. Indeed, most of the convenience and efficiency benefits that consumers experience online can be provided by businesses that minimize the collection and use of personal data to what is reasonably necessary and proportionate to provide the goods and services that consumers request and expect. The Commission should prohibit businesses from collecting or using personal data beyond what is necessary to achieve the primary processing purposes for which it was collected, consistent with the average consumer's expectations and with the context in which the data was collected.

Businesses that operate websites, apps, and other online services deploy a wide range of systems that automatically collect personal data, often without consumers' knowledge. Other companies do not have any direct relationship with consumers and instead focus entirely on deploying systems to collect, store, sell, transfer, trade, and analyze data to profile and track consumers. These data brokers and other third parties involved in the surveillance economy sell profiles, personal data, and analytics services to advertisers, brand managers, publishers, and other entities for their own commercial (or other) purposes. In many cases, these profiles are used to target or shape customers' experience of the websites and services they visit in ways that are entirely opaque to them. These profiles can alter what we see, what prices we pay, and whether we are able to find the information that we seek online (including information about job opportunities, health services, and relationships).

Data collection is the initial stage of commercial surveillance systems, and it fuels harmful out-of-context secondary uses of personal data. Much of the collection of personal data happens so routinely and automatically in the online

ecosystem that customers have little to no knowledge of its scope. Tracking systems are embedded in most websites, apps, and services and begin to collect information as soon as a consumer connects to a service. Indeed, with the increasing proliferation of "smart" devices in homes, offices, and other locations, the collection of personal data frequently happens even when customers aren't intending to interact with an online service at all. And other activities like credit card purchases[135] and even physical movements[136] can be logged and tracked without the consumer's awareness or control. These countless data points can be combined to reveal sensitive details about consumers and put them at risk of many harms, including discrimination, stalking, harassment, and government scrutiny.[137]

Personal data is generated and collected in several different ways during the course of consumers' routine online and offline activities. First, personal data is generated and collected whenever a user loads content from a website, app, service, or connected device. Some of this data is necessary to request, route, and load content and services, but other data might be collected and stored even if it isn't necessary to complete a consumer's request. Second, data can be created and collected through interactions with and use of a website, app, service, or device. Some of this data is sent or generated by the user themself (e.g., search queries, messages, and profile updates), but other data might be collected based on what the user is doing and how they are interacting with the system (e.g., what they click on, how long they stay on a page, or even where their focus shifts). And third, data is collected and transferred to and from a broad range of sources by entities who have

---

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

[136] Michael Kwet, *In Stores, Secret Surveillance Tracks Your Every Move*, N.Y. Times (June 14, 2019), https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html.

[137] Manuela López Restrepo, *Does Your Rewards Card Know if You're Pregnant? Privacy Experts Sound the Alarm*, NPR (Aug. 13, 2022), https://www.npr.org/2022/08/13/1115414467/consumer-data-abortion-roe-wade-pregnancy-test-rewards-card-target-walgreens; *see also* Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, Forbes (Feb. 16, 2022), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

no direct relationship to the consumer (e.g., data brokers, surveillance firms with cameras or embedded sensors, and government agencies).[138]

The next stage of these commercial surveillance systems is the linkage of collected data through identifiers used to track, profile, or target consumers across the online ecosystem. There are several widely used methods to link data collected about consumers online, including: known credentials/first party logins, unique device identifiers, third party tracking cookies, and device fingerprinting. Data about what consumers do online can be linked to them automatically if they are browsing a site or using an app or service that already knows them through an established login or known credential (e.g., e-mail address, phone number, or username), but there are many other ways that data can be linked even by unknown third parties. When data is collected about activities of a consumer using a computer or mobile device, any unique identifiers associated with that device might be used to link that data with other data sets or profiles about the consumer.[139] Web browsers use small files called "cookies" to store information about a user's interactions with the sites they visit, and many firms engaged in commercial surveillance have used versions of these files commonly referred to as "third party tracking cookies" to collect information about what sites users are visiting.[140] And even when a user's browser or device is configured to block these tracking cookies or to not broadcast unique identifiers, online entities can use information about the

---

[138] FTC, *Data Brokers: A Call for Transparency and Accountability* iv (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [hereinafter FTC Data Broker Report].

[139] *See* Rebecca Smith, *What Is IDFA and Why Is This iOS Update Important?*, Mozilla (Apr. 26, 2021), https://blog.mozilla.org/en/internet-culture/mozilla-explains/turn-off-idfa-for-apps-apple-ios-14-5/; *see also* Thompson & Warzel, *supra* note 100 ("Location data is also collected and shared alongside a mobile advertising ID, a supposedly anonymous identifier about 30 digits long that allows advertisers and other businesses to tie activity together across apps. The ID is also used to combine location trails with other information like your name, home address, email, phone number or even an identifier tied to your Wi-Fi network.").

[140] Emily Stewart, *Why Every Website Wants You to Accept Its Cookies*, Vox (Dec. 10, 2019), https://www.vox.com/recode/2019/12/10/18656519/what-are-cookies-website-tracking-gdpr-privacy ("There are first-party cookies that are placed by the site you visit, and then there are third-party cookies, such as those placed by advertisers to see what you're interested in and in turn serve you ads—even when you leave the original site you visited. (This is how ads follow you around the internet.)"); *see Cookies on Mobile 101*, IAB (Nov. 2013), https://www.iab.com/wp-content/uploads/2015/07/CookiesOnMobile101Final.pdf.

consumer's computer configuration (e.g., operating system, browser, versions, etc.) as a sort of "fingerprint" to link their data across apps, sites, and services.[141] For example:

COMMERCIAL SURVEILLANCE AT WORK

A consumer, Frank, goes to a news website, and the website has a third-party tracking cookie from a different and unrelated website that he visited earlier in the day. This cookie identifies him. Data about what he's reading is transferred to a broker and is linked to other things he read that day. The third-party cookies embedded in the webpage automatically collect his personal information, including his location data, time zone, his operating system, his WiFi network, what links he clicks on, and his IP address, linking all of this information to him and his browser. This information is quickly transferred to data brokers or advertising networks which use this information to continue to add to the Frank's already robust profile.

When another user, Alice, reads an article on a news app on their phone, the third-party ad plugins on the app are not able to link their activity based on their phone's device ID because it has been disabled. But data brokers are able to link Alice's unique device configuration fingerprint from another app where they were logged in, and now the information about what news articles they were reading is added to their profile and linked to their earlier browsing activities.

The next stage in the commercial surveillance process is the profiling, targeting, and sale of personal data or personal data analytics services. Consumers' personal data can rapidly move through many different entities and be processed or sold for myriad purposes. The data brokers and analytics companies that transit in this personal data have no relationship with the consumer, and their processing purposes typically have nothing to do with the initial purpose for which the consumers' data was collected. The scale of this profiling by data brokers is staggering. Even eight years ago, the Commission found that the data brokers it studied collected and stored data "on almost every U.S. household and commercial transaction," and the Commission found that one of the largest data brokers had

[141] Chris Hauk, *What Is Browser Fingerprinting? What It Is and How to Stop It.*, PixelPrivacy (Aug. 16, 2022), https://pixelprivacy.com/resources/browser-fingerprinting/ ("Browser fingerprinting is a powerful method that websites use to collect information about your browser type and version, as well as your operating system, active plugins, time zone, language, screen resolution and various other active settings.").

"information on 1.4 billion consumer transactions and over 700 billion aggregated data elements."[142]

Some of the companies operating in this space specialize in building or "enriching" consumer profiles, while others merely buy, combine, and sell data sets from many different sources. Many of these services are used by companies engaged in targeted advertising and marketing to identify audiences that fit within specified demographics or to find "look alike" audiences based on existing customer or target lists. The Commission has found that these data brokers "combine and analyze data about consumers to make inferences about them, including potentially sensitive inferences."[143] The largest companies, like Acxiom and Oracle, offer a panoply of targeting and profiling tools. And the advertising platforms themselves, including Facebook and Google, also offer their own audience analytics tools. These companies profit off data harvested from consumer activities and transactions in ways entirely outside the expectations of consumers in their interactions with first-party businesses.

For example, the "Comprehensive Global Data and Insights" services that Acxiom sells provide a perfect snapshot of the breadth and depth of profiling and targeting in the commercial surveillance marketplace. The company's descriptions of its services reveal how extensive its profiling is and the extensive reach of its personal data acquisitions:

- Build Precise Audiences: Tap into limitless combinations of high-quality data to create and distribute audiences to meet specific campaign needs. Use off-the-shelf packages or let Acxiom data experts help.
- Enrich First-Party Data: Enhance first-party files with third-party descriptive and predictive data. Better understand the needs, wants, and preferences of your audiences.
- Leverage Innovative Data: Pinpoint receptive audiences with new types of data including place-based signals, in-app behaviors, and online consumption.

[142] FTC Data Broker Report, *supra* note 138, at iv.
[143] *Id*.

- Personicx Segmentation Solutions: Better understand and engage the modern customer. Group customers into similar segments based on specific behaviors and demographic characteristics.
- Predictive Audiences: Likely affinity and preferences. These ready-to-use predictive analytics enable you to deliver relevant messages.
- Top Data Packages: Captive audiences by Season or Interest. Acxiom offers the industry's most comprehensive consumer data. [144]

The goal of these and other similar systems is to enable companies to track and target specific users based what they watch, what they read, what they buy, who they know, and where they go. And data brokers are continually expanding their reach deeper and deeper into the private lives of individuals, especially as connected devices, services, and even audio and visual sensors become more prevalent on streets, in stores, in offices, and in homes. For example, The Trade Desk, which runs another large targeted advertising platform, promotes its "Connected TV" advertising platform as being able to "go beyond demographics and leverage first- and third-party data to reach your most valuable audiences on every screen."[145] In this context, the consumer is given no agency and is forced to simply make do with the fact that their every move and reaction is being logged and used to target them with advertisements and other content that will follow them across devices, physical spaces, and contexts.

Some data brokers and companies involved in the trafficking of personal data claim that their activities do not implicate privacy because they are only handling "anonymized" data. Typically these claims do not hold up to even the most casual scrutiny, unless the company holds or processes only aggregate data sets processed to ensure robust deidentification.[146] Most data brokers are in the business of selling or offering use of targeted consumer profiles and thus intentionally maintain identifiable data sets. But even data brokers that trade in large or aggregate data sets likely have access to sufficient information that their systems can be used to re-

[144] *Acxiom Data: Comprehensive Global Data and Insights*, Axciom, https://www.acxiom.com/customer-data/ (last visited Nov. 17, 2022).
[145] *Connected TV*, The Trade Desk, https://www.thetradedesk.com/us/our-platform/dsp-demand-side-platform/connected-tv (last visited Nov. 17, 2022).
[146] *See generally* Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 Wash. L. Rev. 703 (2016), https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4948&context=wlr.

identify or link data to individuals across sets.[147] One data point in isolation may not tell an advertiser much, but millions and millions of data points allow data brokers to link information to individual consumers.

One of the largest systems of commercial surveillance, tracking, and profiling is the online advertising process known as real-time bidding (RTB).[148] This is the "process by which the digital ads we see every day are curated."[149] The IAB has explained how ubiquitous this process is: there is "not a single website publisher, mobile app, or advertising brand today that doesn't participate in real-time systems for buying or delivering personalized ads to consumers."[150] RTB systems rapidly relay information about consumers to facilitate auctions that sell digital ad space in real time. "The hundreds of participants in these auctions receive sensitive information about the potential recipient of the ad—device identifiers and cookies, location data, IP addresses, and unique demographic and biometric information such as age and gender."[151] This "bidstream" data flows to hundreds of entities (including domestic and foreign entities that have no intention of actually serving ads) and are used to "compile exhaustive dossiers about" consumers that "include their web browsing, location, and other data, which are then sold by data brokers to hedge funds, political campaigns, and even to the government without court

---

[147] *See* Boris Lubarsky, *Re-Identification of "Anonymized" Data*, 1 Geo. L. Tech. Rev. 202 (2017), https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/; Danny Bradbury, *De-identify, Re-identify: Anonymised Data's Dirty Little Secret*, Register (Sept. 16, 2021), https://www.theregister.com/2021/09/16/anonymising_data_feature/.

[148] Jack Marshall, *WTF Is Real-time Bidding?*, Digiday (Feb. 17, 2014), https://digiday.com/media/what-is-real-time-bidding/.

[149] Letter from Sen. Ron Wyden, et al., to Chairman Joseph Simons, Fed. Trade Comm'n (July 31, 2020), https://www.wyden.senate.gov/imo/media/doc/073120%20Wyden%20Cassidy%20Led%20FTC%20Investigation%20letter.pdf.

[150] Jordan Mitchell, *The Evolution of The Internet, Identity, Privacy And Tracking – How Cookies And Tracking Exploded, And Why We Need New Standards For Consumer Privacy*, IAB Tech Lab (Sept. 4, 2019), https://iabtechlab.com/blog/evolution-of-internet-identity-privacy-tracking/.

[151] *Id*.

orders."[152] Companies have used this bidstream data to violate Americans' privacy on a massive scale and have even used it to profile "participants [in] Black Lives Matter protests" and to track "Americans who visited places of worship and then built religious profiles based on that information."[153]

The collection, sale, and use of personal data for targeted advertising and consumer profiling causes substantial injury to consumers. Privacy harms typically fall within one of seven categories, as explained by Professors Danielle Citron and Daniel Solove in their recent (aptly named) article *Privacy Harms*. Those categories are:

(1) physical harms;
(2) economic harms;
(3) reputational harms;
(4) psychological harms;
(5) autonomy harms;
(6) discrimination harms; and
(7) relationship harms.[154]

Out-of-context secondary uses of personal data by businesses involved in targeted advertising, consumer profiling, and other commercial surveillance practices can cause harm across all these categories, providing a basis for a finding of substantial injury.

The most direct privacy harms caused by out-of-context secondary uses are harms to autonomy. The collection and use of personal data for targeting and profiling purposes inconsistent with the context in which the data was initially collected from the consumer is a violation of "contextual integrity" that fundamentally deprives the individual of autonomy over their data. Consumer autonomy is also lost when consumers' reasonable expectations are thwarted, when individuals are subject to manipulation, or when data collection practices deprive consumers of control over their own data.[155] Targeted advertising and consumer profiling systems infringe on consumer autonomy across all these sub-categories.

[152] *Id.*
[153] *Id.*
[154] Citron & Solove, *supra* note 18, at 831.
[155] Solove & Citron, *supra* note 154, at 845–46.

When a consumer expects that their data will be used in a specific context for a limited purpose, and companies instead use, retain, transfer, or sell that data for an unrelated purpose, that is a substantial injury to an individual's contextual integrity and autonomy. As Professors Citron & Solove have explained,

> Privacy harms are highly contextual, with the harm depending upon how the data is used, what data is involved, and how the data might be combined with other data. Sharing an innocuous piece of data with another company might provide a key link to other data or allow for certain inferences to be made.[156]

The scholar who pioneered the term "contextual integrity," Professor Helen Nissenbaum, has explained that purpose limitations should be focused on the nature and context in which personal data was collected and has argued that access to intimate, sensitive, or confidential information should be restricted.[157] Specifically, Professor Nissenbaum has argued that "context-relative information norms" should govern the flow of personal information in order to protect people from harm and balance power distribution.[158] In other words, personal information shared to ensure that an item is delivered to a customer is an appropriate data flow. In contrast, sensitive information that is collected and shared with advertisers that inform a teenager's father that she is pregnant before she has told him is an inappropriate data flow because it violates the context in which the teenager searched for

---

[156] Solove & Citron, *supra* note 154, at 818.

[157] Helen Nissenbaum, Symposium, *Privacy as Contextual Integrity*, 79 Wash. L. Rev. 119, 128 (2004), https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10 ("In the United States legal landscape, sensitive information is accorded special recognition through a series of key privacy statutes that impose restrictions on explicitly identified categories of sensitive information. Examples include the Family Educational Rights and Privacy Act of 1974, which recognizes information about students as deserving protection; the Right to Financial Privacy Act of 1978, which accords special status to information about people's financial holdings; the Video Privacy Protection Act of 1988, which protects against unconstrained dissemination of video rental records; and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which set a deadline for adoption of privacy rules governing health and medical information by the U.S. Department of Health and Human Services. Further, the common law recognizes a tort of privacy invasion in cases where there has been a "[p]ublic disclosure of embarrassing private facts about the plaintiff' or an "[i]ntrusion ... into [the plaintiffs] private affairs. Similar thoughts were expressed by Samuel D. Warren and Louis D. Brandeis, who were specifically concerned with protecting information about "the private life, habits, acts, and relations of an individual.") (footnotes omitted).

[158] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* 3 (2010).

information.[159] Data from person's purchase history of certain supplements and lotions that enters a "pregnancy-prediction model" is a contextual integrity violation because it violates norms that a person expects when making such purchases.[160]

Consumers should be able to use their devices and apps and browse the internet without fear that every click will be added to a profile and used to push them towards buying something. Commercial surveillance entities surreptitiously monitor consumers' browsing and purchasing habits, then use them to infer sensitive personal characteristics and modify consumer behavior. For example:

[159] *See* Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, Forbes (Feb. 16, 2022), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/; Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times (Feb. 16, 2021), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[160] *Id.* ("Take a fictional Target shopper named Jenny Ward, who is 23, lives in Atlanta and in March bought cocoa-butter lotion, a purse large enough to double as a diaper bag, zinc and magnesium supplements and a bright blue rug. There's, say, an 87 percent chance that she's pregnant and that her delivery date is sometime in late August. What's more, because of the data attached to her Guest ID number, Target knows how to trigger Jenny's habits. They know that if she receives a coupon via e-mail, it will most likely cue her to buy online. They know that if she receives an ad in the mail on Friday, she frequently uses it on a weekend trip to the store. And they know that if they reward her with a printed receipt that entitles her to a free cup of Starbucks coffee, she'll use it when she comes back again.").

COMMERCIAL SURVEILLANCE AT WORK

If a consumer, call her Ronna, decides to shop online for a new bag to use for different personal, professional, and parental tasks, she would likely start by searching for relevant reviews, product listings, and promotions. Each website she visits is providing a specific type of content or service, and some may ask her to register for promotional updates and offers. Many of the sites would be ad-supported, and Ronna would likely expect to see advertisements for shoes and similar items on the pages where she is reading reviews or listings about those products. But Ronna likely does not expect or know that her browsing habits are being logged and used to build and "enrich" profiles held by many different data brokers, as they attempt to fit her into categories based on her age range, level of affluence, frequency of online activity, and family status.[161] These categories, along with data about the specific products and sites she has been visiting, would then be used to target her with ads across other websites and services. She might keep seeing the same bag that was promoted on one of the pages that she visited, its image popping up in ads on news websites and other pages she visits for work, or even in the apps that she uses to manage her infant son's sleep schedule.

Then when she mentions to her friend Sam that she had been shopping for a new bag recently, Sam does a quick search on his phone to look for a recent review and (unbeknownst to Sam) sees an advertisement for the same bag that has been stalking Ronna across all her devices. The data brokers analyzing the personal data collected from both Ronna and Sam's browsing had noticed that they were located in the same place and were linked on social media, and the company marketing the product had automatically targeted individuals linked to or likely to influence other potential customers. When Sam mentions the product during his conversation with Ronna, she mistakenly thinks that her friend is recommending something to her based on his own knowledge, but it is all based on the coercive targeting that has happened without her knowledge and outside of her control.

These types of manipulative practices cause not only violations to contextual integrity, but also thwarted expectations. As Ryan Calo has explained, "the harm caused by thwarted expectations involves the undermining of people's choices, such as breaking promises made about the collection, use, and disclosure of personal data. Thwarted expectations is an autonomy harm because it results in people's inability to make choices in accordance with their preferences."[162] In a more traditional sales transaction, for example, a consumer would contact a seller to buy a

[161] *See, e.g.*, Acxiom, *Acxiom Data Catalogue for Audience Creation and Analysis* 5 (2017), https://marketing.acxiom.com/rs/982-LRE-196/images/Data%20Catalogue%20for%20Audience%20Creation%20and%20Analytics_UK.pdf.
[162] Solove & Citron, *supra* note 154, at 849.

good and provide the seller their payment information, contact information, and shipping information in order to effectuate the sale. The consumer might expect that this information would be sent to a third-party payment processor and the third-party shipping provider to receive the item that they purchased. In today's surveillance economy, that consumer's information is instantly collected, passed down the data stream, and used to build a profile on the consumer. This practice contradicts the expectation of the consumer and undermines the consumer's trust and autonomy, causing a substantial injury.

Manipulation is harmful because it can make a consumer the instrument of another's will, violating their autonomy or offending their dignity by failing to treat the consumer with respect.[163] Solove and Citron have compiled several reasons why manipulation is harmful.[164] Manipulation causes subjective privacy harms when "the consumer has a vague sense that information is being collected and used to her disadvantage, but never truly knows how or when."[165] It might cause objective privacy harms when a firm uses a consumer's personal information to extract as much rent as possible.[166] Manipulation is also is harmful because it impairs a consumer's process of choosing, subjecting them to the influence of third parties.[167] Manipulation is more than an individual harm; it can also create societal harm. For example, the Cambridge Analytica incident involved the use of personal data on a mass scale to influence people's decisions in the 2016 U.S. presidential election and in the United Kingdom's vote for Brexit.[168]

Out-of-context secondary uses also substantially injure consumers' autonomy by depriving them of control over their personal information. "Lack of control involves the inability to make certain choices about one's personal data or to

---

[163] Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. Mktg. Behav. 213, 217 (2015).
[164] *Id.* at 847.
[165] Ryan Calo, *Digital Market Manipulation*, 82 Geo. Wash. L. Rev. 995, 1029 (2014).
[166] *Id.*
[167] Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 Theoretical Inquiries L. 157, 174 (2019).
[168] *See* Carole Cadwalladr, *The Great British Brexit Robbery: How Our Democracy Was Hijacked*, Guardian (July 13, 2021), https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy [https://perma.cc/2L67-ZJG5]; *see also* Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 Calif. L. Rev. 1753, 1816 (2019).

be able to curtail certain uses of the data."[169] This constitutes an injury because it diminishes a consumer's ability to manage risk to the security of their information and denies them the ability to limit its downstream uses.[170] The loss of control poses special concerns for sensitive data about individual consumers' finances, health, intimate relationships, and precise location. Consumers lack control over data that is collected without their knowledge. They also lack control over data that they knowingly provide to a company for a limited purpose because they have no practical ability to prevent the repurposing of that data by the company or other entities in the online ecosystem.

The practice of overcollection of consumers' personal information also injures a consumer's autonomy because they reasonably expect collection for a specific purpose but lack control of their information once it has been collected. This overcollection causes harm because it leads to data being used or changing hands downstream and falling out of consumer control. The Commission has tried for over a decade to require Facebook to give consumers' control over their own data,[171] to no avail.[172] In its recent lawsuit against Kochava, the Commission identified the company's lack of meaningful access controls on its location data feed as causing injury. The Commission wrote:

> [Consumers] do not know who has collected their location data and how it is being used. Indeed, once information is collected about consumers from their mobile devices, the information can be sold multiple times to companies that consumers have never heard of and never interacted with. Consumers have no insight into how this data is used—they do not, for example, typically know or understand that the information collected about them can be used to track and map their past movements and that inferences about them and their behaviors will be drawn from

[169] Solove & Citron, *supra* note 154, at 853.
[170] *Id.*
[171] Press Release, FTC, *FTC Gives Final Approval to Modify FTC's 2012 Privacy Order with Facebook with Provisions from 2019 Settlement* (Apr. 28, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/04/ftc-gives-final-approval-modify-ftcs-2012-privacy-order-facebook-provisions-2019-settlement.
[172] Lorenzo Franceschi-Bicchierai, *Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document*, Vice (Apr. 26, 2022), https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.

> this information. Consumers are therefore unable to take reasonable steps to avoid the above-described injuries.[173]

Noting that Kochava employed no technical controls to limit or prohibit its customers from identifying consumers or tracking their locations, the Commission alleged that these practices caused or were likely to cause substantial injuries to consumers, including "exposure to stigma, discrimination, physical violence, emotional distress, and other harms."[174] Overcollection and the failure to delete data when it is no longer needed can also cause injury to consumers due to lack of control resulting from mergers and acquisitions. For example:

COMMERCIAL SURVEILLANCE AT WORK

Last year Blackstone, a large private equity firm acquired Ancestry, a direct-to-consumer genetic testing company, rightfully worrying consumers that such a firm would have access to their DNA. While Blackstone has claimed that it will not access user DNA,[175] there are plenty of other valuable data points that it now owns. Blackstone could also change that plan at any time. The original purpose for which the consumer's information was collected was to provide them with their genetic information and family tree, and those purposes are entirely unrelated to Blackstone. Ultimately, Blackstone could unilaterally change its policies and access or use customers' DNA information for any commercial or other purpose with no clear mechanism for customers to prevent that.

This demonstrates that overcollection of personal data in itself is harmful, even before it is used for an out-of-context secondary purpose.

As Professors Citron and Solove have explained, "autonomy harms involve restricting, undermining, inhibiting, or unduly influencing people's choices. People are prevented from making choices that advance their preferences. People are either directly denied the freedom to decide or are tricked into thinking that they are freely

---

[173] Complaint for Permanent Injunction and Other Relief, *FTC v. Kochava, Inc.*, 2:22-cv-00377-DCN, 9 (D. Idaho filed Aug. 29, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf.

[174] *Id.* at 7–9.

[175] David Lazarus, *Why Spend Billions for Ancestry's DNA Data If You Don't Plan to Use It?*, L.A. Times (Apr. 13, 2021), https://www.latimes.com/business/story/2021-04-13/column-blackstone-ancestry-genetic-privacy.

making choices when they are not."[176] When consumers are denied autonomy over their personal data, we are denied the ability to "determine and express our identities, by ourselves and with others, but ultimately—and essentially—on our own terms."[177] Harms to autonomy cause substantial injury to consumers.

Commercial surveillance also leads to discrimination harms, which are particularly nefarious because they often hide behind opaque data practices. Targeting and profiling systems are designed to divide, segment, and score individuals based on their characteristics, their demographics, and their behaviors. In many cases, this means that consumers are sorted and scored in ways that reflect and entrench systematic biases. "[C]onsumers of color continue to receive worse treatment and experience unequal access to goods and services due to discriminatory algorithms and exploitative data practices."[178] For example, targeted advertising reinforces discrimination against marginalized and vulnerable groups of individuals and deprives those individuals of equal access to information about employment, housing, educational, credit, and other economic opportunities.[179] Facebook has faced allegations of advertising discrimination on its platform, including several lawsuits. In 2019, the Department of Housing and Urban Development sued Facebook for engaging in housing discrimination by allowing advertisers to control which users saw ads based on characteristics like race, religion, or national origin.[180] In 2022, Facebook settled a related lawsuit with the Department of Justice, agreeing to change its ad delivery system.[181] Yet studies have

---

[176] Solove & Citron, *supra* note 154, at 845–55.
[177] Neil Richards, *Why Privacy Matters* 113 (2021).
[178] David Brody Testimony, *supra* note 18, at 5.
[179] Aaron Rieke & Corrine Yu, *Discrimination's Digital Frontier*, Atlantic (Apr. 15, 2019), https://www.theatlantic.com/ideas/archive/2019/04/facebook-targeted-marketing-perpetuates-discrimination/587059/.
[180] Charge of Discrimination, *HUD, et al v. Facebook, Inc.*, FHEO No. 01-18-0323-8 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.
[181] Press Release, U.S. Atty's Off. for the S. Dist. of N.Y., *United States Attorney Resolves Groundbreaking Suit Against Meta Platforms, Inc., Formerly Known As Facebook, To Address Discriminatory Advertising For Housing* (June 21, 2022), https://www.justice.gov/usao-sdny/pr/united-states-attorney-resolves-groundbreaking-suit-against-meta-platforms-inc-formerly; Naomi Nix & Elizabeth Dwoskin, *Justice Department and Meta Settle Landmark Housing Discrimination Case*, Wash. Post (June 21, 2022), https://www.washingtonpost.com/technology/2022/06/21/facebook-doj-discriminatory-housing-ads/.

shown that an advertiser can still create discriminatory ads without explicitly targeting based on protected characteristics due to the extensive amount of personal information that ad platforms have collected about their users.[182]

In addition to harms to autonomy and discrimination harms, a number of the other harms identified by Citron and Solove are also implicated by commercial surveillance, including physical, economic, reputational, psychological, and relationship harms. Physical harms include stalking, assault, rape, and murder, which all courts recognize as injuries in both the civil and criminal context.[183] Doxing can be found to be a physical harm.[184] Courts have also recognized economic harms stemming from a privacy violation where a heightened risk of identity theft results in financial loss.[185] The expansive collection, transfer, and storage of personal data to feed commercial surveillance systems increases the risk of data breaches and the resulting injuries that are caused by those incidents. Companies that stockpile and retain personal data for longer than is reasonably necessary place that data at risk of breach. These comments discuss issues of data security in further detail in section 6 and propose rules that complement the data minimization rules proposed in this section.

Reputational harms have a long history of judicial recognition through tort claims of libel, false light, defamation, and slander.[186] Misuse of personal data can also cause psychological harms in the form of emotional distress and disturbance spanning from annoyance to anger and can ultimately "impeded someone's life as much as certain physical injuries." Some examples include doxing, threats or harassment online, and fear of exposure or misuse of sensitive data including

---

[182] Till Speicher, *Potential for Discrimination in Online Targeted Advertising, Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 81 Proc. Mach. Learning Rsch. 5 (2018), https://proceedings.mlr.press/v81/speicher18a.html ("The potential for discrimination in targeted advertising arises from the ability of an advertiser to use the extensive personal (demographic, behavioral, and interests) data that ad platforms gather about their users to target their ads. An intentionally malicious—or unintentionally ignorant—advertiser could leverage such data to preferentially target (i.e., include or exclude from targeting) users belonging to certain sensitive social groups (e.g., minority race, religion, or sexual orientation).").
[183] *See* Solove & Citron, *supra* note 154, at 831–43.
[184] *See id*. at 834.
[185] *See id*. at 835–36.
[186] *See id*. at 837–41.

intimate images.[187] Relationship harms in the privacy context can result from the loss of longer-term confidentiality, and in the shorter term "damage to the trust that is essential for the relationship to continue."[188] Finally, "[p]rivacy violations can harm personal and professional relationships as well as relationships with organizations."[189]

In addition to these harms caused by commercial surveillance and out-of-context secondary uses generally, there are some harms that are specific to certain types of data collection and use. This includes location data, which is particularly sensitive, and the sale of data to law enforcement without a warrant or other legal predicate.

Unauthorized secondary use of location data is particularly harmful because it can reveal someone's physical location, both in real time and historically. This can expose an individual to stalking and other physical threats, as well as doxing. Location data can reveal sensitive information about a person's day to day activities, including whether a person goes to an abortion clinic, an AA meeting, or a certain place of worship. Often, location data is available to purchase for a nominal fee, causing significant harm. For example, last year a Catholic priest was outed when a vendor sold his commercially available location data to a news outlet.[190] The U.S. military purchased location data collected from Muslim prayer apps in order to monitor Muslim communities.[191] The U.S. Department of Immigration and Customs Enforcement purchases sensitive personal information to surveil immigrants and carry out deportations.[192]

---

[187] *Id*. at 841–42.
[188] *Id*. at 859.
[189] *Id*. For a more detailed overview, please see the Privacy Harms in Appendix 1.
[190] Associated Press, *Priest Outed via Grindr App Highlights Rampant Data Tracking*, NBC News (July 22, 2021), https://www.nbcnews.com/tech/security/priest-outed-grindr-app-highlights-rampant-data-tracking-rcna1493.
[191] Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, Vice (Nov. 16, 2020), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.
[192] Corin Faife, *ICE Uses Data Brokers to Bypass Surveillance Restrictions, Report Finds*, Verge (May 10, 2022), https://www.theverge.com/2022/5/10/23065080/ice-surveillance-dragnet-data-brokers-georgetown-law.

Victims of domestic violence or stalking live in fear that their abusers or stalkers will purchase their location information for a nominal price.[193] In 2014, a Congressional investigation uncovered the significant harms that unauthorized uses of location data poses to domestic violence victims.[194] There is a common risk that domestic violence victims will be stalked, and "stalking is often a precursor to other forms of violence."[195] There have already been several instances where an abuser used his victim's location data from a stalking app to harm her, including one instance where an abuser used his victim's precise location information from her cell phone and followed her 700 miles away to a shelter where he assaulted and strangled her.[196] In 2019, it was reported that major phone companies sold access to

---

[193] Brian Pia, *Domestic Violence Victim Speaks Out Against Online Data Brokers*, ABC 33/40 News (Oct. 27, 2017), https://abc3340.com/news/abc-3340-news-iteam/domestic-violence-victim-speaks-out-against-online-data-brokers ("'Well, it's a very dangerous situation that puts victims and survivors in imminent danger,' Nunn said. 'Because that information is out there on various public websites, or those that you can pay a fee and obtain information.'").

[194] *The Location Privacy Protection Act of 2014: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 113th Cong. 6 (2014), https://www.govinfo.gov/content/pkg/CHRG-113shrg97739/pdf/CHRG-113shrg97739.pdf (Statement of Jessica Rich, Director, Bureau of Consumer Protection, Federal Trade Commission) ("At the same time, the increasing collection, use, and disclosure of this data presents serious privacy concerns. For this reason, the Commission considers precise geolocation data to be sensitive, warranting opt-in consent prior to collection from a consumer's mobile device. Why is this data so sensitive? A device's geolocation can reveal consumers' movements in real time and over time and, thus, divulge intimate personal details about them, such as the doctor's office they visit, how often they go, their place of worship, and when and what route their kids walk to school in the morning and return home in the afternoon. This data can be accessed and used in many ways consumers do not expect, for example, collected through stalking apps, sold to third parties for unspecified uses, paired with other data to build detailed profiles of consumers' activities, or stolen by hackers. The risks to consumer range from unwanted tracking to threats to personal safety.").

[195] *Id.*

[196] *Id.* at 2 ("The Minnesota Coalition for Battered Women submitted testimony about a northern Minnesota woman who was the victim of domestic violence—and the victim of one of these stalking apps. This victim had decided to get help. And so she went to a domestic violence program located in a county building. She got to the building, and within 5 minutes, she got a text from her abuser asking her why she was in the county building. The woman was terrified. And so an advocate took her to the courthouse to get a restraining order. As soon as she filed for the order, she got a second text from her abuser asking her why she was at the county courthouse and whether she was getting a restraining order against him. They later figured out that she was being tracked through a stalking app installed in her phone. This does not just happen in Minnesota. A national study conducted by the National Network to End Domestic Violence found that 72 percent of victim services programs across the country had seen victims who were tracked through a stalking app or a standalone GPS

their customers' location data, "and that data is ending up in the hands of bounty hunters and others not authorized to possess it, letting them track most phones in the country."[197] A bad actor does not need to install a stalkerware app or device or place a GPS tracking device on their victim's car to locate them in real time. Instead, a bad actor needs only to purchase data from a telecom company or data broker directly. This poses a unique threat to the physical safety and wellbeing of individuals.

Another out-of-context secondary use of personal data that causes substantial injury is the sale of data to law enforcement without a warrant or other legal predicate. Unlike private companies, these agencies use personal data to enable their exercise of coercive power—including the ability to track, arrest, deport, incarcerate, and even use lethal force.[198] It is for precisely this reason that law enforcement authorities' ability to collect personal data has been traditionally bound by constitutional restraints like the Fourth Amendment's warrant requirement or

---

device. Without objection, I will add to the record the accounts of a few other victims. Here is one from a victim in Illinois. She was living in Kansas with her abuser. She fled to Elgin, Illinois, a town three States away. She did not know that the whole time her cell phone was transmitting her precise location to her abuser. He drove the 700 miles to Elgin. He tracked her to a shelter and then to the home of her friend, where he assaulted her and tried to strangle her. Here is one from a victim in Scottsdale, Arizona. Her husband and she were going through a divorce. Her husband tracked her for over a month through her cell phone. Eventually, he murdered their two children in a rage.").

[197] Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Vice (Jan. 8, 2019), https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile (Although many users may be unaware of the practice, telecom companies in the United States sell access to their customers' location data to other companies, called location aggregators, who then sell it to specific clients and industries. Last year, one location aggregator called LocationSmart faced harsh criticism for selling data that ultimately ended up in the hands of Securus, a company which provided phone tracking to low level enforcement without requiring a warrant. LocationSmart also exposed the very data it was selling through a buggy website panel, meaning anyone could geolocate nearly any phone in the United States at a click of a mouse.").

[198] *See* Dana Khabbaz, EPIC, *DHS's Data Reservoir: ICE and CBP's Capture and Circulation of Location Information* 9–20 (2022), https://epic.org/wp-content/uploads/2022/08/DHS-Data-Reservoir-Report-Aug2022.pdf (detailing how DHS uses location data surveillance tools to enable its operations).

statutory regimes like the Electronic Communications Privacy Act, the Stored Communications Act, or the Foreign Intelligence Surveillance Act.[199]

However, as private companies have stockpiled more personal data—and more invasive types of personal data—law enforcement authorities have increasingly relied on the private sector as a conduit through which it can obtain information without traditional legal process.[200] While the Supreme Court has acknowledged the potential for total or near perfect surveillance using many of these types of personal data,[201] constitutional protections have been interpreted narrowly, only applying where the government *compels* disclosure of certain information, and therefore do not protect against scenarios where private companies either sell or otherwise voluntarily disclose information to law enforcement authorities.[202]

By enabling government authorities to circumvent these traditional restrictions, data brokers work to cause substantial injury to consumers and the public writ large. Government data purchases tend to amplify over-policing and further biased and discriminatory law enforcement.[203] Indeed, as EPIC has argued, when that surveillance and information dissemination targets already marginalized populations like immigrants and migrants, the consequences are all the graver—making these populations vulnerable to a disproportionate amount of policing,

---

[199] *See generally* [REDACTED] & [REDACTED], *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, Cong. Rsch. Serv. (Oct. 9, 2012), https://www.everycrsreport.com/files/20121009_98-326_0af79b3147e483f0ce3969fac1790b6794e34aab.pdf (reviewing in detail the framework governing government surveillance).

[200] *See* Khabbaz, *supra* note 198, at 5; Carey Shenkman et al., Ctr. Democracy & Tech., *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers* 36 (2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf.

[201] *Carpenter v. United States*, 138 S. Ct. 2206, 2210 (2018).

[202] *See* Elizabeth Goitein, *The Government Can't Seize Your Digital Data. Except by Buying It.*, Wash. Post (Apr. 26, 2021), https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/. Indeed, Congress has recognized the need to fix this loophole. The Fourth Amendment Is Not for Sale Act, S. 1265, 117th Cong. (2021), https://www.congress.gov/117/bills/s1265/BILLS-117s1265is.pdf. However, there is no indication that legislation is forthcoming.

[203] *See generally* Laura Moy, *A Taxonomy of Police Technology's Racial Inequity Problems*, 2021 U. Ill. L. Rev. 139, 142–43 (2021) (detailing a taxonomy of the ways in which the introduction of a new technology replicates, masks, transfers, and exacerbates inequity in the context of policing).

confinement, and control.[204] Further, government purchases of particular types of data—such as data from facial recognition tools—raise serious civil rights concerns, including misidentification of people of color for crimes with which they have no association.[205] As state governments pass strict anti-abortion legislation, the harms arising from government data purchases will only grow.[206]

Finally, government data purchases enable abusive policing practices. Law enforcement, military, and intelligence agency employees have repeatedly been found to abuse their access to government databases for personal reasons, including stalking romantic partners, business associates, journalists, and others.[207] The same is true where these agencies have purchased data from the private sector without any legal process. For example:

- Several law enforcement officers used their access to a law enforcement tool operated by Securus Technologies to track individuals they knew—including other officers, acquaintances, and a judge—using cell phone location data.[208]
- Bryan Wilson, a former Louisville police officer, used his law enforcement access to Accurint, a data-combing software, to obtain personal data of young

---

[204] Khabbaz, *supra* note 198, at 36.
[205] *See* Nicol Turner Lee & Caitlin Chin, *Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color*, Brookings Inst. (Apr. 12, 2022), https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ ("When disparate accuracy rates in facial recognition technology intersect with the effects of bias in certain policing practices, Black and other people of color are at greater risk of misidentification for a crime that they have no affiliation with.").
[206] *See* Sara Geoghegan & Dana Khabbaz, *Reproductive Privacy in the Age of Surveillance Capitalism*, EPIC (July 7, 2022), https://epic.org/reproductive-privacy-in-the-age-of-surveillance-capitalism/ ("Police and government agencies today have unprecedented access to sophisticated and invasive surveillance tools that they can use to enforce abortion bans.").
[207] *See* Alina Selyukh, *NSA Staff Used Spy Tools on Spouses, Ex-lovers: Watchdog*, Reuters (Sept. 27, 2013), https://www.reuters.com/article/us-usa-surveillance-watchdog/nsa-staff-used-spy-tools-on-spouses-ex-lovers-watchdog-idUSBRE98Q14G20130927; Sadie Gurman, *Across US, Police Officers Abuse Confidential Databases*, Associated Press (Sept. 28, 2016), https://apnews.com/article/699236946e3140659fff8a2362e16f43; Sam Stanton et al., *Hundreds of California Police Misuse Law Enforcement Computer Databases, Investigation Shows*, Sacramento Bee (Nov. 13, 2019), https://www.desertsun.com/story/news/2019/11/13/california-police-misuse-law-enforcement-databases-computers/2509747001/.
[208] *See* Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. Times (May 10, 2018), https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html; Suzanne Smalley, *U.S. Marshal Used Controversial Cell Phone Location Service to Illegally Access Data, DOJ Says*, CyberScoop (June 14, 2022), https://www.cyberscoop.com/us-marshal-cell-phone-location-data-charged-securus/.

> women.[209] Wilson then passed that information to a hacker who would hack into the women's private Snapchat accounts to obtain sexually explicit photos and videos.[210] Wilson would then threaten the young women with disclosure of those photos and videos unless the young women provided him with more sexually explicit material.[211]

Without significant guardrails governing the collection and use of personal data, these patterns of abuse will only continue.

The average consumer cannot reasonably avoid businesses that engage in harmful out-of-context secondary uses of their personal data. Data collection is an integral part of the systems that enable consumers to browse websites and interact with online services and mobile apps. The underlying data collection and processing mechanisms are not controlled by or even visible to the average user. As long as businesses are only collecting the data necessary to provide consumers with the goods and services they have requested, that invisible data processing is not generally a cause for concern. But the average consumer has no way to control what data businesses collect about them as they browse the web or use mobile apps, and they certainly do not have a way to prevent those businesses from selling that data once they have collected it or using it for out-of-context secondary purposes like profiling and targeting.

Indeed, the only way that the average user today could "avoid" most of the tracking and profiling of their searches, site visits, use of apps, and purchases would be to stop using internet connected devices altogether. But in 2022 it is not at all reasonable to suggest that a consumer can avoid using connected apps and services. Indeed, 90% of consumers said that the internet was "essential or important" during first year of pandemic,[212] and the average consumer spends nearly seven hours

---

[209] Josh Wood, *Feds: Ex Louisville Police Officer Used Law Enforcement Tech To Help Hack Sexually Explicit Photos From Women*, LEO Weekly (Oct. 12, 2022), https://www.leoweekly.com/2022/10/feds-ex-louisville-police-officer-used-law-enforcement-tech-to-help-hack-sexually-explicit-photos-from-women/.
[210] *Id.*
[211] *Id.*
[212] Colleen McClain et al., *The Internet and the Pandemic*, Pew Rsch. Ctr. (Sept. 1, 2021), https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/.

online daily.[213] A 2021 Commission report found that one ISP alone had 370 million consumer relationships and that another ISP served one trillion ad requests monthly.[214] A 2021 report showed that 85% of Americans owned a smartphone, an increase from 35% in 2011.[215] That statistic is likely even higher now as the COVID-19 pandemic has driven increased adoption of connected devices like smartphones.

Not only is internet use ubiquitous, it is essential to activities and interactions that are necessary in our modern society. Education, checking one's voter registration, employment, housing, banking, insurance, and other vital civic actions may all take place online. For example, each child needs to attend school to obtain an education, and internet use plays an important role in learning. It has been reported that "[e]ven though the vast majority of students are back to attending school in person, they still need reliable home internet to fully participate in their education, whether it be completing homework assignments, getting virtual tutoring, or attending remote classes during inclement weather."[216] Similarly, internet use in the employment context is widespread and, in many cases, an essential part of working or seeking work. In a 2017, the U.S. Bureau of Labor Statistics stated that the online job search was "the most popular method of jobhunting,"[217] and it is likely dramatically more popular in 2022 given increased digitization of services during the COVID-19 pandemic. Employment is a vital part

---

[213] Simon Kemp, *Digital 2021 April Global Statshot Report*, Data Reportal (Apr. 21, 2021), https://datareportal.com/reports/digital-2021-april-global-statshot.
[214] FTC, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers* 33 (2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacypractices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.
[215] *Mobile Fact Sheet*, Pew Rsch. Ctr. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/.
[216] Arianna Prothero, *Fewer Districts Are Providing Home Internet Access, But Students Still Need It*, EducationWeek (Sept. 30, 2022) https://www.edweek.org/technology/fewer-districts-are-providing-home-internet-access-but-students-still-need-it/2022/09.
[217] Richard Hernandez, *Online Job Search: The New Normal*, U.S. Bureau of Lab. Monthly Lab. Rev. (Feb. 2017), https://www.bls.gov/opub/mlr/2017/beyond-bls/pdf/online-job-search-the-new-normal.pdf ("As more households acquired Internet access, more jobseekers began primarily performing job searches online. In 2000, 25.5 percent of unemployed jobseekers used the Internet to search for a job. That figure rose to 76.3 percent in 2011, as more individuals gained access to the Internet at home (39.4 percent in 2000 compared with 71.0 percent in 2011). Jobseekers using OJS in 2011 had about a 25 percent greater chance of finding a job within a year than jobseekers who used traditional methods in 2000.").

of participating in our society, and the average consumer cannot avoid unfair data collection if they need to apply for a job online.

There are countless ways that consumers rely on online services such as search engines, blogs, forums, reservation portals, and other sites and apps to carry out their daily tasks. And consumers should not subject to unwanted commercial surveillance in the course of these day-to-day activities. For example:

COMMERCIAL SURVEILLANCE AT WORK

A woman applies online to a job located in Washington, DC. from her home in Chicago, IL. She receives an offer and moves to Washington, DC but is unfamiliar with the city. She will likely research neighborhoods online and apply for her apartment online. As soon as she searches, she receives advertisements for airline tickets for a trip to DC and other destinations—this in an out of context use. She will continue to see these advertisements after she has signed her lease and moved.

Perhaps she needs a physician in the area and searches for a local provider online using a healthcare search site. She might reasonably assume that everything she searches for on the healthcare search site will be protected and limited in the same way as her interactions with her doctor would be, but unbeknownst to her that site only complies with stricter health privacy requirements for data collected as part of providing specific services to a healthcare provider.[218] In reality, the healthcare search site discloses information about her device, her geolocation data, her contact information, her demographics, and her searches for healthcare providers to "ad networks" and "analytics partners." She can then be targeted and profiled by these unknown third-party businesses, which is an out-of-context secondary use of her sensitive personal information.

Many basic and necessary tasks require internet use. On any given day, a consumer might need to apply for her library card, buy new furniture, or email her mother. These simple activities, which are necessary for her to fully participate in our economy and society, require her to use online services or apps, which in turn means that her data will be collected and used in out-of-context ways. Many public benefits and programs also increasingly rely on digitized services. A consumer cannot reasonably work, travel, learn, interact with local government services, or participate in the economy without the internet. In 2022, people attend weddings,

[218] *See, e.g.*, ZocDoc, *Privacy Policy* (Jan. 27, 2022), https://www.zocdoc.com/about/privacypolicy.

funerals, and religious events and connect with loved ones on the internet. One should not have to choose between attending such personal events and having their privacy protected.

Many companies will likely argue that consumers should install special software or individually configure "privacy" settings on websites to prevent the collection of information that they do not want to be used. But it is critical that the Commission analyze the proposed rulemaking from the perspective of the average internet user, not the most technology savvy user with unlimited time to spend learning about ways they might be able to block certain tracking. It is the businesses who wish to collect and process personal data that should bear the burden of ensuring that their data processing is minimized to what is necessary and proportionate to accomplish the primary processing purposes.

The average internet user does not understand how their devices operate or how they collect data. Often, consumers express a desire to protect their privacy, but consumers rarely understand the internet or data security well enough to do so. For example, 81% of Americans believe that the potential risks of data collection by companies outweigh the benefits, "78% of U.S. adults say they understand very little or nothing about what the government does with the data it collects, and 59% say the same about the data companies collect."[219] In 2017, Pew Research found that "Despite the risk-reducing impact of good cybersecurity habits and the prevalence of cyberattacks on institutions and individuals alike, . . . many Americans are unclear about some key cybersecurity topics, terms and concepts."[220]

---

[219] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Rsch. Ctr. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ ("But even as the public expresses worry about various aspects of their digital privacy, many Americans acknowledge that they are not always diligent about paying attention to the privacy policies and terms of service they regularly encounter.").

[220] Kenneth Olmstead & Aaron Smith, *What the Public Knows About Cybersecurity*, Pew Rsch. Ctr. (Mar. 22, 2017), https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/ ("Cybersecurity is a complicated and diverse subject, but these questions cover many of the general concepts and basic building blocks that cybersecurity experts stress are

It is particularly unreasonable for companies to argue that individuals should take steps to protect their privacy when these companies have shown that even they don't fully understand how their systems operate or where users' personal data is going. For example, Facebook engineers acknowledged earlier this year that the company does "not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.' And yet, this is exactly what regulators expect us to do, increasing our risk of mistakes and misrepresentation[.]"[221] If one of the largest tech companies in the world does not understand where consumer information goes or how they are using it, then the average internet user cannot reasonably be expected to understand those processes such that she may make an informed decision about them to protect her privacy. This underscores the harms caused by indefinite data retention periods. The Commission should require that companies only retain data as long as reasonably necessary to effectuate the purpose for which the data was collected, with certain limited exceptions.

The Commission should promulgate a rule that protects the average internet user, consistent with its mission. The Commission must protect all consumers, regardless of their tech or internet literacy. While there may be steps a sophisticated internet user may take to protect their privacy, a consumer should not have to understand the complicated internet ecosystem in order to prevent substantial privacy injuries. The Commission promulgated the Eyeglass Rule using its section 5 unfairness authority to protect all consumers who needed eyeglass prescriptions. Perhaps there were some consumers who received their prescriptions and were able to relay their prescription to an eyeglass maker without needing a copy of the

---

important for users to protect themselves online. However, the typical (median) respondent answered only five of these 13 knowledge questions correctly (with a mean of 5.5 correct answers). One-in-five (20%) answered more than eight questions accurately, and just 1% received a "perfect score" by correctly answering all 13 questions [. . . .] For instance, 39% of internet users are aware that internet service providers (ISPs) are able to see the sites their customers are visiting while utilizing the "private browsing" mode on their internet browsers. Private browsing mode only prevents the browser itself, and in some cases the user's computer or smartphone, from saving this information – it is still visible to the ISP. And one-third (33%) are aware that the letter "s" in a URL beginning with "https://" indicates that the traffic on that site is encrypted.").

[221] Franceschi-Bicchierai, *supra* note 172.

prescription, thus they did not *need* the Eyeglass Rule to protect them. However, the Commission upheld its mandate to protect all consumers, regardless of their level of understanding of optometry and eyeglass prescriptions. The Commission should similarly promulgate a rule that protects all consumers, regardless of their understanding of a complex digital ecosystem.

The harms from unfair secondary uses of personal data are not outweighed by countervailing benefits to consumers or competition. One of the fundamental principles of privacy and data protection law—recognized and enshrined in many international and global standards—is that processing should be limited to what is *necessary* to accomplish the purpose for which the data was collected and that any interference with privacy must be *proportionate* to the broader public interests at stake.[222] Applying this standard to secondary data uses would be consistent with the Commission's unfairness authority because uses that violate the necessary and proportionate standard would not offer countervailing benefits to consumers or competition that outweigh the injury to privacy caused by the processing.

There are certainly uses of personal data that do provide benefits to consumers, but most of them fall within the primary purpose for which the data was collected or are consistent with the context and reasonable expectations of the consumers. There are other routine uses of data, such as for fraud prevention, spam filtering, business administration, and product improvement that are clearly necessary to provide goods and services to consumers. And for other secondary uses of data, including those that arise in the business-to-business context, the question should be whether that processing is necessary to serve the interests of the individuals to whom the personal data pertains or, if not, whether the benefits of the processing are proportionate to the intrusion.

For example, an internal phone or e-mail directory at a large company contains the personal data of all of its employees, and processing is necessary to ensure that they can communicate with each other. This processing clearly benefits the individual employees even though they are not the "customers" of the service,

[222] *See, e.g.*, Org. of Am. States, *supra* note 96, at 37–38; Euro. Data Prot. Supervisor, *The EDPS Quick Guide to Necessity and Proportionality* (Jan. 28, 2020), https://edps.europa.eu/data-protection/our-work/publications/factsheets/edps-quick-guide-necessity-and-proportionality_en.

and the use of their names and contact details in this limited way is proportionate to any minor intrusion on their privacy caused by the collection. Other secondary uses limited to what data a business is legally obligated to process or disclose, or limited to what is necessary in emergency circumstances involving a bona fide risk to death or serious physical injury, are clearly proportionate given that the business has no choice but to fulfill those obligations. But it is still necessary to evaluate the extent to which the business retains personal information, because the improper retention of personal data beyond what is necessary can cause significant harm to consumers if the business is later subject to a legal order to disclose that information against the interests of the individual.

The more complicated secondary use cases to evaluate under the necessary and proportionate standard are those involving peer-reviewed scientific, historical, or other statistical research. Such research uses are typically in the public interest, but they are not necessary for the underlying purpose for which the consumer's data was processed; the question therefore turns on whether the public interest in the research outweighs the infringement of the individuals' privacy and, relatedly, the extent to which the use of personal data has been minimized to the greatest extent possible to fulfil the research purpose. Any unfairness rule limiting out-of-context secondary uses of data should account for these special categories of secondary uses and provide a framework for their evaluation.

Businesses involved in the commercial surveillance industry will likely argue that their ability to compete in that marketplace by collecting, buying, selling, and analyzing personal data benefits competition and should weigh against a strong privacy rule. But there is substantial evidence that, contrary to providing benefits to competition, the proliferation of consumer targeting and profiling has led to greater consolidation of power among a few large entities and has driven an expansion in invasive business practices that have also extracted an increasing amount from publishers and small businesses. When a handful of tech companies control most of the data and the ad space, there are few if any benefits to competition. The House Subcommittee on Antitrust, Commercial and Administrative Law of the Judiciary Committee found in its 2020 Report that "Over the past decade, the digital economy

has become highly concentrated and prone to monopolization."[223] For years, it was reported that Facebook and Google had a duopoly on internet ad revenue. In 2015, 65% of all ad revenue went to Google and Facebook, and the two companies alone accounted for 90% of the growth of the ad industry in 2016.[224] In its most recent annual report, the IAB reported that the top ten companies represented over three-quarters of digital ad revenue with their revenues approaching $150 billion. Some reports today consider the digital ad industry to be a triopoly with the marketshare dominated by the three tech giants: Google, Facebook, and Amazon, explaining that the triopoly "increased their share of the U.S. digital-ad market from 80% in 2019 to a range approaching 90% in 2020."[225] In contrast, "the rest of the online ad market is growing at a combined growth rate of 3% year-on-year in comparison[.]"[226] Facebook has long known this. Facebook's strategy to maintain its dominance by buying competitive startups or threats has worked.[227] "Platforms with market power can leverage their position into downstream or adjacent markets, giving themselves an advantage over potential competitors and undermining competition in those markets."[228]

Industry continues to argue that targeted advertising helps small businesses but the numbers say otherwise: the current online digital advertising industry, which relies on the vast overcollection of personal information and the proliferation

---

[223] Investigation of Competition in Digital Markets, *supra* note 133, at 11.
[224] Matthew Ingram, *How Google and Facebook Have Taken Over the Digital Ad Industry*, Fortune (Jan. 4, 2017), https://fortune.com/2017/01/04/google-facebook-ad-industry/.
[225] Keach Haggey & Suzanna Vranica, *How Covid-19 Supercharged the Advertising 'Triopoly' of Google, Facebook and Amazon*, Wall St. J. (Mar. 19, 2021), https://www.wsj.com/articles/how-covid-19-supercharged-the-advertising-triopoly-of-google-facebook-and-amazon-11616163738 ("The Big Three of digital advertising—Google, Facebook and Amazon—already dominated that sector going into 2020. The pandemic pushed them into command of the entire advertising economy. According to a provisional analysis by ad agency GroupM, the three tech titans for the first time collected the majority of all ad spending in the U.S. last year.").
[226] Seb Joseph & Ronan Shields, *The Rundown: Google, Meta and Amazon Are on Track to Absorb More than 50% of All Ad Money in 2022*, Digiday (Feb. 4, 2022), https://digiday.com/marketing/the-rundown-google-meta-and-amazon-are-on-track-to-absorb-more-than-50-of-all-ad-money-in-2022/.
[227] Investigation of Competition in Digital Markets, *supra* note 133, at 13 (citing Production from Facebook, to H. Comm. on the Judiciary, FB-HJC-ACAL-00067600 (Apr. 9, 2012), https://judiciary.house.gov/uploadedfiles/0006760000067601.pdf).
[228] Competition & Markets Authority, *Online Platforms and Digital Advertising* 56 (2020), https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf.

of out-of-context secondary uses, benefits a handful of tech companies at the expense of smaller companies, competition, and consumers. Facebook "considers competition within its own family of products to be more considerable than competition from any other firm."[229] As Accountable Tech explained in its petition for an unfair methods of competition rulemaking, "Because many digital markets are prone to "tipping"—whereby early competition is for the entirety of the market—dominant firms have gained access to massive user bases and self-perpetuating data advantages that provide high barriers to entry and easy leverage into adjacent markets."[230] Privacy protective measures that distribute market power are beneficial to competition; our current digital ad ecosystem is not. For example, privacy improves data markets.[231] Establishing data minimization standards will help all business, especially small businesses. Currently, big tech companies write off fines from privacy violations as the cost of doing business, a cost that small businesses cannot afford. Creating clear and consistent standards helps all businesses stay competitive.

It is also important to note that the Commission's unfairness standard requires an evaluation of countervailing benefits to *consumers or competition*, not benefits to businesses or their shareholders. Industry often argues that companies' profits benefit greatly from out of context secondary uses, especially from targeted advertising. Indeed, Facebook's effects on the market provide "strong tipping points in the social networking market that create competition for the market, rather than competition within the market."[232] The correct analysis does not focus on whether large companies may experience benefits from their harmful practices, but whether those practices provide benefits to consumers or competition such that they outweigh the harms that they cause. The Commission's standard analyzes whether

[229] Investigation of Competition in Digital Markets, *supra* note 133, at 13.
[230] Accountable Tech, *supra* note 102, at 4 (citing Investigation of Competition in Digital Markets, *supra* note 133, at 42–45).
[231] Berjon, *supra* note 103.
[232] Investigation of Competition in Digital Markets, *supra* note 133, at 13 (citing Production of Facebook, to Comm. on the Judiciary FB-HJC-ACAL-00111406 (Oct. 2018) (on file with Comm.) ("Facebook has high reach and time-spent in most countries. User growth is tracking internet growth: global reach is roughly stable.")).

there are benefits to consumers or competition that outweigh the harms to consumers—and it is clear there are none.

The practice of secondary, out-of-context data use is widespread and prevalent. There can be no question that the collection and use of consumers' personal data online for tracking, profiling, and other out-of-context secondary purposes is endemic in the digital ecosystem. Globally, Google has tracking reach on 80.3% of all websites.[233] News and e-commerce sites had an average of 12.9 and 9.1 trackers in 2020. And the Commission found in its earlier data report from 2014 that numerous companies are building profiles of nearly every consumer in the country.[234] The problem has only gotten worse in the last eight years, with reporters lamenting that "online and off, nearly every life choice you've made, every item you've purchased, or every website you've visited has been logged, categorized, and then entered in a spreadsheet to be sold off."[235]

Data brokers buy, use, sell, share, transfer, and retain personal information about consumers in ways that far exceed the scope of the original purpose for which the data was collected. Data brokers collect information whenever and wherever possible,[236] including from offline activities.[237] They are able to "create an accurate

---

[233] *Tracking The Trackers 2020: Web Tracking's Opaque Business Model Of Selling Users*, Ghostery (2020), https://www.ghostery.com/blog/tracking-the-trackers-2020-web-trackings-opaque-business-model-of-selling-users [https://web.archive.org/web/20220907090605/https://www.ghostery.com/blog/tracking-the-trackers-2020-web-trackings-opaque-business-model-of-selling-users]; *see Tracking the Trackers One Page*, Ghostery (2020), https://cdn.ghostery.com/website/wp-content/uploads/2020/12/10152106/TrackingTheTrackers2020.pdf.

[234] FTC Data Broker Report, *supra* note 138, at iv.

[235] Thorin Klosowski, *Big Companies Harvest Our Data. This Is Who They Think I Am.*, N.Y. Times (May 28, 2020), https://www.nytimes.com/wirecutter/blog/data-harvesting-by-companies/.

[236] *Id.* ("Data brokers are companies that collect and sell information about consumers to other data brokers or to individual companies. Data brokers collect information from everywhere they can, including public records, commercial sources, and Web browsing. They then collate that data into a profile.").

[237] Yael Grauer, *What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?*, Vice (Mar. 27, 2018), https://www.vice.com/en/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection ("There are data brokers that focus on marketing, such as Datalogix (owned by Oracle), or divisions or subsidiaries of companies like Experian and Equifax. They develop dossiers on individuals which can be used to tailor marketing. Data brokers typically place consumers in categories based on their age, ethnicity, education level, income, number of children, and interests. Companies purchase lists of names, email addresses, interests and offline activity to assist in soliciting or marketing to those individuals.").

profile of you, even when you try to minimize your online footprint"[238] due to the vast swaths of personal information that they obtain.

Along with this significant growth in the corporate surveillance industry—both in the scope of surveillance and the breadth and invasiveness of the types of personal data collected—there has been a significant expansion in the government's collection and use of personal information supplied by data brokers. For example:

- The U.S. military has purchased access to X-Mode, which runs an SDK that is embedded in apps targeting Muslims.[239]
- ICE, Customs and Border Protection, the Federal Bureau of Investigation, and the Drug Enforcement Administration have all purchased access to Venntel, which aggregates location data from 80,000 apps, including X-Mode apps.[240]
- Law enforcement authorities across the country have used a tool called FogReveal to track cell phones through time using unique advertising IDs.[241]

The largest data brokers offer products that merge live location tracking and social media surveillance to offer comprehensive surveillance packages.[242] These partnerships with law enforcement, military, and intelligence authorities are so pervasive precisely because they offer law enforcement agencies the opportunity to circumvent the warrant requirement by purchasing that data.

Out-of-context secondary data uses are a widespread and prevalent practice, long recognized by the Commission as harming millions of consumers. The Commission recently imposed a $150 million civil penalty on Twitter for its

---

[238] Klosowksi, *supra* note 235.
[239] Cox, *supra* note 191.
[240] Hamed Aleaziz & Caroline Haskins, *DHS Authorities Are Buying Moment-By-Moment Geolocation Cellphone Data To Track People*, Buzzfeed News (Oct. 30, 2020), https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation; Joseph Cox, *How an ICE Contractor Tracks Phones Around the World*, Vice (Dec. 3, 2020), https://www.vice.com/en/article/epdpdm/ice-dhs-fbi-location-data-venntel-apps; Joseph Cox, *The DEA Abruptly Cut Off Its App Location Data Contract*, Vice (Dec. 7, 2020), https://www.vice.com/en/article/z3v3yy/dea-venntel-location-data.
[241] Garance Burke & Jason Dearen, *Tech Tool Offers Police 'Mass Surveillance on a Budget'*, Associated Press (Sept. 2, 2022), https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef.
[242] Sam Biddle & Jack Poulson, *American Phone Tracking Firm Demo'd Surveillance Powers by Spying on CIA and NSA*, Intercept (Apr. 22, 2022), https://theintercept.com/2022/04/22/anomaly-six-phonetracking-zignal-surveillance-cia-nsa/.

violations of an earlier consent decree, "alleging that Twitter violated the order in the earlier case by collecting customers' personal information for the stated purpose of security and then exploiting it commercially."[243] The case follows Twitter's long history of collecting consumers' personal information for one stated purpose and using it for another. Twitter purported to collect users' personal information, including phone numbers and email addresses, for security purposes, like two factor authentication or password recovery. Twitter then used the personal information to allow advertisers to target ads to specific users by linking information with information that they had obtained from data brokers.[244] From 2014 to 2019, 140 million users' personal information was collected for security purposes and ultimately used for commercial purposes. These harmful practices are widespread and affect millions of consumers.

The Commission should hold that it is an unfair trade practice to collect, use, transfer, or retain personal data beyond what is reasonably necessary and proportionate to the primary purpose for which it was collected, consistent with consumer expectations and the context in which the data was collected. This rule is necessary to prevent substantial injuries to consumers from the unrestricted collection and invasive secondary uses of their data by a wide range of entities including data brokers, targeted advertising firms, and other entities facilitating commercial surveillance. It is not possible for consumers to avoid these harmful practices because the generation and collection of their personal data is necessary to use connected services and apps, to browse the internet, and even to engage in routine financial transactions, work, and personal interactions. The improper extraction and use of personal data to target and profile consumers is a widespread problem in the online ecosystem that should be addressed through a Trade Regulation Rule. And the rule can be scoped to enable practices that provide

[243] Lesley Fair, *Twitter to Pay $150 Million Penalty for Allegedly Breaking Its Privacy Promises – Again*, FTC Bus. Blog (May 25, 2022), https://www.ftc.gov/business-guidance/blog/2022/05/twitter-pay-150-million-penalty-allegedly-breaking-its-privacy-promises-again.
[244] Complaint for Civil Penalties, Permanent Injunction, Monetary Relief, and Other Equitable Relief, *In re Twitter, Inc.*, FTC File No. 202-30623 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023062C4316TwitterOrderReopeningProceedings.pdf.

benefits to consumers and competition by applying the necessary and proportionate standard to ensure that data is properly minimized.

It is important that the Commission's rule reflect the reality that the average consumer is not able to "avoid" these harmful business practices by engaging in a technological arms race with the entities that seek to target and profile them. The fact that some consumers could install or use special software to block tracking ads does not mean that commercial surveillance is "reasonably avoidable" to the average consumer. And in order to distinguish between "primary" and "secondary" uses of data, it is also important to evaluate the purpose for which data was collected from the perspective of what the average consumer would expect given the context. For example, the Commission can distinguish between uses of data to personalize recommendations for goods or products within an app or service from the use of that same data to create a profile of consumers' browsing habits and activities over time to target the consumer with ads or other messages based on that profile. Without a rule prohibiting these commercial surveillance practices, consumers' personal data will continue to be misused, and the use of commercial surveillance techniques will continue to expand unchecked in ways that undermine consumer trust and autonomy and harm our society writ large.

2. AUTOMATED DECISION-MAKING SYSTEMS

Responsive to questions 53–60.

EPIC urges the Commission to declare that it is an unfair and deceptive practice to use an automated decision-making system implicating the interests of consumers without first demonstrating that it is effective, accurate, and free from impermissible bias; that it is an unfair and deceptive practice to use an automated decision-making system without providing adequate notice of such use; and that it is an unfair and deceptive practice to use one-to-many facial recognition or emotion detection technology.

2.1. It is an unfair and deceptive practice to use an automated decision-making system implicating the interests of consumers without first demonstrating that it is effective, accurate, and free from impermissible bias.

Responsive to questions 37, 38, 40, 47, 48, 53–65, 68, 70, 84, 86, 87, 89-91.

Commercial entities frequently use automated decision-making systems without substantiating the claims made about the systems, verifying the systems' accuracy, or evaluating the systems for disparate impact. These systems, which include a broad range of statistical and machine-learning tools that perform operations on data to aid or replace human decision-making, cause substantial injury to consumers when used without proper disclosure and oversight. As Commissioner Slaughter has written, companies "must bear the responsibility of (1) conducting regular audits and impact assessments and (2) facilitating appropriate redress for erroneous or unfair algorithmic decisions."[245] Businesses should be compelled to regularly conduct risk assessments that consider the harms of authorized and unauthorized uses of personal data, including discrimination and disproportionate harms affecting particular populations. The Commission should declare that a failure to do so is an unfair practice.

The use of automated decision-making systems that have not undergone sufficient testing, oversight, and disclosure causes substantial injury. These systems can cause bodily harm, loss of liberty, loss of opportunity, financial harms, dignitary harms, and discrimination harms.[246]

Automated decision-making systems that are untested can lead to bodily harm. In 2020, Epic Health Systems marketed the Epic Sepsis Model as an algorithm that can predict when patients are experiencing sepsis—a life-threatening emergency. The model, which uses statistical models to predict details about sepsis

[245] Rebecca Kelly Slaughter et al., *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission*, 23 Yale J.L. & Tech 1, 51 (2021).
[246] *See* Citron & Solove, *supra* note 18, at 855; Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. Mach. Learning Rsch. 1 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

in patients,[247] was adopted widely by hospitals throughout the country and marketed as 76–83% accurate. But when validated independently, the system's accuracy was shown to be significantly lower. In a study of over 27,000 patients in a Michigan Hospital, researchers found that the Epic Sepsis Model's prediction was closer to 63% accurate—and that there was significant "alert fatigue" among hospital staff because the tool generated alarming results for 18% of all hospital patients (most of which turned out not to have sepsis) while failing to identify risk in 67% of the total patients that actually experienced sepsis.[248] In this case, the use of an automated decision making system that was not properly validated could have (and indeed, may have) caused physical harm to individuals, as health care workers relied on the system to identify sepsis rather than employing traditional methods.

Similarly, a recent study of health records from 57,000 people found that an algorithm used in determining eligibility and prioritization for kidney transplants unfairly prevented Black patients from receiving transplants:[249]

> One third of Black patients, more than 700 people, would have been placed into a more severe category of kidney disease if their kidney function had been estimated using the same formula as for white patients. . . . In 64 cases, patients' recalculated scores would have qualified them for a kidney transplant wait list. None had been referred or evaluated for transplant, suggesting that doctors did not question the race-based recommendations.[250]

---

[247] Hannah Mitchell, *Epic's sepsis model used at 100+ hospitals has conflicting results: 6 things to know*, Becker's Health IT Rev. (Sept. 14, 2021), https://www.beckershospitalreview.com/ehrs/epic-s-sepsis-model-used-at-100-hospitals-has-conflicting-results-6-things-to-know.html; *see also* Heather Landi, *Olive rakes in $400M to turbocharge growth of 'humanized' AI for healthcare*, Fierce Healthcare (July 1, 2021), https://www.fiercehealthcare.com/tech/olive-rakes-400m-to-turbocharge-growth-humanized-ai-for-healthcare; Tyler Buchanan & Erin Brodwin, *Local Health Tech Startup Olive Overpromises*, Axios (Apr. 7, 2022), https://www.axios.com/local/columbus/2022/04/07/local-health-tech-startup-olive-overpromises.

[248] Andrew Wong et al., *External Validation of a Widely Implemented Proprietary Sepsis Prediction Model in Hospitalized Patients*, 181(8) JAMA Intern Med. 1065 (June 2021), https://pubmed.ncbi.nlm.nih.gov/34152373/.

[249] Tom Simonite, *How an algorithm blocked kidney transplants to Black patients*, Wired (Oct. 26, 2020), https://www.wired.com/story/how-algorithm-blocked-kidney-transplants-black-patients/.

[250] *Id.*

Untested systems, or systems that have not proven to be highly accurate, simply should not be implemented in the health care sector or similarly consequential settings. Our lives should not depend on the result of an unproven algorithm.

Automated decision-making systems can also force consumers to restrict or regulate their behavior to conform to a system's expectations, leading to a loss of liberty. For example, students are subjected to unavoidable automated decision-making and analysis on a daily basis, including through surveillance, exam monitoring, and communications screening on school-mandated laptops.[251] Automated exam monitoring and proctoring systems provided by vendors like Respondus,[252] ProctorU,[253] Proctorio,[254] Examity,[255] and Honorlock,[256] in particular, have been adopted by a wide range of educational institutions. According to the systems' vendors, these automated decision-making systems can accurately detect indicators of cheating by tracking factors like student speech, eye movements, mouse clicks, and pacing.[257] In reality, these systems are prone to bias[258] and error,[259] placing students' academic standing in jeopardy. For example, this past February, a Florida teenager was flagged for potential cheating by Honorlock's automated proctoring system when she looked away from her screen during a test.[260] As a result, the student received a zero on the exam.[261] These intrusive monitoring

---

[251] Charlie Warzel, *Welcome to the K-12 Surveillance State*, N.Y. Times (July 2, 2019), https://www.nytimes.com/2019/07/02/opinion/surveillance-state-schools.html.
[252] *Who We Are,* Respondus (2020), https://web.respondus.com/.
[253] *Protect Any Online Exam*, ProctorU (2020), https://www.proctoru.com/; *see also* Drew Harwell, *Mass School Closures in the Wake of the Coronavirus are Driving a New wave of Student Surveillance*, Wash. Post (Apr. 1, 2020), https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/.
[254] *Exam Monitoring*, Proctorio (2020), https://proctorio.com/platform/exam-monitoring.
[255] *Automated Proctoring*, Examity (2020), https://www.examity.com/#.
[256] *Honorlock*, Honorlock (2020), https://honorlock.com/.
[257] *See* Harwell, *supra* note 253.
[258] *See* Mitchell Clark, *Students of Color Are Getting Flagged to Their Teachers Because Testing Software Can't See Them*, Verge (Apr. 8, 2021), https://www.theverge.com/2021/4/8/22374386/proctorio-racial-bias-issues-opencv-facial-detection-schools-tests-remote-learning.
[259] *Cf.* Drew Harwell, *Cheating-detection Companies Made Millions During the Pandemic. Now Students are Fighting Back*, Wash. Post (Nov. 12, 2020), https://www.washingtonpost.com/technology/2020/11/12/test-monitoring-student-revolt/.
[260] Kashmir Hill, *Accused of Cheating by an Algorithm, and a Professor She Had Never Met*, N.Y. Times (May 27, 2022), https://www.nytimes.com/2022/05/27/technology/college-students-cheating-software-honorlock.html.
[261] *Id.*

systems, like other commercial surveillance technologies, can force students to carefully regulate how they act in order to avoid an adverse automated decision—even when their behavior is innocuous.

The use of untested and unproven automated decision-making systems can also lead to a loss of opportunity. HireVue is a service that uses a proprietary automated decision-making system to evaluate the fitness of job candidates based largely vocal patterns (and previously on video analysis). In 2020, EPIC filed an FTC complaint highlighting the unfairness of HireVue's screening practices.[262] When a job candidate seeks employment at a company that uses HireVue's algorithmic assessment services, HireVue administers an automated interview and/or an online "game-based challenge[]" to the candidate.[263] HireVue collects "tens of thousands of data points"[264] from each interview and a "rich and complex" array of data from each "psychometric game[.]"[265] HireVue then inputs these personal data points into "predictive algorithms"[266] that allegedly determine each job candidate's "employability," "cognitive ability," "psychological traits," "emotional intelligence," and "social aptitudes."[267] But HireVue does not give candidates access to the training data, factors, logic, or techniques used to generate each algorithmic assessment. In some cases, even HireVue is unaware of the basis for an assessment.[268]

RentGrow, like many tenant-screening companies, first generates reports by collecting data like past eviction information, credit scores, and criminal records of all members of an applicant's household, then recommends who should be rejected. In theory, these factors may be legal bases to screen housing applicants. In practice, landlords can use these factors as proxies for criteria that are illegal to consider, such

---

[262] EPIC HireVue Complaint, *supra* note 6.
[263] *Id.*
[264] *How to Prepare for Your HireVue Assessment*, HireVue (Apr. 16, 2019), https://www.hirevue.com/blog/how-to-prepare-for-your-hirevue-assessment; Nathan Mondragon et al., HireVue, *The Next Generation of Assessments* 6 (2019).
[265] Mondragon et al., *supra* note 264, at 5.
[266] *Id.* at 7.
[267] HireVue, *supra* note 264; Mondragon et al., *supra* note 264, at 6.
[268] Drew Harwell, *A face-scanning algorithm increasingly decides whether you deserve the job*, Wash. Post (Oct. 25, 2019), https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

as race, familial status, and age. Scholars including Dr. Safiya Noble have called this process "technological redlining," wherein racial, cultural, and economic inequities are perpetuated by technology.[269] For example, automated systems that reject applicants based on criminal records, poor rental payment histories, or a history of eviction can unfairly disadvantage people of color, victims of domestic violence, and people with disabilities.[270] Black people, specifically, are overpoliced, over-evicted, and tend to rely most heavily on of housing assistance programs.[271]

RentGrow's tenant screening services perpetuate housing inequality by giving landlords what appears to be an objective basis for rejecting applicants, even when the information underlying the company's reports reflects historical bias and injustice. Even if RentGrow excludes factors like race its screening reports, the company can still use proxy variables like ZIP codes.[272] Because the United States is deeply segregated, a ZIP code is a reliable proxy for race.[273]

Untested and unproven automated systems can also cause financial harm. Upstart, a financial entity that offers student loan refinancing, offered the allure of loan decisions based on "alternative data," a term used to describe data outside the scope of information normally in loan decisions.[274] But Upstart was found to have discriminated based on individuals that attended Historically Black Colleges and Universities, assigning them higher interest rates. This case, which was ultimately

---

[269] *See* Noble, *supra* note 3, at 1.
[270] Lydia X. Z. Brown, *Tenant Screening Algorithms Enable Racial and Disability Discrimination at Scale, and Contribute to Broader Patterns of Injustice*, Ctr. for Democracy & Tech. (July 7, 2021), https://perma.cc/L4ST-6C8D.
[271] *See, e.g.*, Brian J. McCabe & Eva Rosen, *Eviction in Washington D.C.: Racial and Geographic Disparities in Housing Instability* 7, 22 (2020), https://perma.cc/4DWW-VMDC. More than 90% of the Housing Choice Vouchers in D.C. are used by Black families. *See* U.S. Dep't of Hous. & Urb. Dev., *Assisted Housing: National and Local–Picture of Subsidized Households* (2020), https://perma.cc/5MM3-CHHD.
[272] Anya E.R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 Iowa L. Rev. 1257 (2020), https://perma.cc/SC2T-8RHN.
[273] Devin G. Pope & Justin R. Sydnor, *Implementing Anti-Discrimination Policies in Statistical Profiling Models*, 3 Am. Econ. J. Econ. Pol'y 206, 209 (2011), https://perma.cc/EG84-SPNB.
[274] Press Release, NAACP Legal Def. & Educ. Fund, *NAACP Legal Defense and Educational Fund and Student Borrower Protection Center Announce Fair Lending Testing Agreement with Upstart Network* (Dec. 1, 2020), https://www.naacpldf.org/press-release/naacp-legal-defense-and-educational-fund-and-student-borrower-protection-center-announce-fair-lending-testing-agreement-with-upstart-network/.

addressed through a monitorship settlement, illustrates the danger of deploying algorithms to make critical individualized decisions without adequate testing or transparency.

Automated decision-making systems can also cause or exacerbate less tangible consumer harms like reputational harms and harms to consumer dignity. These dignitary harms occur when flaws or biases in automated decision-making systems negatively impact how consumers are treated by and compared to their peers—often in hidden and unavoidable ways. For example, in 2019, researchers reported that Twitter's content moderation algorithm was 1.5 times more likely to flag tweets written by Black users as offensive or hateful and 2.2 times more likely to flag tweets written in African-American Vernacular English (AAVE).[275] Content moderation algorithms and similar automated decision-making systems can perpetuate racial biases in ways that disproportionately subject Black users to greater scrutiny, restrict their ability to participate in moderated spaces, and limit their creative expression.

Automated decision-making systems can facilitate or exacerbate discrimination harms. Extensive research has established racial and gender bias in advertisement delivery on social media;[276] racial bias in prediction of healthcare needs that lead to black patients being underserved;[277] racial, ethnic, and gender bias

[275] Shirin Ghaffary, *The Algorithms that Detect Hate Speech Online are Biased Against Black People*, Vox (Aug. 15, 2019), https://www.vox.com/recode/2019/8/15/20806384/social-media-hate-speech-bias-black-african-american-facebook-twitter; *see also* Maarten Sap et al., *The Risk of Racial Bias in Hate Speech Detection*, Proc. 57th Ann. Meeting Ass'n for Comp. Ling. 1668 (Aug. 2, 2019), https://maartensap.com/pdfs/sap2019risk.pdf.

[276] *See, e.g.*, Muhammad Ali et al., *Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes*, arXiv (Apr. 3, 2019), https://arxiv.org/abs/1904.02095.

[277] U.S. Gov't Accountability Off., GAO-21-519SP, *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities* (2021), https://www.gao.gov/products/gao-21-519sp [hereinafter GAO AI Framework]; *see also* Ziad Obermeyer et al., *Dissecting racial bias in an algorithm used to manage the health of populations*, 366 Sci. 447 (2019), https://escholarship.org/content/qt6h92v832/qt6h92v832.pdf; Simonite, *supra* note 249.

in all parts of the job acquisition process from search[278] to resume screening[279] to interviewing; racial bias in interest rates for loan financing;[280] racial and gender bias in access to credit;[281] socioeconomic discrimination in grading algorithms;[282] and more.

Discrimination in automated decision-making systems persists regardless of the level of human involvement. In education, college counselors use automated systems to separate students based on algorithmic determinations of potential, thereby sorting and trapping some students in different tracks. For example, EAB's Navigate enables schools to "segment students" based on "demographic data, academic performance, and success indicators."[283] It uses historical academic and demographic data to create models that can predict and flag "at-risk students." Navigate allows schools to customize the factors considered by the predictive model, including allowing race to be considered a high-impact predictor. In an analysis of student risk data from large public universities, researchers found that Black students were deemed high-risk at up to four times the rate of White students.[284] Navigate's "major explorer" tool—software that helps students pick

---

[278] Amit Datta et al., *Automated Experiments and Privacy Settings: A Tale of Opacity, Choice, and Discrimination,* arXiv 17 (Mar. 18, 2015), https://arxiv.org/pdf/1408.6491.pdf; Sheridan Wall & Hilke Schellmann, *LinkedIn's job-matching AI was biased. The company's solution? More AI*, MIT Tech. Rev. (June 23, 2021), https://www.technologyreview.com/2021/06/23/1026825/linkedin-ai-bias-ziprecruiter-monster-artificial-intelligence/.

[279] Amani Carter & Rangita de Silva de Alwis, *Unmasking Coded Bias: Why We Need Inclusion and Equity in AI* 11 (2021), https://www.law.upenn.edu/live/files/11528-unmasking-coded-bias ("Evidence suggests resumes containing minority racial cues, such as a distinctively Black name[,] lead to thirty to fifty percent fewer callbacks from employers than do otherwise equivalent resumes without such cues.").

[280] NAACP Legal Def. & Educ. Fund, *supra* note 274.

[281] Genevieve Smith & Ishita Rustagi, *When Good Algorithms Go Sexist: Why and How to Advance AI Gender Equity*, Stan. Soc. Innovation Rev. (Mar. 31, 2021), https://ssir.org/articles/entry/when_good_algorithms_go_sexist_why_and_how_to_advance_ai_gender_equity.

[282] Daan Kolkman, *"F**k the algorithm?" What the world can learn from the UK's A-level grading fiasco*, London Sch. Econ. Impact Blog (Aug. 26, 2020), https://blogs.lse.ac.uk/impactofsocialsciences/2020/08/26/fk-the-algorithm-what-the-world-can-learn-from-the-uks-a-level-grading-fiasco/.

[283] *Navigate*, EAB, https://eab.com/products/navigate/ (last visited Nov. 21, 2022).

[284] Todd Feathers, *Major Universities Are Using Race as a "High Impact Predictor" of Student Success*, Markup (Mar. 2, 2021), https://themarkup.org/machine-learning/2021/03/02/major-universities-are-using-race-as-a-high-impact-predictor-of-student-success.

majors that suit their interests—has been found to recommend students from historically underrepresented communities exploring a major change to a different major where their "risk score" is lower.[285] And in response to an inability to test normally during the COVID-19 pandemic, school systems in the United Kingdom used a deeply flawed automated decision-making system to model out and assign grades based on a series of factors that "relied primarily on two pieces of information . . . the ranking of students within a school and their school's historical performance."[286] The results yielded disproportionate increases in grades for fee-paying private schools over state-funded public schools, which discriminated against students of lower socioeconomic status.[287]

Automated decision-making systems are unavoidable. They are used throughout the economy, from insurance to healthcare to video recommendation systems. Especially in the housing, health, hiring, and credit contexts, consumers are rarely aware when a company is using an automated decision-making system, let alone capable of avoiding that system.[288]

As the White House Office of Science and Technology Policy wrote in the introduction to its *Blueprint for an AI Bill of Rights*:

> In America and around the world, systems supposed to help with patient care have proven unsafe, ineffective, or biased. Algorithms used in hiring and credit decisions have been found to reflect and reproduce existing unwanted inequities or embed new harmful bias and discrimination. Unchecked social media data collection has been used to threaten people's opportunities, undermine their privacy, or pervasively track their activity—often without their knowledge or consent. These outcomes are deeply harmful—but they are not inevitable.

---

[285] *Help Students Pick The Right Major, Faster*, EAB (Mar. 26, 2018), https://eab.com/insights/daily-briefing/student-success/help-students-pick-the-right-major-faster/.
[286] Jon Porter, *UK ditches exam results generated by biased algorithm after student protests*, Verge (Aug. 17, 2020), https://www.theverge.com/2020/8/17/21372045/uk-a-level-results-algorithm-biased-coronavirus-covid-19-pandemic-university-applications.
[287] *Id.*
[288] *See* Ari Ezra Waldman, *Power, Process and Automated Decision-Making*, 88 Fordham L. Rev. 613, 615–16 (2019)("Using algorithms to make commercial and social decisions is really a story about power, the people who have it, and how it affects the rest of us.").

The scope of automated decision-making in employment screening is sweeping. HireVue—just one competitor in the employment screening field—has over 700 corporate customers, including major companies like Hilton, Ikea, Oracle, Dow Jones, Koch Industries, Unilever, Urban Outfitters, Carnival, Under Armour, Vodafone, Dunkin' Brands, Keurig, Dr Pepper, Cathay Pacific, AB InBev, HBO, Sequoia, Staples, BASF, CARFAX, CDW, Conoco Phillips, Panda Express, Penguin Random House, and Anheuser-Busch.[289] Nonprofits and public sector employers also use HireVue's assessment services, including Atlanta Public Schools and Thurgood Marshall College Fund.[290] Talview Inc., a competitor to HireVue, offers a similar suite of automated resume scanning, "AI video interviews with behavioral insights," and "[o]nline assessments."[291] And Affectiva, Inc. "analyzes human states in context," using "computer vision, speech analytics, deep learning and a lot of data."[292]

Students often cannot avoid the use of automated decision-making systems in schools. Educational institutions are increasingly using opaque algorithms to generate predictions about students and according differential treatment based on those predictions. Sometimes this can lead to improved outcomes, as when an at-risk student is identified and provided with the support they need to succeed. But it can also do the opposite, labeling a student as "at-risk" at a young age, leaving the student or their teachers to feel their fate is sealed, stunting educational progress, and limiting life opportunities for the student. The Markup reported this year that K-12 data warehousing giant PowerSchool, which claims to hold data on over 75% of K-12 students in North America,[293] provides tools to school districts that generate "predictions about whether students are at low, moderate, or high risk of not graduating high school on time, not meeting certain standards on the SATs, or not completing two years of college, among other outcomes" as early as the first

[289] *Customers*, HireVue (2019), https://www.hirevue.com/customers.
[290] *Id.*
[291] Talview (2020), https://www.talview.com/.
[292] Affectiva (2020), https://www.affectiva.com/.
[293] Press Release, PowerSchool, *PowerSchool Completes Acquisition of Naviance and Intersect Providing More Students with Greater Access to Personalized and Equitable Opportunities for Life After High School* (Mar. 3, 2021), https://www.powerschool.com/news/powerschool-and-naviance-and-intersect-close/.

grade.[294] Alarmingly, free and reduced lunch status and gender were among the factors most heavily weighted by PowerSchool.[295]

Businesses are regularly relying on biometric information, financial records, and other highly sensitive personal data to make individualized, automated decisions about consumers. Many of these automated processes are completely unknown to consumers, as in the secret collection and processing of billions of facial images by Clearview AI.[296] And even if consumers are notified that an automated decision-making system is in use, they are frequently given no explanation of the decisions made by that system and no meaningful opportunity to opt out. For example, many job applicants have little choice but to submit to HireVue's automated screening tool or else forgo an ever-growing list of employment opportunities.

The use of automated decision-making systems without disclosure and due diligence is not outweighed by countervailing benefits to consumers or competition.[297] When balancing the harms of a business practice against their countervailing benefits, the Commission considers only those benefits and harms that directly result from the business practice at issue.[298] Companies often tout the promise of automated decision-making as a way to improve consumers' lives, but the commercial use of automated systems is not a monolithic business practice. While the effects of automated decision-making vary widely across industry and context, the practice of using automated decision-making systems without proper disclosure and due diligence is widespread across industries. Therefore, the Commission need not balance the harms and benefits of automated decision-making

---

[294] Todd Feathers, *This Private Equity Firm Is Amassing Companies That Collect Data on America's Children*, Markup (June 11, 2022), https://themarkup.org/machine-learning/2022/01/11/this-private-equity-firm-is-amassing-companies-that-collect-data-on-americas-children.
[295] *Id.*
[296] *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[297] 15 U.S.C. § 45(n).
[298] *See* Beales, *supra* note 93; Maureen K. Ohlhausen, *Weigh the Label, Not the Tractor: What Goes on the Scale in an FTC Unfairness Cost-Benefit Analysis?*, 83 Geo. Wash. L. Rev. 1999, 2018–24 (2015), https://www.gwlr.org/wp-content/uploads/2016/01/83-Geo-Wash-L-Rev-1999.pdf.

writ large; it need only consider the practice of using automated decision-making systems without the requisite transparency and testing.

Using automated decision-making systems without proper disclosure and due diligence causes myriad harms to consumers. For example, improperly evaluated systems like the Epic Sepsis Model can cause serious bodily injury within hospitals,[299] and biased automated decision-making systems deployed across sectors—from education[300] to employment[301] to credit[302]—can facilitate or exacerbate discrimination in ways that harm consumers' earning potential and financial wellbeing.

In comparison, the countervailing benefits of implementing automated decision-making systems without first ensuring the systems are effective, accurate, and nondiscriminatory are minor. In fact, there appear to be only two: implementing automated decision-making systems more quickly and saving companies money. No reasonable consumer would contend that companies should affirmatively withhold key information about the effectiveness, accuracy, and potential bias of the automated decision-making systems that make determinations about them. No reasonable consumer would prefer to be subjected to ineffective, inaccurate, and biased systems so companies can profit. However, companies make these decisions for consumers every day, subjecting consumers to opaque and unreliable automated decision-making without sufficient disclosure and due diligence. As a result, companies undermine consumer trust in automated decision-making systems—systems that can provide significant social and economic benefits when properly developed and evaluated—and chill the development of more effective, accurate, and unbiased systems without producing meaningful benefits to consumers or competition.

The use of these systems without testing, oversight, and substantiation is also deceptive. By using an automated system to make individualized

---

[299] *See* Mitchell, *supra* note 247.
[300] *See Navigate*, EAB, https://eab.com/products/navigate/ (last visited Nov. 21, 2022); Kolkman, *supra* note 282.
[301] *See* Datta et al., *supra* note 278; Wall & Schellmann, *supra* note 278; Carter & de Silva de Alwis, *supra* note 279.
[302] *See* NAACP Legal Def. & Educ. Fund, *supra* note 274; Smith & Rustagi, *supra* note 281.

determinations about consumers, companies are implicitly warranting that the system is effective, accurate, fair, and nondiscriminatory.[303] If in fact the system is ineffective, inaccurate, unfair, or discriminatory, the use of that system is deceptive, and failure to disclose that fact constitutes a material omission. This type of deception can profoundly affect an individual's life, as seen in the example of the Epic Sepsis Model.

Commercial uses of automated decision-making systems without disclosure have become widespread and prevalent.[304] The uses of automated decision-making systems described above—though extensive and alarming—are merely the tip of the iceberg.[305] A 2019 Garner study found that the commercial use of automated decision-making systems had increased 270% in the preceding four years, with 37% of businesses using some form of the technology.[306] By other accounts, the scale of commercial automation is even greater. Nearly half of respondents in one survey reported that "their organizations have embedded at least one [automated decision-making system] into their standard business processes, while another 30 percent report piloting the use of [such systems]."[307] And the National Academies of Medicine, NIST, and the Consumer Financial Protection Bureau have documented the growing role of automated decision-making systems in medicine, banking, and the defense sector.[308]

---

[303] *Cf.* U.C.C. § 2-315 ("Where the seller at the time of contracting has reason to know any particular purpose for which the goods are required and that the buyer is relying on the seller's skill or judgment to select or furnish suitable goods, there is unless excluded or modified under the next section an implied warranty that the goods shall be fit for such purpose.").
[304] 15 U.S.C. § 57a(b)(3).
[305] *See* Waldman, *supra* note 288, at 615–22.
[306] Press Release, Gartner, *Gartner Survey Shows 37% of Organizations Have Implemented AI in Some Form* (Jan. 21, 2019), https://www.gartner.com/en/newsroom/press-releases/2019-01-21-gartner-survey-shows-37-percent-of-organizations-have.
[307] McKinsey & Co., *AI adoption advances, but foundational barriers remain* (Nov. 13, 2018), https://www.mckinsey.com/featured-insights/artificial-intelligence/ai-adoption-advances-but-foundational-barriers-remain.
[308] Nat'l Acad. of Med., *Artificial Intelligence in Health Care: The Hope, The Hype, the Promise, the Peril* (Michael Matheny et al. eds., 2019), https://nam.edu/wp-content/uploads/2019/12/AI-in-Health-Care-PREPUB-FINAL.pdf; Nat'l Inst. of Sci. & Tech., *AI: Using Standards to Mitigate Risks* 7 (May 20, 2019), https://www.nist.gov/system/files/documents/2019/05/20/nist-ai-rfi-dhs-001.pdf;

Moreover, the rapidly escalating scale of unfair automated decision-making systems makes it essential for the Commission to conduct a rulemaking rather than rely solely on case-by-case enforcement. By defining unfair and deceptive practices ex ante, and "with specificity,"[309] a trade regulation rule would "make it easier for the FTC to take action against" parties[310] that harm consumers through the use of automated systems. A rule on automated decision-making would also preclude arguments—like those raised by LabMD in response to the Commission's data security enforcement action—"that the Commission failed to provide fair notice"[311] concerning which practices are unfair and unlawful.

The omission of critical transparency and accountability mechanisms in the use of automated decision-making systems is prevalent. The frequency of deception surrounding the use of AI spurred a 2021 FTC blog post warning companies not to exaggerate the capabilities of their automated decision-making systems:

> Under the FTC Act, your statements to business customers and consumers alike must be truthful, non-deceptive, and backed up by evidence. In a rush to embrace new technology, be careful not to overpromise what your algorithm can deliver. For example, let's say an AI developer tells clients that its product will provide '100% unbiased hiring decisions,' but the algorithm was built with data that lacked racial or gender diversity. The result may be deception, discrimination—and an FTC law enforcement action.[312]

Professor Arvind Narayanan explains in *How to Recognize AI Snake Oil* that many companies call a system "AI" for marketing but are simply automating a

---

Consumer Fin. Prot. Bureau, *BCFP Collaborates With Regulators Around The World To Create Global Financial Innovation Network* (Aug. 7, 2018), https://www.consumerfinance.gov/about-us/newsroom/bcfp-collaborates-regulators-around-world-create-global-financial-innovation-network/.

[309] 15 U.S.C. § 57a(a)(1)(B).

[310] Press Release, FTC, *FTC Approves Final Amendments to its R-Value Rule for Home Insulation Products* (Oct. 28, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/ftc-approves-final-amendments-its-r-value-rule-home-insulation.

[311] *LabMD, Inc. v. FTC*, 894 F.3d 1221, 1227 (11th Cir. 2018).

[312] Elisa Jillson, *Aiming for truth, fairness, and equity in your company's use of AI*, FTC Bus. Blog (Apr. 19, 2021), https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

subjective judgment and passing it off as science-backed and objective.[313] Others, similarly, promise a given technological feat that research fundamentally refutes is possible—like emotion detection.[314] Others still simply assert inaccurate, incomplete, or misleading claims about capability, accuracy, or lack of bias. As Professors Citron and Pasquale have explained, "though automated scoring is pervasive and consequential, it is also opaque and lacking oversight."[315]

Currently, audits for both accuracy and bias are not common, consistent, or required, and there is no mandate to meet minimum thresholds or to correct inaccuracies or bias once found. Facebook and HireVue, two prominent technology companies with harmful automated decision-making systems, are illustrative of issues of with audits: (1) companies often only do them when they are forced to or after extensive harm has been publicized, and (2) companies perform insufficient or unacceptable audits.

In 2012, Facebook was ordered to have biennial independent third-party audits performed for twenty years as part of an FTC consent order.[316] These audits have not been made public in full, and Facebook was found to have violated the consent order in 2019.[317] In 2018, the company agreed to perform a civil rights audit following sustained pressure from Congress and over 100 civil rights organizations.[318] In analyzing the civil rights impact of Facebook's algorithms, the

---

[313] Arvind Narayanan, *How to Recognize AI Snake Oil,* Princeton Univ. Ctr. for Info. Tech. Pol'y, https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf (last visited Nov. 20, 2022).
[314] *See, e.g.*, Lisa Feldman Barrett et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements*, 20 Psych. Sci. Pub. Int. 1 (July 17, 2019), https://journals.sagepub.com/eprint/SAUES8UM69EN8TSMUGF9/full.
[315] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 1 (2014), http://www.datascienceassn.org/sites/default/files/The%20Scored%20Society%20-%20Due%20Process%20for%20Automated%20Predictions.pdf.
[316] Decision and Order, *In re Facebook, Inc.*, FTC File No. 092-3184 (2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.
[317] Press Release, FTC, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.
[318] *See* Facebook, *Facebook's Civil Rights Audit Report – Final Report* (2020), https://about.fb.com/wp-content/uploads/2020/07/Civil-Rights-Audit-Final-Report.pdf.

auditor's report explained that Facebook did not provide them with access to sufficient information to meaningfully perform an audit of their civil right impact:

> When it comes to Facebook's own algorithms and machine learning models, the Auditors cannot speak to the effectiveness of any of the pilots Facebook has launched to better identify and address potential sources of bias or discriminatory outcomes. (Both because the pilots are still in nascent stages and the Auditors have not had full access to the full details of these programs.) The Auditors do, however, credit Facebook for taking steps to explore ways to improve Facebook's AI infrastructure and develop processes designed to help spot and correct biases, skews, and inaccuracies in Facebook's models.[319]

Still, throughout the audit, the independent group of experts grew "concerned that [any] gains could be obscured by the vexing and heartbreaking decisions Facebook has made that represent significant setbacks for civil rights," and were left to repeatedly suggest that Facebook take civil rights concerns more seriously than it does.[320] Frances Haugen, a former Facebook employee, recently explained the danger of limited transparency and incomplete audits:

> Only Facebook knows how it personalizes your feed for you. It hides behind walls that keep the eyes of researchers and regulators from understanding the true dynamics of the system. When the tobacco companies claimed that filtered cigarettes were safer for consumers, it was possible for scientists to independently invalidate that marketing message and confirm that in fact they posed a greater threat to human health. But today we can't make this kind of independent assessment of Facebook. We have to just trust what Facebook says is true — and they have repeatedly proved that they do not deserve our blind faith…This inability to see into the actual systems of Facebook and confirm that Facebook's systems work like they say is like the Department of Transportation regulating cars by watching them drive down the highway. Imagine if no regulator could ride in a car, pump up its wheels, crash test a car, or even know that seat belts could exist. Facebook's regulators can see some of the problems—but they are kept blind to what is causing them and thus can't craft specific solutions. They cannot even access the company's own data on product safety, much less conduct an independent audit. How is the public supposed to assess if Facebook is

[319] *Id.* at 81.
[320] *Id.* at 8.

> resolving conflicts of interest in a way that is aligned with the public good if it has no visibility and no context into how Facebook really operates?[321]

In 2021, HireVue[322] announced that it had undergone two audits by third-party organizations but did not freely release the audits in full. The audits came after scrutiny about the company's use of opaque facial recognition and voice analysis in interview software, in part due to an EPIC FTC Complaint about these practices.[323] Although members of the public could access summaries of the audits on HireVue's website, HireVue required the disclosure of personal information to view each summary and a commitment that the reader would not reproduce any part of the summary.[324] And at least one of the audits was an analysis narrowly tailored to a specific use case of HireVue's platform—not the clean bill of health the company implied it was.[325] Further, key details about the algorithms used to make judgments in the hiring process are kept secret from applicants under evaluation. These examples illustrate the broader phenomenon of performing incomplete,

---

[321] Frances Haugen, Statement of Frances Haugen, *United States Senate Committee on Commerce, Science, and Transportation, Sub-Committee on Consumer Protection, Product Safety, and Data Security* (Oct. 4, 2021) https://www.commerce.senate.gov/services/files/FC8A558E-824E-4914-BEDB-3A7B1190BD49.

[322] *See* EPIC HireVue Complaint, *supra* note 6; HireVue, *supra* note 264; Mondragon et al., *supra* note 264.

[323] EPIC HireVue Complaint, *supra* note 6.

[324] *Download Report*, HireVue (2021), https://www.hirevue.com/resources/orcaa-report. To access the report, the website requires entry of First name, Last name, Work Email, Company Name, and has the following information before the "Submit Button": "Sharing your information helps us understand who is reading our research. The report you are downloading is being made available for review only. By downloading this document, you acknowledge and agree this report is the sole and exclusive intellectual property of HireVue, Inc., and you agree you shall not use, copy, excerpt, reproduce, distribute, display, publish, etc. the contents of this report in whole, or in part, for any purpose not expressly authorized in writing by HireVue, Inc."

[325] *See* Alex C. Engler, *Independent auditors are struggling to hold AI companies accountable*, Fast Company (Jan. 26, 2021), https://www.fastcompany.com/90597594/ai-algorithm-auditing-hirevue ("[H]aving viewed a copy of the ORCAA audit, I don't believe it supports the conclusion that all of HireVue's assessments are unbiased. The audit was narrowly focused on a specific use case, and it didn't examine the assessments for which HireVue has been criticized, which include facial analysis and employee performance predictions.").

constrained, or misleading audits or impact assessments that give the false appearance of meaningful transparency or accountability.[326]

The FTC should promulgate a rule requiring companies to publicly substantiate their claims about automated decision-making systems implicating the interests of consumers; articulate the purposes of those systems; evaluate the accuracy of those systems; and analyze potential disparate impacts of those systems.

The FTC should issue a rule that requires companies using automated decision-making systems implicating the interests of consumers to disclose, at minimum, the following about each system they use or sell:[327]

1. A detailed description of the intended purpose and proposed use of the system, including:
    a. What decision(s) the system will make or support;
    b. Whether the system makes final decision(s) itself or whether and how it supports decision(s);
    c. The system's intended benefits and research that demonstrates such benefits;
2. A detailed description of the system's capabilities, including capabilities outside of the scope of its intended use and when the system should not be used;
3. An assessment of the relative benefits and costs to the consumer given the system's purpose, capabilities, and probable use cases;
4. The inputs and logic of the system;
5. Data use and generation information, including:

[326] *See* Mona Sloane, *The Algorithmic Auditing Trap*, Medium (Mar. 17, 2021), https://onezero.medium.com/the-algorithmic-auditing-trap-9a6f2d4d461d.
[327] *See generally* S.B. 5116, 67th Leg., 2021 Reg. Sess. (Wash. 2021), https://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bills/Senate%20Bills/5116.pdf?q=20211202142727; Dillon Reisman et al., *Algorithmic Impact Assessments: A practical framework for public agency accountability,* AI Now Inst. (Apr. 2018) https://ainowinstitute.org/aiareport2018.pdf; *Algorithmic Impact Assessment*, Gov't of Can., https://open.canada.ca/aia-eia-js/ (last visited Nov. 20, 2022).

   a. How the data relied on by the system is populated, collected, and processed;
   b. The type(s) data the system is programmed to generate;[328]
   c. Whether the outputs generated by the system are used downstream for any purpose not already articulated;
6. Yearly validation studies and audits of accuracy, bias, and disparate impact;[329] and
7. A detailed use and data management policy.

Among other benefits to consumers, requiring these disclosures will help narrow the use of automated decision-making systems to circumstances in which they are genuinely necessary and appropriate and ensure that businesses restrict their use of automated decision-making systems to the purposes for which they are designed, evaluated, and advertised to the public.

The FTC should ensure that "disparate impact" is part of the required disclosures. The term "bias" may be understood to include an intent element, and disclosures or audits that focus solely on this term may be less helpful in establishing whether a violation of the Civil Rights Act of 1964, the Fair Housing Act, or the Age Discrimination in Employment Act has occurred.[330]

Finally, detailed audit requirements will help remedy some of the existing issues with audits, such as those raised with Facebook's audits above. Ari Ezra Waldman has contended that today's "[a]mbiguous privacy rules . . . with process-oriented regulatory levers open the door for companies to reframe the law in ways that serve corporate, rather than consumer, interests."[331] As a result, the compliance ecosystem has often become merely symbolic: it allows companies to interpret its legal requirements and implement process-oriented compliance structures—such as

[328] This should be done in descriptive terms (e.g., a number on a scale of 1–100 or a rating of low, medium, or high).
[329] *See* Jillson, *supra* note 312 ("How can you reduce the risk of your company becoming the example of a business whose well-intentioned algorithm perpetuates racial inequity? It is essential to test your algorithm—both before you use it and periodically after that—to make sure that it doesn't discriminate on the basis of race, gender, or other protected class.").
[330] 42 U.S.C. §§ 2000e-2(a)–(b); 42 U.S.C. § 3601 *et seq.*; 29 U.S.C. § 621 *et seq.*
[331] Ari Ezra Waldman, *Privacy Law's False Promise*, 97 Wash. U. L. Rev. 773, 792 (2020).

risk assessments and privacy policies—that shield them from liability or mitigate corporate risk.[332]

To remedy the failures of these structures and fulfill the goals of anti-discrimination law, the FTC must create an auditing standard that reflects substantive anti-discrimination protections rather than mere procedural requirements.[333] Such standards should require independent, third-party investigations and reports. The FTC has an opportunity to address the shortcomings of its consent decrees and company-driven privacy compliance programs. As the de facto federal privacy regulator, the Commission must not defer to symbolic structures and pro forma industry practices, but rather force companies to meaningfully question and test their systems.

Regulating upstream actors will not only address problems before they result in discrimination, but "any remedial actions taken by the vendor would [also] cascade down to all its clients."[334] The FTC has a strong argument that these upstream actors are the least cost avoiders. Rules should place the burden of addressing the risks of automated decision-making systems on the entities most capable of averting them—that is, the creators and users of such products, rather than the millions of online consumers exposed to their harmful effects.

2.2. It is an unfair and deceptive practice to use an automated decision-making system implicating the interests of consumers without providing adequate notice of such use, which includes meaningful, readable, and understandable disclosure of the logic, factors, inputs, and training data on which such system relies.

Responsive to questions 53, 55, 56, 58, and 60.

Transparency offers a pathway to understanding how the algorithms function. By requiring developers, data controllers, and users of algorithmic decision-making systems to disclose information about the process, third parties can

---

[332] *Id.* at 796–97, 799.
[333] *See id.* at 803.
[334] Andrew D. Selbst & Solon Barocas, *Unfair Artificial Intelligence: How FTC Intervention Can Overcome the Limitations of Discrimination Law*, U. Penn. L. Rev. 7, 12 (forthcoming 2023).

investigate algorithmic bias, and consumers can make more informed decisions about their use of such technologies.[335] Individuals have a right to know when they are being subject to automated decision-making.[336] Moreover, whether an automated decision-making system is being used to make decisions about consumers is material to consumers' decisions about whether to engage the product or service utilizing that system.[337] Regardless of whether disclosure of automated decision-making usage is widespread, the usage itself is widespread—and many of these companies are explicitly aware of the risks to civil rights.[338] Notice must be meaningful and is essential to effectuate any option for opt-out. The Commission should rule that failure to providing adequate notice of the use of automated decision-making, which includes meaningful, readable, and understandable disclosure of the logic, factors, inputs, and training data on which such system relies, is an unfair practice.

Although algorithmic governance frameworks sometimes define transparency as "explainability" (i.e., whether the underlying logic of an automated decision-making system is explainable, rather than whether companies are

---

[335] *Id.* at 49.

[336] *AI & Human Rights*, EPIC (2022), https://epic.org/issues/ai/; *see also* CCPA §§ 1798.110, 1798.115, 1798.121 (providing similar rights by statute in California).

[337] Consumer polls regularly indicate use of automated decision-making is a relevant concern to consumers, especially regarding their trust in the company using automated systems. *See, e.g.*, Aaron Smith, *Public Attitudes Toward Computer Algorithms*, Pew Rsch. Ctr. (Nov. 16, 2018), https://www.pewresearch.org/internet/2018/11/16/public-attitudes-toward-computer-algorithms/ (majority of survey respondents find use of automated decision-making unacceptable where it has real-world consequences for humans); Cisco, *Consumer Privacy Survey* 14 (2021), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf (37% of respondents would trust a company less that used automated decision-making to match consumers with a sales rep, 53% would trust a company less that used automated decision-making for job interviews); *id.* at 15 (49% of respondents in the US would lose trust in a company due to their use of automated decision-making); Press Release, Gartner, *Gartner Survey Finds Consumers Would Use AI to Save Time and Money* (Sept. 12, 2018), https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-survey-finds-consumers-would-use-ai-to-save-time-and-money (65% of respondents believe automated decision-making will destroy their privacy rather than improve it).

[338] *See e.g.*, McKinsey & Co., *The State of AI in 2020* (Nov. 17, 2020), https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/global-survey-the-state-of-ai-in-2020 (50% of respondent companies utilized automated decision-making in at least one business function, 22% reported more than 5% of EBIT due to automated decision-making, 39% acknowledged personal/individual privacy as a relevant risk).

disclosing their use of automated decision-making at all), disclosing the use of automated decision-making systems—or a prohibition on secret profiling—is a necessary predicate to more meaningful transparency.

The use of automated decision-making systems without meaningful notice to those subject to the processing is an unfair practice which causes substantial injury. In 2017, Amazon discontinued undisclosed use of an automated decision-making system it had used to assist with screening candidates upon discovering that it was reinforcing existing gender disparities within the company and being unable to correct that problem after two years of trying. While in this instance, the public learned that a screening algorithm had been used for several years and was biased, job candidates might never know such an algorithm was being used on them. This unacceptable reality has ramifications for a harmed individual seeking recourse, as they might never learn that they were a victim.[339] Even before any applicant screening process occurs, an individual might never learn that automated decision-making prevented a job posting from being displayed to them in the first place,[340] as has been the case on Facebook[341] and Google.[342]

When Apple launched its credit card, consumers found that women with similar credit profiles received less credit and less favorable decisions by Apple's

---

[339] *See* Jeffrey Dastin, *Amazon scraps secret AI recruiting tool that showed bias against women*, Reuters (Oct. 10, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

[340] *See* Tyler Sonnemaker, *Here's why an AI expert says job recruiting sites promote employment discrimination*, Bus. Insider (Jan. 18, 2020), https://www.businessinsider.com/ai-expert-job-sites-must-prove-not-exacerbating-inequality-2020-1 ("The problem actually lies before the application comes in. The problem lies in the pipeline to match job seekers with jobs.") (quoting Cathy O'Neil, data scientist and author of *Weapons of Math Destruction*).

[341] *See* Miranda Bogen, *All the Ways Hiring Algorithms Can Introduce Bias*, Harv. Bus. Rev. (May 6, 2019), https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias ("supermarket cashier positions were shown to an audience of 85% women, while jobs with taxi companies went to an audience that was approximately 75% black") (citing Ali et al., *supra* note 276, at 4); Basileal Imana et al., *Auditing for Discrimination in Algorithms Delivering Job Ads*, Proc. Web Conf. 2021 (WWW '21) (Apr. 19, 2021), https://www.ftc.gov/system/files/documents/public_events/1582978/auditing_for_discrimination_in_algorithms_delivering_job_ads.pdf (observing skewed ad delivery for open job positions on Facebook, Google, and LinkedIn due to hidden AI).

[342] *See* Datta et al., *supra* note 278, at 102 (finding "females received fewer instances of an ad encouraging the taking of high paying jobs than males").

partner bank Goldman Sachs.[343] Even Apple co-founder Steve Wozniak said he was approved for "10x [the credit limit] despite not having any separate assets or accounts."[344] This was an exemplar of a black box algorithm that was not made clear to the user, and insufficient details were disclosed or tested in order to make notice meaningful. As a result, individuals suffered confusion due to a lack of transparency of how the credit limit was determined and a lack of notice that the decision was being made through an automated decision-making system. When systems have discriminatory results, the lack of meaningful notice becomes even more consequential and can obfuscate opportunities for recourse.

Consumer profiling has become "pervasive, secret, and automated," posing "threats to human dignity[.]"[345] "At the very least, individuals should have a meaningful form of notice and a chance to challenge predictive scores that harm their ability to obtain credit, jobs, housing, and other important opportunities."[346]

Several recommendations from the White House Blueprint for an AI Bill of Rights support the view that a lack of adequate notice is an unfair and deceptive practice:

- Consent for non-necessary functions should be optional, i.e., **should not be required, incentivized, or coerced to receive opportunities or access to services**. In cases where data is provided to an entity (e.g., health insurance company) to facilitate payment for such a need, that data should only be used for that purpose.
- **You should know how and why** an outcome impacting you was determined by an automated system, including when the automated system is not the sole input determining the outcome.
- Sensitive data should only be used for **functions strictly necessary for that domain or for functions that are required for administrative reasons**

[343] *See* Neama Dadkhahnikoo, *Incident Number 92: Apple Card's Credit Assessment Algorithm Allegedly Discriminated against Women*, *in* Artificial Intelligence Incident Database (Sean McGregor & Khoa Lam eds. 2019), https://incidentdatabase.ai/cite/92.
[344] Clare Duffy, *Apple Co-founders Steve Wozniak says Apple discriminated against his wife*, CNN (Nov. 11, 2019), https://www.cnn.com/2019/11/10/business/goldman-sachs-apple-card-discrimination.
[345] Citron & Pasquale, *supra* note 315, at 27.
[346] *Id.*

(e.g., school attendance records), unless consent is acquired, if appropriate, and the additional expectations in this section are met.

- Civil liberties and civil rights must not be limited by the threat of surveillance or harassment facilitated or aided by an automated system. Surveillance systems should not be used to monitor the exercise of democratic rights, such as voting, privacy, peaceful assembly, speech, or association, in a way that limits the exercise of civil rights or civil liberties.

One of the most alarming examples of violations of these principles is Clearview AI.[347] Using a powerful algorithm and billions of facial images collected without consent, Clearview has created a facial recognition app capable of quickly identifying a person based on a single photo.[348] By the time the public was made aware of Clearview's existence, the app was already in use by hundreds of law enforcement agencies.[349] Clearview built its tool in effective secrecy, in violation of numerous terms of service, and with no oversight. Yet despite the recent public outcry over Clearview's use of automated decision-making, individual consumers have little ability to hold the company accountable for developing and operating a facial recognition tool based on their personal data. And Clearview is not alone in the field: companies including Amazon,[350] FaceFirst,[351] and Vigilant Solutions[352] have also developed large-scale—and largely unaccountable—facial recognition tools. Businesses are engaged in secret profiling of consumers, and the FTC should establish safeguards to prevent this unfair practice.

Clearview AI is a notable example of secret profiling of consumers, but there are many others. In 2017, Airbnb acquired Trooly, an automated risk assessment tool that can be used to rate potential guests[353] (or in the words of Trooly's patent, to

---

[347] Hill, *supra* note 296.
[348] *Id.*
[349] *Id.*
[350] *Amazon Rekognition*, AWS (2020), https://aws.amazon.com/rekognition/.
[351] FaceFirst (2020), https://www.facefirst.com/.
[352] *Vigilant FaceSearch*, Vigilant Solutions (2020), https://www.vigilantsolutions.com/products/facial-recognition/.
[353] Mark Blunden, *Booker beware: Airbnb can scan your online life to see if you're a suitable guest*, Evening Standard (Jan. 3, 2020), https://www.standard.co.uk/tech/airbnb-software-scan-online-life-suitable-guest-a4325551.html.

"determin[e] trustworthiness and compatibility of a person").[354] The automated decision-making system analyzes information collected from third parties—including service providers, blogs, public and commercial databases, and social networks—to generate a "trustworthiness" score.[355] The patent claims that the system can identify whether an individual is involved with drugs or alcohol; hate websites or organizations; sex work and pornography; criminal activity; civil litigation; and fraud.[356] According to the patent, the system can also identify "badness, anti-social tendencies, goodness, conscientiousness, openness, extraversion, agreeableness, neuroticism, narcissism, Machiavellianism, [and] psychopathy." Yet whether and how Airbnb uses each of Trooly's capabilities to screen consumers remains a secret.[357]

Several jurisdictions have proposed bans on different types of AI-enabled profiling, including the European Union and Washington state.[358] In Canada, Clearview was deemed unlawful by the Privacy Commissioner, who wrote that "What Clearview does is mass surveillance, and it is illegal. It is completely unacceptable for millions of people who will never be implicated in any crime to find themselves continually in a police lineup."[359]

The use of automated decision-making systems without meaningful notice and opt-out opportunities is not reasonably avoidable. Surprise is a common consumer response to learning that healthcare or credit decisions[360] were made

---

[354] U.S. Patent No. 9,070,088 (filed June 30, 2015), http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=9070088.PN.&OS=PN/9070088&RS=PN/9070088.

[355] *Id.*

[356] *Id.*

[357] Aaron Holmes, *Airbnb has patented software that digs through social media to root out people who display 'narcissism or psychopathy'*, Bus. Insider (Jan. 6, 2020), https://www.businessinsider.com/airbnb-software-predicts-if-guests-are-psychopaths-patent-2020-1.

[358] S.B. 5116, 67th Leg., 2021 Reg. Sess. (Wash. 2021), https://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bills/Senate%20Bills/5116.pdf?q=20211202142727.

[359] News Release, Off. of the Privacy Comm'r of Can., *Clearview AI's unlawful practices represented mass surveillance of Canadians, commissioners say* (Feb. 3, 2021), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210203/.

[360] *See* Smith & Rustagi, *supra* note 281 ("A husband and wife compared their Apple Card spending limits and found that the husband's credit line was 20 times greater. Customer service employees were unable to explain why the algorithm deemed the wife significantly less creditworthy.").

based on a predictive automated decision-making system. In the healthcare context, consumers have been shocked to learn that data collected by their necessary health equipment was used to make reimbursement decisions.[361] Various firms have used patient's investments and types of cars owned, or cell phone numbers and property records, fed into algorithms to predict health outcomes and generate patient health risk scores.[362] Notably, the ProPublica journalist who wrote the article detailing this practice sought their own health risk score data and was denied by LexisNexis because LexisNexis's client was the insurance company, not the consumer.[363]

Certain automated decision-making practices are unforeseeable to a consumer without notice. In the credit context, whether a consumer filled their credit application using proper capitalization could inform an automated determination as to their creditworthiness.[364] Data that consumers would not likely consider credit data (and importantly which falls outside the scope of the Fair Credit

---

[361] *See* All Things Considered, *How Insurers Are Profiting Off Patients With Sleep Apnea*, NPR (Nov. 21, 2018, 5:33 PM), https://www.npr.org/2018/11/21/670142105/how-insurers-are-profiting-off-patients-with-sleep-apnea ("And that's when he realized that the machine was actually spying on him and tracking his sleep habits and sleep patterns. And the irony is he wasn't able to use the machine because he didn't have the new mask and yet they hadn't been sending the new mask because they said he wasn't using the machine.").

[362] ProPublica disclosed that Optum, owned by UnitedHealth Group, has medical, financial, and socioeconomic data on more than 150 million Americans dating back to 1993, which it advertises in the context of predicting health outcomes. In 2012, analytics company SAS worked with a major health insurance company to predict health care costs using 1,500 data elements, including a patient's investments and types of cars owned. LexisNexis uses 442 non-medical personal attributes to predict medical costs, including cellphone numbers, criminal records, bankruptcies, property records, and indicia of neighborhood safety. *See* Marshall Allen, *Health Insurers Are Vacuuming Up Details About You – And It Could Raise Your Rates*, ProPublica (July 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.

[363] *See id.*

[364] *See* Mikella Hurley & Julius Adebayo, *Credit Scoring in the Era of Big Data*, 18 Yale J.L. & Tech. 148, 164 n.74 (2016), https://openyls.law.yale.edu/bitstream/handle/20.500.13051/7808/Hurley_Mikella.pdf (citing Michael Carney, *Flush with $20M from Peter Thiel, ZestFinance is Measuring Credit Risk Through Non-traditional Big Data,* Pando (July 31, 2013), https://perma.cc/PZ5R-WPJG ("Merrill [ZestFinance CEO] explains… that the way a consumer types their name in the credit application – using all lowercase, all uppercase, or correct case – can be a predictor of credit risk.")).

Reporting Act), such as their IP address or device ID, has also been used for alternative credit determinations.[365]

Using automated decision-making systems without meaningful notice and opt-out opportunities is not outweighed by any countervailing benefits. When a company deploys automated decision-making systems without disclosing its use or explaining what the systems do, it makes a conscious choice to expose consumers to potential harm without letting consumers make informed decisions about whether and how to engage with the company's systems. This practice of nondisclosure can exacerbate harm caused by flawed or biased automated decision-making systems, as with consumer profiling and surveillance, by obfuscating the harm to consumers. For example, consumers may not be aware of the harm or whether an automated decision-making system is injuring them specifically. However, this practice of nondisclosure also causes consumer and competitive harms when the automated decision-making systems themselves do not. Many commercial applications of automated decision-making rely on the collection and use of consumer data, which often subsidizes the financial cost of products and services.[366] Consumers may not be aware of the existence, nature, or extent of this data collection and use by automated decision-making systems, so their preferences may not be accurately reflected by their market participation. Without meaningful notice and opt-out opportunities, consumers cannot meaningfully respond to market conditions and decide how they want to engage with the array of products and services supported by automated decision-making.

By comparison, the countervailing benefits of nondisclosure are minimal. First, companies may claim that nondisclosure provides an administrative and financial benefit: any meaningful notice and opt-out opportunities would take time

---

[365] *See id.* ("Experian collects offline data for individual consumers that is linked to 'match keys' like a consumer's address, credit card number, phone number, and also collects online and mobile data that is linked to match keys such as device ID, IP address, geolocation, a consumer's Twitter 'handle,' time stamp, and other identifiers.") (citing Marcus Tewksbury, *The 2013 Big Data Planning Guide for Marketers*, Experian Mktg. Servs. (2013), https://perma.cc/FY9T-G28A).

[366] *See, e.g.*, Daniel L. Rubinfeld & Michal Gal, *The Hidden Costs of Free Goods: Implications for Antitrust Enforcement*, 80 Antitrust L.J. 521, 521 n.1 (2016), https://www.law.berkeley.edu/wp-content/uploads/2015/04/80AntitrustLJ521_stamped.pdf (markets for free goods and services encompass "situations in which the consumer pays indirectly… by providing information about his or her preferences.").

and money to enact—and doing so may push some consumers away from the company's products or services. However, these benefits are not true cost savings; rather, they are savings provided by trapping consumers into an unavoidable and inescapable practice of data collection and analysis. The one-time cost of implementing notice and opt-out opportunities is far outweighed by the various benefits that disclosure would provide to consumers.

Second, companies may claim that nondisclosure provides important protections for trade secrets and other proprietary information from competitors. Meaningful notice and opt-out opportunities may, in fact, provide competitors with information about a company's automated decision-making systems, but the disclosures that would benefit consumers—information about the logic, factors, inputs, and training data used by an automated decision-making system—are distinct from the information that would meaningfully impact competitor behavior. Several key aspects of automated decision-making systems would remain hidden from competitors, including the data collected and used by a system, the methods used to train a system, and the underlying code and input weights used in a system. While nondisclosure does provide competitive benefits to companies using automating decision-making systems, these benefits do not outweigh the various harms felt by consumers subjected to automated decision-making every day.

Using automated decision-making systems without meaningful notice or an opportunity to opt out is a deceptive practice that is likely to mislead a reasonable consumer. When a person is subject to automated decision-making systems without meaningful notice or even cursory notice a system is being used, it is likely to mislead a consumer, stripping them of choice and individuality. Using automated decision-making systems without meaningful notice or an opportunity to opt out is also material and likely to affect a consumer's choice. When an individual applies for a loan or housing, they are likely to be subject to several types of "scores," algorithms that use a substantial amount of data.[367] In a 2018 Pew Survey, 67% of U.S. adults said it was unacceptable to use automated decision

[367] *See* Chloe Xiang, *JP Morgan Wants to Make Tenant Data Available to Every Landlord*, Vice (Nov. 4, 2022), https://www.vice.com/en/article/k7bkyn/jp-morgan-wants-to-make-tenant-data-available-to-every-landlord.

making systems for video analysis of job interviews, 68% said they found it unacceptable for algorithms to determine a "personal finance score using many types of consumer data," and "automated resume screening of job applicants." In each of these examples, the individual is left to guess whether a given landlord or employer is using an automated decision-making system. Meaningful notice, using information already created from the disclosure rule proposed below in section 6.1, would help correct this power asymmetry and empower consumers.

The use of automated decision-making without adequate notice to affected individuals is prevalent. In 2017, 13% of human resource managers surveyed by Harris said they were already seeing evidence of automated decision-making becoming a regular part of HR, with 55% saying it would be within five years.[368] 63% of talent acquisition professionals surveyed by Korn Ferry in 2018 said that AI has changed the way recruiting is done at their company.[369] In recognition of the problem of a lack of disclosure around hiring algorithms, both Illinois[370] and New York City[371] have passed laws requiring disclosure to the applicant or employee prior to use. People in other parts of the country should not be left in the dark.

Due to current lack of regulations on the collection and use of data by these algorithms, we can expect automated decision-making will continue to be used in

[368] *See* CareerBuilder, *More Than Half of HR Managers Say Artificial Intelligence Will Become a Regular Part of HR in Next 5 Years*, PR Newswire (May 18, 2017), https://www.prnewswire.com/news-releases/more-than-half-of-hr-managers-say-artificial-intelligence-will-become-a-regular-part-of-hr-in-next-5-years-300458775.html.
[369] *See How AI will shape recruiting in 2019*, Monster.com, https://hiring.monster.com/resources/recruiting-strategies/talent-acquisition/future-of-ai-recruiting/ (last visited Nov. 13, 2022).
[370] Illinois Artificial Intelligence Video Interview Act, 820 Ill. Comp. Stat. 42/1 *et seq.* (2020).
[371] N.Y. Local Law Int. No. 1894-A (2021), https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9.

healthcare[372] and credit reporting[373] without any meaningful opportunity for consumers to opt out. Current efforts to track bias suggest that it is prevalent among automated decision-making systems.[374] Experts in the field expect these biases will persist, with 68% saying ethical principles focused primarily on the public good will not be employed in most automated decision-making systems by 2030, and 37% saying the negatives will outweigh the positives. [375] Regardless, experts anticipate use of these systems to only become more prevalent over time.[376]

California has required the newly formed California Privacy Protection Agency to regulate consumer access and opt-out rights regarding automated decision-making technology, including profiling.[377] Colorado and Virginia have passed similar opt-out provisions for profiling,[378] along with requirements for completing data protection assessments where personal data is processed for

---

[372] *See, e.g.*, Allen, *supra* note 362 (quoting Prof. Frank Pasquale: "We have a law that only covers one source of health information. They are rapidly developing another source"); Adam Tanner, *How Data Brokers Make Money Off Your Medical Records*, Sci. Am. (Feb. 1, 2016), https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/ (re-identifying medical data that was de-identified at the time of purchase); Ctr. for Applied A.I. at Chi. Booth, *Algorithmic Bias Playbook* 1 (2021), https://www.ftc.gov/system/files/documents/public_events/1582978/algorithmic-bias-playbook.pdf ("Algorithmic bias is everywhere. Our work with dozens of organizations—healthcare providers, insurers, technology companies, and regulators—has taught us that biased algorithms are deployed throughout the healthcare system, influencing clinical care, operational workflows, and policy.").

[373] *See* Hurley & Adebayo, *supra* note 364, at 1 ("The credit scoring industry has experienced a recent explosion of start-ups that take an 'all data is credit data' approach, combining conventional credit information with thousands of data points mined from consumers' offline and online activities.").

[374] *See* Smith and Rustagi, *supra* note 281 (finding of 113 biased systems, 44% demonstrate gender bias, 25% demonstrate both gender and racial bias).

[375] *See* Lee Rainie et al., *Experts Doubt Ethical AI Design Will Be Broadly Adopted as the Norm Within the Next Decade*, Pew Rsch. Ctr. (June 16, 2021), https://www.pewresearch.org/internet/2021/06/16/experts-doubt-ethical-ai-design-will-be-broadly-adopted-as-the-norm-within-the-next-decade/.

[376] *See* Lee Rainie & Janna Anderson, *Theme 1: Algorithms will continue to spread everywhere*, Pew Rsch. Ctr. (Feb. 8, 2017), https://www.pewresearch.org/internet/2017/02/08/theme-1-algorithms-will-continue-to-spread-everywhere/ ("A significant majority expects [algorithms] to continue to proliferate – mostly invisibly – and expects that there will be an exponential rise in their influence.").

[377] *See* CCPA § 1798.185(a)(16). The state's same regulatory agency recently invited comment on what activities should constitute profiling, what information businesses must provide to consumers, and how an opt-out process should be followed. Cal. Priv. Prot. Agency, Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01-21) (Sept. 22, 2021), https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf.

[378] *See* Colorado Privacy Act § 6-1-1306(a)(I)(C); Va. Code § 59.1-577(A)(5).

profiling purposes.[379] In the context of insurance, as of 2017 at least twenty (20) states had banned use of "price optimization," whereby predictive models can impact consumers' premiums.[380]

To prevent the unfair and deceptive practice of using automated decision-making systems without providing adequate notice, the Commission should adopt rules defining and requiring meaningful notice to consumers prior to the use of those systems. The Commission has recently taken action where consumers were harmed by the lack of notice of the use of automated decision-making.[381] However, it has not explicitly required that companies provide notice where an automated decision-making system has been used.[382]

---

[379] *See* Colorado Privacy Act § 6-1-1309; Va. Code § 59.1-580(A)(3).
[380] *See* Press Release, Consumer Fed'n of America, *Consumer Groups Applaud NV Insurance Commissioner for Banning Price Optimization and Closing the "Underwriting" Loophole: Nevada Becomes 20th State to Take on New Price Gouging Techniques of Some Insurance Companies* (Feb. 1, 2017), https://consumerfed.org/press_release/consumer-groups-applaud-nevada-insurance-commissioner-banning-price-optimization-closing-underwriting-loophole/.
[381] *See, e.g.*, Complaint at 6, *In re Everalbum, Inc.*, FTC File No. 1923172 (2021), https://www.ftc.gov/system/files/documents/cases/everalbum_complaint.pdf ("As described in Paragraph 9, Respondent represented, directly or indirectly, expressly or by implication, that Everalbum was not using face recognition unless the user enabled it or turned it on."); Complaint at 6, *United States v. Facebook*, 456 F. Supp. 3d 115 (D.D.C. 2019) (No. 19-cv-2184), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf ("Finally, in April 2018, Facebook updated its data policy to explain that Facebook would use an updated facial-recognition technology to identify people in user-uploaded pictures and videos '[i]f it is turned on,' implying that users must opt in to use facial recognition. Contrary to the implication of this updated data policy, however, tens of millions of users who still had an older version of Facebook's facial-recognition technology had to opt out to disable facial recognition.").
[382] *Compare* Andrew Smith, *Using Artificial Intelligence and Algorithms*, FTC Bus. Blog (Apr. 8, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms (prohibiting misrepresentation for direct customer interaction with chatbots and fake profiles but not requiring disclosure of use of AI in all contexts) *and* Jillson, *supra* note 312 (pointing to the Commission's Facebook and Everalbum actions as examples of users being deceived about their level of control of data collection for training an AI, but not explicitly stating that companies must disclose that an AI is in use), *with* Competition & Mkts. Auth., *Algorithms: How they can reduce competition and harm consumers*, GOV.UK (Jan. 19, 2021), https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers ("If consumers are not aware that [AI-powered personalization] is occurring, or if it gives rise to unfair distributive effects or harms consumers who are vulnerable, it is more likely to be exploitative….In addition, misleading and aggressive practices are prohibited. This includes omission of material information from consumers which impairs their ability to make an informed choice.").

2.3. It is an unfair practice to use one-to-many facial recognition, emotion recognition, or other biometric technologies for commercial surveillance.

Responsive to questions 53, 55, 56, 58, 60.

The Commission should promulgate a rule prohibiting the commercial use of one-to-many facial recognition and emotion recognition systems in view of the significant and inevitable harms these tools inflict on consumers.

Commercial use of facial recognition technology causes substantial injury to consumers. Each stage of the facial recognition process poses serious harms to consumers. The first phase is detection, where an algorithm is "trained" to learn how to recognize a face.[383] Then the software will analyze or verify the information, and finally compare it with a database of photos, often from a variety of sources for identification.[384] Facial analysis is distinct from facial recognition. "Whereas facial recognition matches a face to a specific identify, facial analysis uses a facial image to estimate or classify personal characteristics such as age, race, or gender."[385] Many facial recognition systems rely on machine learning, and the process is fluid: "[I]f the technology detects a face, an algorithm then matches and compares the template to that of another photo and calculates their similarities."[386]

Harms can result from the photos initially fed into the database or how the algorithm informing the analysis and recognition fails to accurately identify certain faces. A study from National Institute of Standards and Technology ("NIST") analyzed the facial recognition algorithms of a "majority of the industry" and found the software up to 100 times more likely to return a false positive for a non-white individual than for a white individual.[387] Specifically, NIST found "for one-to-many

---

[383] Thorin Klosowski, *Facial Recognition Is Everywhere. Here's What We Can Do About It*, N.Y. Times (July 15, 2020), https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/.
[384] *Id.*
[385] U.S. Gov't Accountability Off., GAO-20-522, *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses* 6 (2020), https://www.gao.gov/products/gao-20-522 [hereinafter GAO Facial Recognition Report].
[386] *Id.* at 5.
[387] Press Release, Nat'l Inst. of Standards & Tech., *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software* (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

matching, the team saw higher rates of false positives for African American females," a finding that is "particularly important because the consequences could include false accusations."[388] A separate study by Stanford University and MIT, which looked at three widely used commercial facial recognition tools, found an error rate of 34.7% for dark-skinned women compared to an error rate of 0.8% for light-skinned men.[389] Relatedly, the classifications themselves "can limit understanding of how FRTs perform across groups that are not accounted for by commonly used classification systems," increasing exposure for marginalized groups to machine-based discrimination.[390]

In the absence of accountability and regulation, the risks and harms of facial recognition have proliferated in commercial settings. Commercial applications of facial recognition range from secure access and safety to photo identification, marketing services, payment, and attendance tracking for events.[391] Facial recognition has been used to identify consumers in retail settings,[392] at concerts,[393] and other public events.[394] But these systems are often coupled with risky retention and data security practices[395] and exhibit inaccuracy and bias, which can reify harmful racial stereotypes. Moreover, one-to-many facial recognition diminishes an

---

[388] *Id.*

[389] Larry Hardesty, *Study finds gender and skin-type bias in commercial artificial-intelligence systems*, MIT News (Feb. 11, 2018), https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

[390] Erik Learned-Miller et al., Algorithmic Just. League, *Facial Recognition Technologies in the Wild: A Call for Federal Office* 7 (May 29, 2020), https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_FRTsFederalOfficeMay2020.pdf [hereinafter FRT in the Wild].

[391] *See* GAO Facial Recognition Report, *supra* note 385, at 11–13.

[392] *See* Nick Tabor, *Smile! The Secretive Business of Facial Recognition Software in Retail Stores*, N.Y. Mag. (Oct. 20, 2018), https://nymag.com/intelligencer/2018/10/retailers-are-using-facial-recognition-technology-too.html.

[393] *See* Steve Knopper, *Why Taylor Swift is Using Facial Recognition at Concerts*, Rolling Stone (Dec. 13, 2018), https://www.rollingstone.com/music/music-news/taylor-swift-facial-recognition-concerts-768741/.

[394] *See* Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, N.Y. Times (Mar. 13, 2018), https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html; Vas Panagiotopoulos, *Soccer Fans, You're Being Watched*, Wired (Nov. 3, 2022), https://www.wired.com/story/soccer-world-cup-biometric-surveillance/.

[395] *See* FRT in the Wild, *supra* note 390, at 9 ("FRTs can rely on large stores of valuable personal data and biometric information, making these systems the target of data theft attacks.").

individual's ability to remain anonymous in public[396] and causes personal information to be "used, shared, or sold in ways that consumers do not understand, anticipate or consent to."[397]

One company increasing its facial recognition use is PopID, which offers facial recognition technology for buildings and events (PopEntry) and payments (PopPay). PopID recently announced that "over 100 different restaurant and retail brands (both small businesses and chains) now accept its payment product."[398] As of last year, the product had 70,000 registered users and had been employed to authenticate faces "over four million times."[399]

Facial recognition technology is increasingly unavoidable. It is exceedingly difficult for a consumer to avoid the consumer surveillance harms associated with facial recognition technology. There is little a consumer can do to prevent or avoid the capture or use of their image by a private company for facial recognition purposes. Participation in society often exposes one's images in public spaces and online, but facial recognition technology nearly eliminates an individual's ability to control the disclosure of their identity to others, posing unique harms.[400] These systems "can be quickly deployed using face data available online and inexpensive camera systems. Such easy deployment enables the mass collection of personal information without consent."[401] Additionally, there is insufficient information available about the details or even existence of facial recognition uses in commercial

---

[396] *See id.* at 8 ("[D]eploying face recognition systems on video surveillance networks can enable mass surveillance that erodes the ability to be anonymous in a public space.").
[397] GAO Facial Recognition Report, *supra* note 385, at 4; *see also* Woodrow Hartzog, *Facial Recognition Is the Perfect Tool for Oppression*, Medium (Aug. 2, 2018) (listing privacy and civil liberties harms from facial recognition use).
[398] Press Release, BusinessWire, *Pop ID's Payment Platform Grows to Over 100 Brands Following Series B Investment* (Sept. 7, 2021), https://www.businesswire.com/news/home/20210907005311/en/PopID%E2%80%99s-Payment-Platform-Grows-to-Over-100-Brands-Following-Series-B-Investment.
[399] *Id.*
[400] *See* Julie Cohen, *The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy*, 31 Phil. & Tech. 213, 219–20 (2017) (describing the "extension of surveillance capability" over time to capture personal and biometric information through sensing networks and facial recognition technology).
[401] FRT in the Wild, *supra* note 390, at 7.

settings. Therefore, individuals cannot reasonably avoid, nor "protest or seek redress to harm for decisions that are informed by FRTs they do not know about."[402]

Commercial use of facial recognition does not confer countervailing benefits on consumers or competition that outweigh the substantial injury it causes to consumers. Arguable upsides to consumers include quicker and more secure entry to places of business or registering for events, and safety and fraud protection at ATMs or while logging onto online accounts. However, there are substantial dark spots in the security, and maintaining databases of personal information poses increased risks to privacy and security because "FRTs can rely on large stores of valuable personal data and biometric information, making these systems the target of data theft attacks."[403] And research identifying pervasive accuracy and bias issues in facial recognition technology calls into question the value of such systems to consumers.

Alleged competitive benefits range from security to advertising benefits. The advertising and marketing sector is increasingly using facial recognition to track consumer behavior for customized ads online.[404] However, these potential benefits are far outweighed by the security risk, discriminatory effects, and general ineffectiveness of facial recognition technology.[405] In June, Microsoft announced that it would restrict use of its facial recognition software and stop offering certain automated tools for "detecting, analyzing and recognizing faces."[406] Microsoft sells its "Face API" technology to companies across sectors, including Uber.[407] Meta also shut down its facial recognition software last year due to privacy, and broader

---

[402] *Id.* at 8.
[403] *Id.* at 9.
[404] Molly St. Louis, *How Facial Recognition Technology is Shaping the Future of Marketing Innovation*, Inc. (Feb. 16, 2017), https://www.inc.com/molly-reynolds/how-facial-recognition-is-shaping-the-future-of-marketing-innovation.html.
[405] Kashmir Hill, *Microsoft Plans to Eliminate Face Analysis Tools in Push for 'Responsible AI,'* N.Y. Times (June 21, 2022), https://www.nytimes.com/2022/06/21/technology/microsoft-facial-recognition.html.
[406] *Id.*
[407] *Face API*, Microsoft, https://azure.microsoft.com/en-us/products/cognitive-services/face/#customer-stories (last visited Nov. 13, 2022).

societal concerns.[408] Moreover, there is a high upfront cost for the technology itself and increased liability under the Illinois Biometric Information Privacy Act and other developing biometric data laws.[409] Facial recognition technology lacks sufficient benefits to outweigh the harms it causes in the commercial setting.

The use of emotion recognition technology in security, education, employment, and other contexts is an unfair practice that causes substantial injury. Emotion recognition technology is a growing industry that uses AI to detect emotions from various facial expressions and cues. Privacy, civil liberties, and discrimination-based harms can result from commercial use of emotional recognition technology. Despite research suggesting its use is inaccurate, unfair, and susceptible to misuse, companies continue to sell and use emotion recognition software.[410] "Job applicants are being judged unfairly because their facial expressions or vocal tones don't match those of employees; students are being flagged at school because their faces seem angry."[411]

Algorithms often fail to capture the complexity of human emotion when used in the real world. For instance, data shows that people only scowl approximately 30% of the time when they are angry, so if an algorithm views a scowl as a necessary component of anger, it will be wrong about 70% of the time.[412] In the commercial context, companies employ emotion recognition systems to generate "employability" scores for job applicants, analyze the impact of advertisements and

---

[408] Kashmir Hill & Ryan Mac, *Facebook, Citing Societal Concerns, Plans to Shut Down Facial Recognition System*, N.Y. Times (Nov. 5, 2021), https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html.
[409] Taylor Hatmaker, *Clearview AI Banned From Selling Its Facial Recognition Software to Most US Companies*, TechCrunch (May 9, 2022), https://techcrunch.com/2022/05/09/clearview-settlement-bipa/.
[410] *See* Daniel Thomas, *The Cameras That Know if You're Happy – Or A Threat*, BBC (July 17, 2018), https://www.bbc.com/news/business-44799239.
[411] Kate Crawford, *Time to Regulate AI That Interprets Human Emotions*, Nature (Apr. 6, 2021), https://www.nature.com/articles/d41586-021-00868-5.
[412] James Vincent, *AI "Emotion Recognition" Can't Be Trusted*, Verge (July 25, 2019), https://www.theverge.com/2019/7/25/8929793/emotion-recognition-analysis-ai-machine-learning-facial-expression-review.

the emotional status of customers, and attempt to detect shoplifters.[413] These systems all rely on algorithms based on early research that proposed the existence of universal emotions and a strong correlation between emotion and facial expression.[414] However, a 2019 meta-analysis of the relevant scientific literature revealed that there is actually no reliable evidence that an individual's emotional state can be inferred from their facial movements.[415] Emotion recognition technology is unable to "confidently infer happiness from a smile, anger from a scowl, or sadness from a frown" because it glosses over cultural and social contexts.[416]

Harms stemming from emotion recognition can be unique to a certain demographic or gender. For example, since women are often socialized to smile in the workplace in order to avoid negative repercussions, a smile is not a reliable indicator of actual happiness or agreement.[417] Emotion recognition systems do not consider other factors such as an individual's body movement, personality, and tone of voice in their perception of emotion, and cannot even distinguish between the meanings of an intentional wink and an involuntary blink.[418] Emotion detection technology also may lead to harmful racial stereotypes. These algorithms have racist tendencies, frequently assigning the faces of Black men more negative and threatening emotions than White men regardless of how much they smiled.[419] One software system, Face++, rates Black faces twice as angry as their White

---

[413] James Vincent, *Discover the Stupidity of AI Emotion Recognition with This Little Browser Game*, Verge (Apr. 6, 2021), https://www.theverge.com/2021/4/6/22369698/ai-emotion-recognition-unscientific-emojify-web-browser-game; *see also* Kate Crawford, *Artificial Intelligence is Misreading Human Emotion*, Atlantic (Apr. 27, 2021), https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/.

[414] Charlotte Gifford, *The Problem with Emotion-Detection Technology*, New Econ. (June 15, 2020), https://www.theneweconomy.com/technology/the-problem-with-emotion-detection-technology; *see also* Crawford, *supra* note 411.

[415] Barrett et al., *supra* note 314, at 46.

[416] *Id.*; *see also* Gifford, *supra* note 414.

[417] Cheryl Teh, "*Every Smile You Fake" – an AI Emotion-Recognition System Can Assess How "Happy" China's Workers are in the Office*, Insider (June 25, 2021), https://www.insider.com/ai-emotion-recognition-system-tracks-how-happy-chinas-workers-are-2021-6.

[418] Douglas Heaven, *Why Faces Don't Always Tell the Truth About Feelings*, Nature (Feb. 26, 2020), https://www.nature.com/articles/d41586-020-00507-5; Vincent, *supra* note 412.

[419] Lauren Rhue, *Emotion-Reading Tech Fails the Racial Bias Test*, Conversation (Jan. 3, 2019), https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404.

counterparts, and Microsoft's Face API scores Black faces three times more "contemptuous" than White faces.[420]

A consumer cannot avoid harms resulting from emotion recognition technology because they may not understand the mechanism and cannot control how their emotional markers or other biometric data are categorized. Biometric categorization systems, which attempt to link an individual's biometric data to certain traits and proclivities, are similarly based on false assumptions and threaten dangerous repercussions. Far from an objective method of analysis, biometric categorization harkens back to the dark days of phrenology and physiognomy, when researchers attempted to draw inferences on an individual's character from their skull measurements and facial features. [421] These pseudoscientific techniques were used to fuel nationalism, white supremacy, and xenophobia, and the spurious science behind new biometric technologies threatens to entrench these same insidious power structures.[422] At least one company currently offers automated services that predict how likely someone is to be a terrorist or pedophile based only on facial features, and other researchers have claimed algorithms that can predict autism, detect a person's sexuality, or predict a person's likelihood of engaging in criminal behavior just from analyzing their face.[423]

---

[420] *Id.*

[421] Blaise Aguera y Arcas et al., *Physiognomy's New Clothes*, Medium (May 6, 2017), https://medium.com/@blaisea/physiognomys-new-clothes-f2d4b59fdd6a; *see also* Crawford, *supra* note 411.

[422] *Id.*

[423] *See* Sally Adee, *Controversial Software Claims to Tell Your Personality From Your Face*, New Scientist (May 27, 2016), https://www.newscientist.com/article/2090656-controversial-software-claims-to-tell-personality-from-your-face/; Press Release, Duke Pratt Sch. of Eng'g, *Researchers Are Using Machine Learning to Screen for Autism in Children* (July 11, 2019), https://pratt.duke.edu/about/news/amazon-autism-app-video; Paul Lewis, *"I was Shocked it was so Easy": Meet the Professor Who Says Facial Recognition Can Tell if You're Gay*, Guardian (July 7, 2018), https://www.theguardian.com/technology/2018/jul/07/artificial-intelligence-can-tell-your-sexuality-politics-surveillance-paul-lewis; Madhi Hashemi & Margaret Hall, *Criminal Tendency Detection from Facial Images and the Gender Bias Effect*, 7 J. Big Data, 1, 1 (2020), https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0282-4#Sec9 (since retracted); Luana Pascu, *Biometric Software that Allegedly Predicts Criminals Based on Their Face Sparks Industry Controversy*, Biometric Update (May 6, 2020), https://www.biometricupdate.com/202005/biometric-software-that-allegedly-predicts-criminals-based-on-their-face-sparks-industry-controversy.

Moreover, since predictive algorithms rely heavily on historical data, they tend to reproduce traditions and practices of the past that have been unjust to marginalized individuals. For instance, algorithms that purport to predict the likelihood of a person's criminality are trained using data from racist criminal justice systems that punish people of color at disproportionate rates, which results in a similarly racist algorithm.[424] Similarly, attempting to use biometric data to determine an individual's sexuality is not only methodologically flawed, but may also be used to discriminate against people believed to be gay.[425] Biometric technologies also frequently operate in trans-exclusive ways, since scientists inevitably use their own perceptions of gender to train their algorithms to recognize various traits, which means that these systems are infused with dominant norms and stereotypes.[426] Ultimately, biometric categorization systems tend to subject anyone whose appearance deviates from imposed norms to heightened scrutiny, resulting in larger burdens on people of color, gender minorities, and people with disabilities.[427]

Potential benefits to the consumer or competition do not outweigh the many harms of emotion recognition technology. Many software companies claim high rates of accuracy but refuse to produce evidence that proves these automated

---

[424] *See* Pascu, *supra* note 423; *see also* Luana Pascu, *Scientists, Sociologists Speak Out Against Biometrics Research that Allegedly Predicts Criminals*, Biometric Update (June 23, 2020), https://www.biometricupdate.com/202006/scientists-sociologists-speak-out-against-biometrics-research-that-allegedly-predicts-criminals; *Facial Recognition to "Predict Bias" Sparks Row Over AI Bias*, BBC News (June 24, 2020), https://www.bbc.com/news/technology-53165286; Abeba Birhane, *The Impossibility of Automating Ambiguity*, 27 MIT Artificial Life 44, 46 (2021), https://direct.mit.edu/artl/article-abstract/27/1/44/101872/The-Impossibility-of-Automating-Ambiguity (noting that predictive algorithms rely on historical data that reproduces harmful trends for marginalized individuals).

[425] James Vincent, *The Invention of AI "Gaydar" Could be the Start of Something Much Worse*, Verge (Sept. 21, 2017), https://www.theverge.com/2017/9/21/16332760/ai-sexuality-gaydar-photo-physiognomy; Sam Levin, *LGBT Groups Denounce "Dangerous" AI that Uses Your Face to Guess Your Sexuality*, Guardian (Sept. 8, 2017), https://www.theguardian.com/world/2017/sep/08/ai-gay-gaydar-algorithm-facial-recognition-criticism-stanford.

[426] *See* Rosa Wevers, *Unmasking Biometrics' Biases: Facing Gender, Race, Class and Ability in Biometric Data Collection*, 21 TMG J. Media Hist. 89, 92 (2018), https://www.tmgonline.nl/articles/10.18146/2213-7653.2018.368/; Os Keyes, *The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition*, 2 Proc. ACM on Hum.-Comput. Interaction 1, 12 (2018), https://ironholds.org/resources/papers/agr_paper.pdf.

[427] *See* Wevers, *supra* note 426.

techniques actually work, and other research has demonstrated how easy it is to "trick" these algorithms into perceiving certain emotions that don't reflect how an individual is truly feeling.[428] These systems are ineffective and often prone to error.[429] People will "bear the costs of systems that are not just technically imperfect, but based on questionable methodologies."[430] Emotion recognition programs threaten individual privacy and freedom of thought by constantly surveilling a person's demeanor and forcing people to act according to an algorithm's idea of "mainstream" behavior in order to avoid getting flagged.[431]

There is also danger of discrimination when automating "mainstream" behavior. "These tools can take us back to the phrenological past, when spurious claims were used to support existing systems of power."[432] For example, the employment and hiring software company HireVue disbanded its use of facial analysis in its facial and emotional recognition algorithms due to concerns of bias in job interviews.[433] In particular, "cultural biases can result in harmful discrimination for qualified candidates whose facial movements are judged unfavorably by a machine."[434] There are ongoing questions in the industry and scientific communities about whether facial expressions are an accurate or reliable indicator of emotions.[435] The inaccuracy and high risk involved with commercial use of emotion recognition technology does not benefit competition more than it harms consumers.

The commercial use of facial recognition and emotion recognition technologies is prevalent. The Commission has the authority to issue a rule banning the unfair use of one-to-many facial recognition and emotional recognition technologies because that use is prevalent. The commercial market for facial recognition technology is growing. It is used broadly for identification on smartphone applications (including for payment services on smartphones),[436]

---

[428] Heaven, *supra* note 418; Vincent, *supra* note 425.
[429] *See* Crawford, *supra* note 411.
[430] *Id.*
[431] Teh, *supra* note 417.
[432] Crawford, *supra* note 411.
[433] Jeremy Kahn, *HireVue drops facial monitoring amid A.I. algorithm audit*, Fortune (Jan. 19, 2021), https://fortune.com/2021/01/19/hirevue-drops-facial-monitoring-amid-a-i-algorithm-audit/.
[434] FRT in the Wild, *supra* note 390, at 9.
[435] Hill, *supra* note 405.
[436] GAO Facial Recognition Report, *supra* note 385, at 10.

airlines,[437] in schools and universities,[438] and mass surveillance in commercial settings like stadiums and arenas.[439] According to a recent Government Accountability Office report, "Market research, patent data, and the growing number of vendors participating in NIST vendor tests all suggest that the number and types of businesses that use facial recognition technology are increasing."[440] In the next two years, revenue for the global facial recognition technology market is projected to increase from $7 to $10 billion.[441] Additionally, the number of facial recognition related patents granted have increased and expanded into various industries including: "technology, retail, entertainment, insurance, and telecommunications companies, among others."[442]

Emotion detection and recognition is also a growing, multi-billion-dollar industry.[443] Under current trends, the market is expected to rise to $56 billion by 2024.[444] The technology is widely deployed in various areas of commerce. In addition to hiring and human resources applications,[445] emotion recognition is also used for advertising and marketing. CBS, Unilever, Mars, and Kellogg's have used it

---

[437] Sean O'Kane, *British Airways Brings its Biometric Identification Gates to Three More US Airports*, Verge (Mar. 9, 2018), https://www.theverge.com/2018/3/9/17100314/british-airways-facial-recognition-boarding-airports.
[438] *See* John S. Cusick & Clarence Okoh, *Why Schools Need to Abandon Facial Recognition, Not Double Down On It*, Fast Company (July 23, 2021), https://www.fastcompany.com/90657769/schools-facial-recognition; GAO Facial Recognition Report, *supra* note 385, at 12 ("[S]ome schools and universities use the technology to identify students in the classroom and keep track of their course attendance. In addition, one market research report stated that many educational institutions are using the technology to manage and authenticate the identities of students throughout online sessions, examinations, and certification activities.").
[439] *See* Draper, *supra* note 394.
[440] GAO Facial Recognition Report, *supra* note 385, at 8–9.
[441] *Id.*
[442] *Id.*
[443] Alexa Hagerty & Alexandra Albert, *AI Is Increasingly Being Used To Identify Emotions – Here's What's At Stake*, Conversation (Apr. 15, 2021), https://theconversation.com/ai-is-increasingly-being-used-to-identify-emotions-heres-whats-at-stake-158809.
[444] *Global Emotion Detection & Recognition Market Size is Projected to Grow from USD 21.6 Billion in 2019 to USD 56.0 Billion by 2024, at a CAGR of 21.0% - ResearchAndMarkets.com*, BusinessWire (Feb. 13, 2020), https://www.businesswire.com/news/home/20200213005614/en/Global-Emotion-Detection-Recognition-Market-Size-is-Projected-to-Grow-from-USD-21.6-Billion-in-2019-to-USD-56.0-Billion-by-2024-at-a-CAGR-of-21.0---ResearchAndMarkets.com.
[445] *See* Fortune, *supra* note 433.

for branding and advertisement development.[446] Disney, for example, has used emotion recognition to record facial expressions and infer audience reactions during movies and has deployed the technology at theme parks and restaurants to understand guest experiences.[447] Emotion recognition technology is also increasingly being considered for healthcare settings.[448]

To prevent the many serious and systemic harms that both technologies inflict on individuals, the Commission should adopt a categorical ban on commercial uses of one-to-many facial recognition and emotion recognition systems. Commercial use of one-to-many facial recognition is particularly dangerous: apart from its well documented history of bias and inaccuracy, the core function of the technology is inherently injurious to consumers. And research suggests that AI systems will never be able to classify human behavior accurately and consistently because human behavior is inherently open-ended, fluid, and ambiguous, rendering our behavioral pathways too complex and unpredictable for an automated system to grasp.[449] Because it is not possible to simply reform these technologies to be less biased or more accurate, their use in commercial settings should be banned in order to protect privacy, freedom, and civil rights.

---

[446] RTI International, *Facial Emotion Recognition Market Research Brief* 5 (July 2020), https://www.rti.org/brochures/facial-emotion-recognition*; see* Lora Kolodny, *Affectiva Raises $14 Million to Bring Apps, Robots, Emotional Intelligence*, TechCrunch (May 25, 2016), https://techcrunch.com/2016/05/25/affectiva-raises-14-million-to-bring-apps-robots-emotional-intelligence/.

[447] *See* Gianluca Mezzofiore, *Disney is Using Facial Recognition to Predict How You'll React to Movies*, Mashable (July 27, 2017), https://mashable.com/article/disney-facial-recognition-prediction-movies; Rosalyn Page, *10 Examples of Brands Using Emotion Analytics to Ramp Up Customer Engagement*, CMO (June 26, 2019), https://www.cmo.com.au/article/662788/10-examples-brands-using-emotion-analytics-ramp-up-customer-engagement/.

[448] *See* Nicole Martinez-Martin, *What Are Important Ethical Implications of Using Facial Recognition Technology in Healthcare?*, AMA J. Ethics (Feb. 2019), https://journalofethics.ama-assn.org/article/what-are-important-ethical-implications-using-facial-recognition-technology-health-care/2019-02.

[449] Birhane, *supra* note 424.

3. DISCRIMINATION

Responsive to questions 65–72.

3.1. It is an unfair practice to discriminate in or otherwise make unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, sexual orientation, disability, or other protected characteristics.

As discussed in many sections of these comments, commercial surveillance systems and automated decision-making systems can lead to discrimination harms. Targeting and profiling systems are designed to divide, segment, and score individuals based on their characteristics, their demographics, and their behaviors. In many cases, this means that consumers are sorted and scored in ways that reflect and entrench systematic biases. Automated decision-making systems can facilitate or exacerbate discrimination harms. Extensive research has established racial and gender bias in numerous facets of the commercial surveillance ecosystem.

EPIC supports the comments of the Lawyers' Committee for Civil Rights Under the Law and joins its call to the Commission to prohibit discrimination as an unfair practice under the FTC Act; to recognize a diverse array of protected characteristics; and to prohibit any commercial surveillance practices that result in discrimination—including targeted advertising.

The following section answers the Commission's specific questions regarding discrimination.

3.2. Responses to questions 65–72 regarding discrimination based on protected categories.

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

The prevalence of algorithmic discrimination in U.S. commerce is hard to precisely quantify because commercial algorithms are often treated as proprietary and competitive information and withheld as industry trade secrets.[450] Nevertheless,

[450] *Id.* at 1501–02; *see also* Simson Garfinkel, *A Peek at Proprietary Algorithms*, 105 Am. Scientist 326 (2017), https://www.americanscientist.org/article/a-peek-at-proprietary-algorithms.

legal, media, and scholarly sources demonstrate that algorithmic discrimination based on protected characteristics is widespread.[451]

Commercially marketed algorithms and algorithmic products can be divided broadly into two groups based on the applicability of federal anti-discrimination laws.[452] The first group of commercial algorithms are those used by entities subject to sector-specific federal anti-discrimination laws: algorithms meant to optimize decisions to extend credit, housing, employment, and healthcare. The second group includes commercial algorithms deployed across different sectors that may violate federal anti-discrimination laws depending on the context. This group includes algorithms used to enhance marketing and surveillance capabilities, such as targeted advertising and facial recognition technology.[453]

This section provides information about the prevalence of several different types of algorithmic discrimination that violate federal law, including: (1) credit discrimination, (2) discrimination enabled by targeted advertising, (3) discrimination enabled by biometric data, and (4) healthcare discrimination.

Credit discrimination. Federal law prohibits discrimination in access to credit based on certain protected characteristics.[454] The incidence of algorithmic

---

[451] *See generally* Anirudh VK, *How Is AI Changing the Finance, Healthcare, HR, and Marketing Industries?*, Spiceworks (Feb. 10, 2022), https://www.spiceworks.com/finance/fintech/articles/how-is-ai-changing-industries/; Benjamin Cheatham et al., *Confronting the Risks of Artificial Intelligence,* McKinsey & Co. (Apr. 26, 2019), https://www.mckinsey.com/capabilities/quantumblack/our-insights/confronting-the-risks-of-artificial-intelligence.

[452] Protected classes under federal law include racial, ethnic, religious, and national minorities; women; seniors; and people with certain disabilities or pre-existing medical conditions. Protections are generally limited to discrimination in access to credit, housing, employment, public accommodation, public education, healthcare programs receiving federal assistance, and jury service; and access to employment and insurance based on genetic information. *See* Mark MacCarthy, *Fairness in Algorithmic Decision-making*, Brookings Inst. (Dec. 6, 2019), https://www.brookings.edu/research/fairness-in-algorithmic-decision-making/.

[453] Tanya Kant, *Identity, Advertising, and Algorithmic Targeting: Or How (Not) to Target Your "Ideal User"*, MIT Case Stud. Soc. & Ethical Resp. Computing, Aug. 10, 2021, https://doi.org/10.21428/2c646de5.929a7db6.

[454] *See, e.g.*, Equal Credit Opportunity Act, 15 U.S.C. § 1691 *et seq.* (prohibiting credit discrimination); Fair Housing Act, 42 U.S.C. § 3601 *et seq.* (same).

discrimination in both credit scoring and lending decisions is well documented and prevalent.

Credit scoring algorithms. Credit scoring algorithms have in some cases been shown to discriminate based on ethnicity and race.[455] According to a study on credit data, majority-Black communities and majority-indigenous communities had the lowest median credit scores.[456] Research has found that credit data excludes information about the 1 in 10 U.S. adults who do not have a credit profile, a disproportionate amount of whom are people of color.[457]

Studies have found that people of color are given lower credit scores because proxies for creditworthiness used by the algorithm disproportionately affect people of color.[458] For example, Fannie Mae and Freddie Mac still require mortgage lenders to use the Classic FICO model, a credit scoring algorithm that was developed in the 1990s that has historically favored White borrowers by rewarding traditional measures of credit.[459] Traditional measures of credit include an individual's history of consistent credit and loan repayments and any negative financial performance, such as foreclosures and bankruptcies.[460]

Credit pricing algorithms. According to a 2019 study, algorithmic discrimination against Black and Latine/Latinx borrowers also occurs in mortgage

[455] *See* Citron & Pasquale, *supra* note 315, at 14–15.
[456] *Credit Health during the COVID-19 Pandemic*, Urb. Inst. (Mar. 8, 2022), https://apps.urban.org/features/credit-health-during-pandemic/.
[457] Kenneth P. Brevoort et al., Consumer Fin. Prot. Bureau Off. of Rsch., *Data Point: Credit Invisibles* 15 (2015), https://www.consumerfinance.gov/about-us/newsroom/cfpb-report-finds-26-million-consumers-are-credit-invisible/.
[458] *See* Lisa Rice & Deidre Swesnik, *Discriminatory Effects of Credit Scoring on Communities of Color*, 46 Suffolk L. Rev. 936, 952–53 (2013); Sahiba Chopra, *Current Regulatory Challenges in Consumer Credit Scoring Using Alternative Data-Driven Methodologies*, 23 Vand. J. Ent. & Tech. L. 625, 641 (2021).
[459] Emmanuel Martinez & Lauren Kirchner, *The Secret Bias Hidden in Mortgage-Approval Algorithms*, Markup (Aug. 25, 2021), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.
[460] *See* U.S. Gov't Accountability Off., GAO-19-111, *Agencies Should Provide Clarification on Lenders' Use of Alternative Data* 34 (2018); U.S. Gov't Accountability Off., GAO-22-104380, *Alternative Data in Mortgage Lending* 3 (2021).

loan pricing.[461] For example, the study found that algorithmic lenders charged Black and Latine/Latinx borrowers considerably more in interest for home purchase and refinance mortgages by 7.9 and 3.6 basis points, respectively.[462] The study estimated that the cost of extra interest resulting from algorithmic and in-person lending discrimination for Black and Latine/Latinx borrowers was $765 million per year.[463] And Black and Latine/Latinx borrowers paid 5.3 basis points and 2.0 base points more in interest for home purchase mortgages and refinance mortgages originated online, respectively.[464]

Discrimination in targeted advertising. Left unregulated, targeted advertising carries a high risk of algorithmic discrimination.[465] Most of the advertisements that consumers see online are driven by tracking and profiling systems that use algorithms[466] In 2021, Google was the largest online ad seller in the United States, accounting for 28.6% of the country's total annual online advertising revenue. Facebook and Amazon followed, accounting for 23.8% and 11.3%, respectively.[467] The impact of algorithmic targeting has been especially damaging to individuals seeking housing and employment because these systems have been used to enable discriminatory marketing.

Between 2016 and 2018, five employment and credit discrimination actions were brought against Facebook by civil rights groups, a national labor organization,

---

[461] Robert Bartlett et al., *Consumer-Lending Discrimination in the FinTech Era* 6 (Nat'l Bureau of Econ. Rsch., Working Paper No. 25943, 2019), https://www.nber.org/system/files/working_papers/w25943/w25943.pdf.
[462] *Id.* at 6.
[463] *Id.* at 1.
[464] *Id.* at 6.
[465] *See e.g.*, Emma Cott et al., *They Searched Online for Abortion Clinics. They Found Anti-Abortion Centers*, N.Y. Times (June 23, 2022), https://www.nytimes.com/interactive/2022/us/texas-abortion-human-coalition.html; Complaint for Permanent Injunction & Other Relief, *FTC v. Kochava, Inc.*, No. 2:22-cv-377 (D. Idaho filed Aug. 29, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf.
[466] Veronica Marotta et al., *Online Tracking and Publishers' Revenues: An Empirical Analysis* 13 (May 2019) (unpublished manuscript), https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.
[467] *Share of Amazon, Facebook, and Google in Net Digital Ad Revenue in the United States From 2019 to 2023*, Statista (Mar. 14, 2022), https://www.statista.com/statistics/242549/digital-ad-market-share-of-major-ad-selling-companies-in-the-us-by-revenue/.

workers, and consumers.[468] As part of the resulting settlements, Facebook agreed to launch a different advertising portal for credit, housing, and employment ads that would exclude options to place ads based on gender, age, religion, race, "ethnic affinity," or ZIP code.[469] However, in November 2019, Facebook was sued again by consumers for discriminating against older and female users by withholding ads for financial services such as bank accounts, insurance, investments and loans based on age and gender.[470] In December 2019, a study showed that bias persisted in Facebook's modified algorithm because it still relied on proxies that correlated with age or gender.[471] Yet again, in April 2021, The Markup found discriminatory credit ads from several companies that targeted specific age group of users.[472]

In June 2022, the Department of Justice and Meta (Facebook's parent company) entered into a settlement that resolved allegations that the company's advertising algorithms discriminated against consumers based on characteristics protected under the Fair Housing Act.[473] In its complaint, the DOJ alleged that

---

[468] *See* Nat'l Fair Hous. All., *Summary of Settlements Between Civil Rights Advocates and Facebook* 1-3 (Mar. 18, 2019), https://nationalfairhousing.org/wp-content/uploads/2022/01/3.18.2019-Joint-Statement-FINAL-1.pdf.

[469] *Id.*; *see also* Julia Angwin et al., *Facebook (Still) Letting Housing Advertisers Exclude Users by Race*, ProPublica (Nov. 21, 2017), https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin; Kaya Yurieff, *Facebook Settles Lawsuits Alleging Discriminatory Ads*, CNN (Mar. 19, 2019), https://www.cnn.com/2019/03/19/tech/facebook-discriminatory-ads-settlement.

[470] Jonathan Stempel, *Facebook Sued For Age, Gender Bias In Financial Services Ads*, Reuters (Oct. 31, 2019), https://www.reuters.com/article/us-%20facebook-lawsuit-bias/facebook-sued-for-age-gender-bias-in-financial-services-ads-idUSKBN1XA2G8; Ava Kofman & Ariana Tobin, *Facebook Ads Can Still Discriminate Against Women and Older Workers, Despite a Civil Rights Settlement*, ProPublica (Dec. 13, 2019), https://www.propublica.org/article/facebook-ads-can-still-discriminate-against-women-and-older-workers-despite-a-civil-rights-settlement.

[471] Piotr Sapiezynski et al., *Algorithms that "Don't See Color": Measuring Biases in Lookalike and Special Ad Audiences*, arXiv (May 31, 2022, 10:36 AM), https://arxiv.org/pdf/1912.07579.pdf; Kofman & Tobin, *supra* note 470.

[472] Corin Faife & Alfred Ng, *Credit Card Ads Were Targeted by Age, Violating Facebook's Anti-Discrimination Policy*, Markup (Apr. 29, 2021), https://themarkup.org/citizen-browser/2021/04/29/credit-card-ads-were-targeted-by-age-violating-facebooks-anti-discrimination-policy.

[473] Settlement Agreement, *United States v. Meta Platforms, Inc.*, No. 22-cv-05187 (S.D.N.Y. filed June 21, 2022), https://www.justice.gov/crt/case-document/file/1514126/download; Ariana Tobin & Ava Kofman, *Facebook Finally Agrees to Eliminate Tool That Enabled Discriminatory Advertising*, ProPublica (June 22, 2022), https://www.propublica.org/article/facebook-doj-advertising-discrimination-settlement.

Meta's advertising algorithm violated the FHA by "steering ads for housing in majority-White neighborhoods disproportionately to White users and steering ads for housing in majority-Black neighborhoods disproportionately to Black users."[474]

Discrimination using biometric data. The use of biometric identification and evaluation systems in employment and other settings also poses a significant risk of discrimination on the basis of protected characteristics.[475] In 2019, EPIC filed a complaint with the FTC urging the Commission to investigate HireVue, a hiring software that uses voice analysis (and previously facial recognition) to score applicants based on automated interviews. On May 12, 2022, the DOJ and the U.S. Equal Employment Opportunity Commission jointly issued guidance to employers explaining that AI-powered hiring tools, including video interviews, can violate both biometric data laws and the Americans with Disabilities Act.[476] The DOJ and EEOC explained that video interviewing software that evaluates candidates' skills and abilities based on their facial expressions and speech patterns could unfairly discriminate against disabled candidates.[477]

Healthcare discrimination. Federal law prohibits discrimination in access to healthcare based on certain protected characteristics.[478] The increasing prevalence of clinical algorithms in health care is well documented. Algorithms are often used

---

[474] Complaint, *United States v. Meta Platforms, Inc.*, No. 22-cv-05187 (S.D.N.Y. filed June 21, 2022), https://www.justice.gov/usao-sdny/press-release/file/1514051/download.
[475] *Cf. The Evolution of Biometric Data Privacy Laws*, Bloomberg L. (Nov. 4, 2021), https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws-and-lawsuits/. *See generally* Kerri Thompson, *Countenancing Employment Discrimination: Facial Recognition in Background Checks*, 8 Tex. A&M L. Rev. 63 (2020).
[476] Press Release, U.S. Dep't of Just., *Justice Department and EEOC Warn Against Disability Discrimination* (May 12, 2022), https://www.justice.gov/opa/pr/justice-department-and-eeoc-warn-against-disability-discrimination.
[477] U.S. Equal Emp. Opportunity Comm'n, EEOC-NVTA-2022-2, *The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees* (2022), https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence [hereinafter EEOC AI Hiring Report]; Civ. Rts. Div., U.S. Dep't of Just., *Algorithms, Artificial Intelligence, and Disability Discrimination in Hiring* (2022), https://beta.ada.gov/resources/ai-guidance/.
[478] *See* 42 U.S.C. §§ 2000d, 18116(a); *cf.* 42 U.S.C. § 2000ff *et seq.* (prohibiting discriminating in access to employment and health insurance based on genetic information). *But cf.* Sharona Hoffman & Andy Podgurski, *Artificial Intelligence and Discrimination in Health Care*, 19 Yale J. Health Pol'y L. & Ethics 3, 26–30 (2020) (highlighting underenforcement of algorithmic discrimination).

with the intention of optimizing drug research and development, improving medical treatment, deploying medical devices, and streamlining operations.[479] However, the incidence of algorithmic discrimination in clinical decisions has also been well documented, and a systemic review of the issue by the Agency for Healthcare Research and Quality, an agency of the Department of Health and Human Services, is underway.[480] The potential for bias in healthcare settings is especially troubling given that skewed decisions and recommendations can lead to mistreatment and bodily harm.

In 2020, the New England Journal of Medicine identified racial bias in clinical algorithms across different medical specialties: (1) Black patients at a hospital were disproportionately categorized at lower risk of fatal heart risk failure, which could have raised the threshold for expending resources for Black patients; (2) Black patients were categorized as having better kidney functions, which could have delayed referral to specialist care or listing for kidney transplant; (3) Black patients presented to the emergency department with flank pain were categorized at lower risk of kidney stones, which could have discouraged evaluation for kidney stones in Black patients; (5) Black and Latine/Latinx patients who had previously undergone a C-section were categorized at higher risk for complications during vaginal deliveries, excluding them from the possible health benefits of vaginal deliveries; and (6) Black patients were categorized at lower health risk than White patients with the same health level because the algorithm assigned risk scores based on past health care spending.[481]

---

[479] Daniel Cohen et al., *Healthtech In the Fast Lane: What Is Fueling Investor Excitement?*, McKinsey & Co. (Dec. 1, 2020), https://www.mckinsey.com/industries/life-sciences/our-insights/healthtech-in-the-fast-lane-what-is-fueling-investor-excitement.

[480] Agency for Healthcare Rsch. & Quality, U.S. Dep't of Health & Hum. Servs., *Impact of Healthcare Algorithms on Racial and Ethnic Disparities in Health and Healthcare* (2022), https://effectivehealthcare.ahrq.gov/sites/default/files/product/pdf/racial-disparities-health-healthcare-protocol.pdf; *see also* Gina Kolata, *Many Medical Decision Tools Disadvantage Black Patients*, N.Y. Times (June 17, 2020), https://www.nytimes.com/2020/06/17/health/many-medical-decision-tools-disadvantage-black-patients.html.

[481] Darshali Vyas et al., *Hidden in Plain Sight – Reconsidering the Use of Race Correction in Clinical Algorithms*, 383 New Eng. J. Med. 874, 879 (2020), https://www.nejm.org/doi/full/10.1056/NEJMms2004740.

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

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

Algorithmic discrimination affects consumers both directly and indirectly. Discriminatory algorithmic practices reduce innovation and competition, encourage monopolies and market control, and induce systemic unfairness and inequity.

Algorithmic discrimination affects consumers both directly and indirectly. Consumers interact with algorithms constantly. Discriminatory algorithms impact those who are discriminated against directly (e.g., job applicants) as well as those who are indirectly harmed (e.g., employers—"consumers" of job applicants in the labor market—who lose access to highly qualified job applicants screened out on discriminatory grounds).

When searching for employment, algorithms can influence which jobs are shown to the applicant.[482] Even if a job is shown to the applicant, other algorithms may predict the candidate's desired salary and assess whether the candidate meets minimum qualifications.[483] These predictive systems often rely on prior hires as data, which can reinforce existing institutional biases.[484] In addition to employers, insurance companies use algorithms to calculate appropriate insurance premiums, taking into account various risk variables.[485] If the algorithm determines that an applicant lives in a majority-minority area, the rate may be higher compared to an applicant in a White neighborhood even if other factors are the same.[486] Landlords use tenant screening algorithms, which often erroneously flag applicants as having criminal backgrounds.[487] These examples are just the tip of the iceberg of algorithmic

[482] Miranda Bogen & Aaron Rieke, Upturn, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias* 21 (2018), https://www.upturn.org/work/help-wanted/.
[483] *Id.* at 26, 39.
[484] *Id.* at 28–29.
[485] Julia Angwin et al., *Minority Neighborhoods Pay Higher Car Insurance Premiums Than White Areas With the Same Risk*, ProPublica (Apr. 5, 2017), https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk.
[486] *Id.*
[487] *Id.*

discrimination. Direct discrimination is also present in education,[488] access to credit,[489] and healthcare,[490] and other fields.

Even those consumers who are not the direct targets of discrimination can be indirectly harmed by such practices—such as an employer who loses out on qualified job applicants who are screened out, based on protected characteristics, by a third-party algorithm. Further, the use of algorithms to make profiling-based decisions will likely lead to an uneven chilling effect on certain populations.[491] Algorithmic decision-making leads to traditional chilling—the self-censorship of action—and an indirect social chilling where behavior is not just prevented or allowed but shaped in a certain way.[492] The sale and repurposing of personal data also contributes to individual reticence to participate in certain activities.[493] Thus, individuals may be guided towards certain activities and chilled from participation in others.

Additionally, the use of profiling and decision-making algorithms has two other adverse effects on consumers. First is the privatization of public decisions,[494] such as which individuals are considered 'risky.' Second is the normalization of discrimination, as the lack of human control over algorithms and the lack of a 'mind'

---

[488] *See* Benjamin Herold, *Schools Are Deploying Massive Digital Surveillance Systems. The Results Are Alarming*, Educ. Wk. (May 30, 2019), https://www.edweek.org/technology/schools-are-deploying-massive-digital-surveillance-systems-the-results-are-alarming/2019/05.
[489] *See* Persis Yu et al., Nat'l Consumer L. Ctr., *Big Data: A Big Disappointment for Scoring Consumer Credit Risk* 27 (2014), https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf.
[490] *See* Heidi Ledford, *Millions of black people affected by racial bias in health-care Algorithms*, Nature (Oct. 26, 2019), https://www.nature.com/articles/d41586-019-03228-6.
[491] *See* Jonathan W. Penney, *Understanding Chilling Effects*, 1452 Mn. L. Rev 1455, 1523–25 (2022).
[492] *See id.* at 1479–87.
[493] Karen Yeung, Steering Comm. on Media & Info. Soc'y, *A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework*, Council Eur. (2018), https://rm.coe.int/a-study-of-the-implications-of-advanced-digital-technologies-including/168096bdab.
[494] *Id.*

or *mens rea* tends to reduce the perceived moral harm of algorithmic discrimination compared to human discrimination.[495]

Algorithmic discrimination stifles innovation and competition. Algorithms provide new opportunities for anti-competitive collusion since algorithms can lead to tacit "agreement" without human interaction.[496] One example is price discrimination: sellers often use similar data sets leading to tacit collusion between algorithms.[497] This can lead to price fixing, as algorithms "discover" that coordinating prices is an effective method to maximize profits.[498]

Algorithmic systems can also act as market gatekeepers and reduce competition by excluding outsiders or altering rankings to minimize competition in-market.[499] These actions reduce the incentive for companies to innovate and reduce the overall competitive nature of the marketplace.

Restrictions on discrimination by automated decision-making systems would benefit all consumers. Properly regulated, algorithm developers and controllers would implement controls to ensure that their algorithms do not discriminate against protected classes. Rules to this end stand to benefit all consumers and market participants by promoting fairness and equity in the market.

Even where algorithms rely on facially neutral personal traits—for example, income, hobbies, or spending habits—they may nevertheless cause disparate impact

---

[495] Yochanan E. Bigman et al., *Algorithmic Discrimination Causes Less Moral Outrage Than Human Discrimination*, J. Experimental Psych. Gen., 2022, at 6–7, 9, https://www.apa.org/pubs/journals/releases/xge-xge0001250.pdf; Andrea Bonezzi & Massimiliano Ostinelli, *Can Algorithms Legitimize Discrimination?*, J. Experimental Psych. Applied, Mar. 22, 2021, at 4, 7–8, https://www.researchgate.net/profile/Andrea-Bonezzi/publication/350299764_Can_algorithms_legitimize_discrimination/links/609679e2458515d3150491fa/Can-algorithms-legitimize-discrimination.pdf.

[496] *See* OECD, *Algorithms and Collusion: Competition Policy in the Digital Age* 34 (2017), https://www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm.

[497] *Id.* at 16.

[498] *See* Allen Grunes, *Two New Papers Suggest Antitrust Law is Not Equipped to Address Personalized Pricing and Algorithmic Cartels*, ProMarket (July 14, 2022), https://www.promarket.org/2022/07/14/two-new-papers-suggest-antitrust-law-is-not-equipped-to-address-personalized-pricing-and-algorithmic-cartels/.

[499] U.K. Competition & Mkts. Auth., *supra* note 382.

by relying on proxies for protected characteristics.[500] Traditional proxy discrimination is exemplified by practices such as redlining, wherein facially neutral proxies (e.g., a ZIP code) enable discrimination.[501] Depending on the design process for an algorithm, proxies for protected characteristics may develop without human input.[502] For example, Amazon used automated employment screening software that developed proxies for screening out women.[503] The system "learned" to discriminate against women based on proxies like attendance at an historically women's college or participation in a women's chess club.[504]

Disparate impacts from algorithms can negatively affect market participants at all levels, even though employees and other consumers subject to discriminatory impact are the ones most directly affected. An employer like Amazon may be harmed if, due to a discriminatory algorithm, the employer is deterred from fully considering well qualified applicants. This type of discrimination also affects consumers as a whole: the job market is less efficient and competitive if an algorithm effectively bars strong applicants from consideration. It is therefore critical for all consumers that the Commission's rule on commercial surveillance prohibit disparate impact[505]—not merely decision-making expressly based on membership in a protected class.

Algorithmic discrimination is pervasive in modern commerce. It affects consumers indirectly and directly. It reduces innovation and competition and encourages monopolies and market control. Given the rapidly evolving nature of algorithms and their cross-cutting commercial applications, the Commission should

---

[500] Schwarcz & Prince, *supra* note 272, at 1260–64 (2020), https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1695&context=faculty_articles.
[501] *Id.* at 1268–69.
[502] *Id.* at 1262–64, 1275–76.
[503] Dastin, *supra* note 339; Rebecca Heilweil, *Why algorithms can be racist and sexist*, Vox (Feb. 18, 2020), https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency.
[504] *Id.*
[505] Subject only to "narrowly tailored exceptions . . . for affirmative action, diversity initiatives, and programs for self-testing to identify biases." Laws.' Comm. Civ. Rts. Under L., *Comments in Response to the Advanced Notice of Proposed Rulemaking* 60 (Nov. 2022), https://www.lawyerscommittee.org/wp-content/uploads/2022/11/LCCRUL-FTC-Privacy-Comments.pdf.

develop new anti-discrimination rules rather than expecting existing structures to do the job.

> Question 67. How should the Commission address such algorithmic discrimination? Should it consider new trade regulation rules that bar or somehow limit the deployment of any system that produces discrimination, irrespective of the data or processes on which those outcomes are based? If so, which standards should the Commission use to measure or evaluate disparate outcomes? How should the Commission analyze discrimination based on proxies for protected categories? How should the Commission analyze discrimination when more than one protected category is implicated (e.g., pregnant veteran or Black woman)?

As algorithmic discrimination has grown prevalent, the dangers have become more pronounced. And yet consumers remain largely powerless against algorithmic discrimination and the harms it causes—particularly to people of color, women, and low-wage workers.[506] The Commission should promulgate rules to combat algorithmic discrimination and stop unfair and deceptive business practices.[507]

There is mounting evidence of algorithmic discrimination in employment, online advertising, credit, healthcare, and housing. This discrimination can often be categorized in one of three ways: denial of a benefit, exclusion from opportunity, or predatory targeting.[508] Algorithms can change society by perpetuating, reinforcing, or surfacing discriminatory patterns, leading to disparate outcomes, over-monitoring, and over-policing.[509]

This is a problem of increasing importance as algorithms have grown in prominence. The artificial intelligence market has doubled in the last year, with

---

[506] *See* Monique Mann & Tobias Matzner, *Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination*, Big Data & Soc'y, July–December 2019, at 2.
[507] For FTC authority, see 15 U.S.C. § 45(n).
[508] *See* Rebecca Kelly Slaughter, Comm'r, FTC, Remarks of Federal Trade Commissioner Rebecca Kelly Slaughter at the UCLA School of Law 15–16 (Jan. 24, 2020), https://www.ftc.gov/system/files/documents/public_statements/1564883/remarks_of_commissioner_rebecca_kelly_slaughter_on_algorithmic_and_economic_justice_01-24-2020.pdf.
[509] *See* Mann & Matzner, *supra* note 506; *see generally* Noble, *supra* note 18.

private investment reaching $93.8 billion.[510] Google alone has reportedly collected information on 70% of American credit and debit transactions.[511] Unfair and deceptive business practices are now so prevalent that the Commission must promulgate rules rather than rely on case-by-case adjudication to develop standards. The time to act is now. As algorithmic complexity increases and the use of big data becomes more ubiquitous, it will be more difficult to identify, control for, and combat algorithmic discrimination.

We lay out our specific recommendations for rules concerning algorithmic discrimination in the previous section. However, we highlight two points here: the need for the Commission to adopt a disparate impact standard and the need for an effective rule to account for intersectional discrimination.

Rather than focusing narrowly on discriminatory intent when evaluating the fairness of an algorithm, the Commission should focus on disparate impact, which turns on the effects of an algorithm. As discussed below, many federal civil rights laws provide for consideration of disparate impact. Disparate impact results from practices, or in this case algorithms, that may be facially neutral but nevertheless have a discriminatory effect. Given the challenges in identifying differential treatment and discriminatory intent, an approach that focuses on disparate impact will be more successful in preventing discrimination than would a traditional discriminatory intent framework.

The Commission should borrow from existing civil rights statutes to develop a rule that prohibits algorithms causing disparate outcomes, regardless of discriminatory intent. Title VII of the Civil Rights Act prohibits discrimination by employers that causes disparate impact based on race, sex, national origins, color, or religion if the practice is not "job related for the position in question and consistent with business necessity" and if there is no alternative employment practice that

---

[510] *Artificial intelligence market size to hit US$ 1,811.9 billion by 2030*, BioSpace (Aug. 10, 2022), https://www.biospace.com/article/artificial-intelligence-market-size-to-hit-us-1-811-9-billion-by-2030/.

[511] Erin Simpson & Adam Conner, *How To Regulate Tech: A Technology Policy Framework for Online Services,* Ctr. for Am. Progress (Nov. 16, 2021), https://www.americanprogress.org/article/how-to-regulate-tech-a-technology-policy-framework-for-online-services/.

would meet the needs of the employer without causing the disparate impact.[512] The Equal Credit Opportunity Act also relies on a disparate impact standard,[513] as does the Fair Housing Act.[514]

A disparate impact analysis for commercial algorithms could entail a three-stage inquiry: first, whether the algorithm disproportionately impacts a protected class; second, whether the algorithm serves a valid purpose; and third, whether there are alternative approaches that could achieve the legitimate objective with a less disparate impact.[515] Success at the first stage may be complicated by a lack of reliable data or other evidence (one reason why the FTC should include in its proposed rule a provision that requires greater algorithmic transparency).[516] In the second stage, a business would need to demonstrate that its algorithm achieved a legitimate objective; and in stage three, a company would need to show it had no alternative model with equivalent predictive value but a lesser impact on the protected classes.[517] Adopting this approach would also guard against the reliance of algorithms on proxies.

It is also important for the Commission to account for intersectionality: the ways in which patterns or systems of inequality can combine to affect individuals or groups who are multiply marginalized. Leading scholars including Profesor Kimberlé Crenshaw have shown that when there are two forms of discrimination—for example, discrimination based gender and race, or gender and sexuality—the harms are compounded.[518] In *Algorithms of Oppression*, Dr. Safiya Noble described

---

[512] 42 U.S.C. §§ 2000e-2(a)–(b); *see also* Mark McCarthy, *Standards of Fairness for Disparate Impact Assessment of Big Data Algorithms*, 48 Cumb. L. Rev. 68, 76 (2019). *But see Alexander v. Sandoval*, 532 U.S. 275, 285–87 (2001).
[513] McCarthy, *supra* note 512, at 80; *cf.* 15 U.S.C. § 1691(a)(1).
[514] 42 U.S.C. § 3604(a); *Tex. Dep't of Hous. & Cmty. Affs. v. Inclusive Cmtys. Project, Inc.*, 576 U.S. 519, 545–47 (2015).
[515] McCarthy, *supra* note 512, at 82.
[516] McCarthy, *supra* note 512, at 82–83.
[517] *Id.*
[518] *See* Kimberlé Crenshaw, *Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color*, 43 Stan. L. Rev. 1241, 1280 (1991); Kimberlé Crenshaw, *Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics*, 1989 U. Chi. Legal F. 139, 148–50 (1989); Kimberlé Crenshaw, *The Urgency of*

how a Google search for "Black girls" produced search results of sexualized images and porn websites.[519] Meanwhile a search for "beautiful" produced images of almost exclusively White women in bikinis or lingerie. After this critique, Google adjusted its algorithm and the results improved, suggesting there was no justifiable basis for the disparate impact. In developing standards for identifying and preventing disparate impact, the Commission must be mindful of the special harms that can result from intersectional discrimination.

The Commission should promulgate rules to limit and prevent harm to consumers caused by algorithmic decision-making, a practice that increasingly exposes marginalized individuals to discrimination without their knowledge. Whether intentionally discriminatory or not, such algorithms can have discriminatory outcomes that the FTC has a responsibility to mitigate and eliminate. The Commission should ensure greater transparency, safeguard against potential harm, and create an environment in which algorithmic decision-making can instead, in Commissioner Slaughter's words, promote economic and social justice by "distributing opportunity more broadly, resources more efficiently, and benefits more effectively."[520]

> Question 68. Should the Commission focus on harms based on protected classes? Should the Commission consider harms to other underserved groups that current law does not recognize as protected from discrimination (e.g., unhoused people or residents of rural communities)?

Commercial surveillance has transformed the way that consumers participate in the economy. By its nature, a commercial surveillance economy exploits consumers.[521] A lack of regulation has facilitated the unrestrained extraction of consumer data, which has led to the widespread use of statistical models and

---

Intersectionality, TED (2016), https://www.ted.com/talks/kimberle_crenshaw_the_urgency_of_intersectionality/transcript?language=en.

[519] *See* Sean Illing, *How Search engines are making us more racist,* Vox (Apr. 6, 2018), https://www.vox.com/2018/4/3/17168256/google-racism-algorithms-technology.

[520] Slaughter, *supra* note 508.

[521] *See* Zuboff, *supra* note 16, at 8 (explaining that consumers are the sources from which the informational "surplus" is extracted and that the true customers are the firms that purchase it).

algorithmic tools to bend consumer behavior to the corporate will.[522] Consumers are increasingly the subject of harmful algorithmic decision-making that can neither be verified nor contested.[523] Though we may not yet fully realize the extent of consumer harms, it is clear that consumer harms do not just exist in theory.[524]

Though lack of regulation introduces new risks that impact a broad range of consumers, the Commission must give special attention to harms inflicted on protected classes. Below, we illustrate the ways in which harmful data practices further subordinate historically disadvantaged consumers and argue that practices indicating a pattern of discrimination fit squarely within the FTC's unfairness authority.

Algorithmic decision-making systems and other commercial surveillance practices inflict disproportionate harm on marginalized groups and individuals. The statistical legitimization of decisions that produce disparate impact will subject historically disadvantaged consumers to systematic disadvantageous determinations in the future.[525] The result is the further subordination of vulnerable and marginalized consumers.[526]

For example, in the context of tenant screening algorithms, tenants' interactions with eviction court are considered directly relevant to tenants' ability to pay rent.[527] Notably, tenant screening algorithms weigh all interactions with eviction

---

[522] *See* EPIC FTC AI Petition, *supra* note 8.
[523] *Id.*
[524] Schwarcz & Prince, *supra* note 500, at 1279–80 (2020) (citing Leslie Scism, *New York Insurers Can Evaluate Your Social Media Use – If They Can Prove Why It's Needed*, Wall St. J. (Jan. 30, 2019), https://www.wsj.com/articles/new-york-insurers-can-evaluate-your-social-media-useif-they-can-prove-why-its-needed-11548856802) (discussing how life insurance companies are scraping data from social media profiles to predict consumers' life expectancy for the purpose of setting premium rates).
[525] *See* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Calif. L. Rev. 671, 691 (2016).
[526] Inioluwa Deborah Raji et al., *Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing*, Proc. 2020 Conf. Fairness, Accountability, & Transparency 42 (Jan. 27, 2020), https://dl.acm.org/doi/10.1145/3351095.3372873; *see also* Schwarcz & Prince, *supra* note 500, at 1295–97.
[527] *See* Matthew Harold Leiwant, Note, *Locked Out: How Algorithmic Tenant Screening Exacerbates the Eviction Crisis in the United States*, 6 Geo. L. Tech. Rev. 276, 280 (2022).

court equally against the tenant, including claims in which the tenant prevailed.[528] However, there exists a strong correlation between eviction court interactions and Black women.[529] One reason for this correlation is that eviction proceedings are often brought against tenants who refuse to pay rent until code violations are fixed.[530] Because consumers from Black communities are more likely to live in rental housing with code violations, consumers from Black communities tend to be overrepresented in the data.[531] As a result, the use of tenant screening algorithms make it harder for Black communities—and for Black women specifically—to secure housing.[532]

Data-based decisions can reinforce harmful feedback loops because scalability can magnify biases and errors in the underlying data and make them "more durable."[533] Data-based decisions tend to enjoy a presumption of truth;[534] however, such decisions are only as good as the assumptions embedded in the data.[535] A reliance on inaccurate or misrepresentative data perpetuates—and can potentially even magnify—human biases and structural and institutional inequalities existing in

---

[528] *See id.* at 285.
[529] *Id.* at 282–83 (citing Matthew Desmond, *Eviction and the Reproduction of Urban Poverty*, 118 Am. J. Socio. 88, 91, 98–99 (2012) (finding that evictions are five times more likely to occur in predominantly Black neighborhoods and that Black women are two and a half times more likely than men to be brought to eviction court).
[530] *Id.*
[531] *Id.*
[532] *See id.* at 284.
[533] Mitra V. Yazdi, *The Digital Revolution and the Demise of Democracy*, 23 Tul. J. Tech. & Intell. Prop. 61, 68–69 (2021) (quoting Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 Yale J.L. & Tech. 103, 129 (2018) (explaining that algorithmic models "pose new risks of unfairness and error because where a problem exists, it will be worse and more durable")); *see also* Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (2017) (referring to feedback loops created by algorithms as "Weapons of Math Destruction" or "WMD feedback loops").
[534] Kate Crawford, *Think Again: Big Data*, Foreign Pol'y (May 10, 2013), https://foreignpolicy.com/2013/05/10/think-again-big-data/.
[535] Charlotte A. Burrows, Comm'r, Equal Emp. Opportunity Comm'n, *Remarks at the Equal Emp. Opportunity Comm'n Meeting of October 13, 2016: Big Data in the Workplace: Examining Implications for Equal Employment Opportunity Law* (2016), https://www.eeoc.gov/meetings/24068/transcript [https://perma.cc/7LHT-T9FL] ("In short, the algorithms used to assess big data are only as good as the assumptions that underlie them.").

the offline world.[536] The reinforcement of harmful feedback loops is likely when algorithms rely on datasets that have missing, incorrect, or unrepresentative data.[537] In addition, the magnification of harmful biases and errors is a risk when decision-making is done on a massive scale.[538] While it is true that human decision-making can also produce discriminatory harms, "the impact of one biased human [decision-maker] . . . is constrained in comparison to the potential adverse reach of algorithms that could be used to exclude millions . . . ."[539] Using Amazon's hiring tool as an example, scalability amplified old patterns of biased and discriminatory hiring practices, causing the algorithm tool to perpetuate and exacerbate the existing gender gap in tech.[540]

A distinct but related danger can arise as a result of algorithmic models' design. For instance, a flawed formulation of problem the algorithm is programmed to resolve can unintentionally replicate, and even magnify, the inequitable distribution of risk that protected groups experience already as a result of systemic disparities.[541] This becomes increasingly likely as the algorithm becomes more complex.[542] Specifically, problems involving "[q]uestions about social life" create heightened risk because such questions are often "vague and not sufficiently operationalized into discrete variables."[543] Thus, ethical and legal challenges result

---

[536] *See e.g.*, Christopher K. Odinet, *The New Data of Student Debt*, 92 S. Cal. L. Rev. 1617, 1670–73 (2019) (explaining how the "structural inequities of American society may very well only be reified through the use of 'highly predictive' . . . data").
[537] Chinmayi Arun, *AI and the Global South: Designing for Other Worlds*, *in The Oxford Handbook of Ethics of AI* 588, 600–01 (Markus D. Dubber et al. eds., 2020).
[538] See Odinet, *supra* note 536, at 1679–80.
[539] *Id.* at 1679 ("The new phenomenon of concern here is that due to the 'volume, velocity, and variety' of data used in automated hiring, any bias introduced in the system will be magnified and multiplied, greatly dwarfing the impact of any prejudice held by any one human manager.").
[540] *See id.*; *see also* Pamela Maynard, *Are We Really Closing The Gender Gap In Tech?*, Forbes (Mar. 3, 2021), https://www.forbes.com/sites/forbesbusinesscouncil/2021/03/03/are-we-really-closing-the-gender-gap-in-tech/(discussing a recent study that found the gender gap is, when taken as a whole, worse now for women in the technology industry than it was in 1984); Arun, *supra* note 537, at 600–01; *see generally* O'Neil, *supra* note 533 (explaining how algorithmic models create feedback loops).
[541] *See* Mehtab Khan & Alex Hanna, *A Framework for Dataset Accountability*, 19 Ohio St. Tech. L.J. 1, 55 (forthcoming 2023).
[542] *See id.*
[543] *Id.*

when complex problems "must be *made* into questions that data science can answer."[544]

For example, the healthcare system relies on risk assessment algorithmic models to "identify and help patients with complex health needs."[545] A study by Obermeyer et al. set out to find why the scores generated by such algorithmic models indicate that Black patients are less in need than White patients, when, in fact, Black patients are often sicker due to untreated illnesses.[546] The study found that some widely used models incorrectly relied on increased healthcare expenditures as a marker for greater healthcare need.[547] Ultimately, such models predicted health care costs rather than actual need, resulting in significant racial bias against Black patients who spend less on healthcare due to "systemic disparities in healthcare access."[548] Thus, the faulty formulation of the problem resulted in a feedback loop, wherein Black patients would receive less healthcare in the future because they have been denied healthcare access in the past.

The evolution of credit scoring exemplifies the feedback loop phenomenon in both off- and online contexts. Historically, the credit scoring system has been criticized for its exclusion of racial and ethnic minorities.[549] The use of nontraditional data by fintech lenders is advertised as promoting equal economic opportunity by extending credit access to those who are excluded under traditional credit scoring systems.[550] Yet the unregulated use of nontraditional data can facilitate the ability of

---

[544] *Id.* (quoting Samir Passi & Solon Barocas, *Problem Formulation and Fairness*, Proc. 2019 Conf. on Fairness, Accountability, & Transparency (Jan. 2019), https://doi.org/10.1145/3287560.3287567).
[545] Obermeyer et al., *supra* note 277, at 447–453.
[546] *See id.*
[547] *See id.*
[548] Khan & Hanna, *supra* note 72, at 55.
[549] *See e.g.*, Jennifer Brown, Assoc. Dir., Econ. Pol'y Project, UnidosUS, *Unscoreable: How the Credit Reporting Agencies Exclude Latinos, Younger Consumers, Low-Income Consumers, and Immigrants* (Feb. 26, 2019), https://www.congress.gov/116/meeting/house/108945/witnesses/HHRG-116-BA00-Wstate-BrownJ-20190226.pdf.
[550] *See* Emily Rosamond, *"All Data is Credit Data:" Reputation, Regulation and Character in the Entrepreneurial Imaginary*, 25 Paragrana 112, 114 (2016); *see also* Lorena Rodriguez, *All Data Is Not Credit Data: Closing the Gap Between the Fair Housing Act and Algorithmic Decisionmaking in the Lending Industry*, 120 Colum. L. Rev. 1843, 1852–61 (2020) (comparing traditional underwriting with credit-scoring by fintech lenders, who utilize nontraditional data).

lenders' to engage in predatory lending practices, thereby replicating the structural inequalities attributed to traditional forms of credit scoring.[551]

When determining the likelihood that a consumer will pay back their loan, fintech lenders are increasingly employing nontraditional data, such as information about a borrower's shopping patterns, browsing habits, social media interests, text messaging habits, health records, and geolocation.[552] For example, ZestFinance considered data such as the speed at which a loan applicant scrolled through an online terms-and-conditions disclosure.[553] The faster the loan applicant scrolled, the higher the risk.[554] ZestFinance claimed that its "all data is credit data" approach[555] to credit-scoring would not only provide more accurate predictions, but would also promote economic opportunity by giving underbanked borrowers access to credit.[556] Ironically, ZestFinance got out of the payday loan business and rebranded itself as Zest AI after it entered into a settlement with borrowers for charging excessive interest rates, some as high as 490%.[557]

A recent investigation in the student loan space revealed a pattern by some fintech lenders of charging higher interest rates to student borrowers attending Historically Black Colleges or Universities.[558] In response to allegations of "educational redlining," Upstart Network, LLC, has maintained that it only

---

[551] Slaughter et al., *supra* note 245, at 22; *see also* Rodriguez, *supra* note 550, at 1858 (discussing how the unfair history of credit scoring is being replicated in algorithmic decision-making).
[552] Rodriguez, *supra* note 550, at 1858.
[553] *Id.* at 1859.
[554] *See id.*
[555] *See* Rosamond, *supra* note 550, at 114 (quoting N.Y. Times interview with Douglas Merrill, former ZestFinance CEO).
[556] *Id.* at 117 (discussing fairness and quoting Wired UK interview with Douglas Merrill, former Zest Finance CEO).
[557] *See* Press Release, Zest AI, *Zest Settles All Claims, Cuts Ties With Payday Lending* (Sept. 11, 2020), https://www.zest.ai/insights/zest-settles-all-claims-cuts-ties-with-payday-lending; Brian Brueggemann, *Former Google exec's company gets caught in 'rent-a-tribe' class action lawsuits; Interest rates allegedly as high as 490%*, Legal Newsline (Apr. 2, 2019), https://legalnewsline.com/stories/512366003-former-google-exec-s-company-gets-caught-in-rent-a-tribe-class-action-lawsuits-interest-rates-allegedly-as-high-as-490.
[558] Katherine Welbeck & Ben Kaufman, *Fintech Lenders' Responses to Senate Probe Heighten Fears of Educational Redlining*, Student Borrower Prot. Ctr. (July 31, 2020), https://protectborrowers.org/fintech-lenders-response-to-senate-probe-heightens-fears-of-educational-redlining/.

considers its borrowers' schools for the purpose of knowing the schools' average incoming standardized test scores.[559] Upstart uses test scores to determine which of eight groups a borrower's school falls into.[560] Groups with lower average test scores are considered higher risk.[561] However, Upstart's model is problematic because minority students are underrepresented in top ranked schools, which have higher incoming standardized test scores.[562] Of Upstart's eight groups, 96% of HBCUs fall into the bottom four groups.[563] Though Upstart's model may not know whether the borrower attended an HBCU, it nonetheless ranks most borrowers attending HBCUs in the lowest tiers[564] and accordingly offers such borrowers less favorable terms of credit reflecting increased risk.

Some fintech lenders have considered the number of times students visited colleges with their parents.[565] Though the number of times a student visited colleges has been linked to increased likelihood of degree completion, the feature disfavors students without the economic means to visit schools as well as students from rural areas where institutions of higher education are sparse ("education deserts").[566] This feature also disparately impacts Native American students, 30% of whom live in education deserts.[567] By offering favorable terms to the same borrowers who have access to credit under traditional credit-scoring systems, this feature reinforces existing feedback loops that systematically disadvantage some student borrowers.[568]

Though commercial surveillance introduces risks across all consumer groups, consumers from protected classes and marginalized groups typically experience the

[559] *See id.*
[560] *See id.*
[561] *Id.*
[562] *See* Odinet, *supra* note 536, at 1622.
[563] *See id.*
[564] *See id.*
[565] *See* Odinet, *supra* note 536, at 1670–73 (citing Daniel Princiotta et al., *Social Indicators Predicting Postsecondary Success* 56–58 (2014), https://www.childtrends.org/wp-content/uploads/2014/05/2014-21SocialIndicatorsLumina.pdf).
[566] *See id.*
[567] *Id.* (explaining that "education deserts" have large Native Americans populations).
[568] *See id.* at 1672.

most acute harms. By exercising its rulemaking authority to declare digital discrimination unlawful, the Commission can begin to change that reality.

Practices indicating a pattern of discrimination fit squarely within the FTC's unfairness authority.[569] The Commission has the authority under section 5 to issue trade regulation rules that define specific commercial practices it deems unfair.[570] The term "unfair" has been used for decades by courts to describe discrimination based on protected characteristics, such that "discrimination" and "unfairness" have often been used synonymously.[571] The theory of unfairness-discrimination argues that unlawful discrimination should be prohibited under state and federal laws that prohibit "unfair, deceptive (and sometimes abusive) acts and practices." As former Commissioner Rohit Chopra writes, discriminatory practices are often "three for three, causing grievous harm that cannot be avoided."[572] Thus, because "[t]his relationship between discrimination and fairness is intuitive and ubiquitous," data practices indicating a pattern of discrimination fit squarely within the FTC's section 5 authority.[573]

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

Though existing civil rights laws may sometimes reach the discriminatory practices of entities that use algorithms in their decision-making processes,[574] the

---

[569] Stephen Hayes & Kali Schellenberg, *Discrimination Is "Unfair": Interpreting UDA(A)P to Prohibit Discrimination*, Student Borrower Prot. Ctr. (Apr. 2021), https://protectborrowers.org/wp-content/uploads/2021/04/Discrimination_is_Unfair.pdf.
[570] 15 U.S.C. § 57a(a)(1)(B).
[571] *Id.; see* Hayes & Schellenberg, *supra* note 569, at 14 ("[I]n disparate-impact cases, effect, not motivation, is the touchstone because a thoughtless housing practice can be as *unfair* to minority rights as a willful scheme.") (emphasis added) (quoting *Reyes v. Waples Mobile Home Park Ltd. P'ship*, 903 F.3d 415, 430 (4th Cir. 2018); *Mt. Holly Gardens Citizens in Action, Inc. v. Twp. Of Mount Holly*, 658 F.3d 375, 383–84 (3d. Cir. 2011); *Smith v. Anchor Bldg. Corp.*, 536 F.2d 231, 233 (8th Cir. 1976)).
[572] Hayes & Schellenberg, *supra* note 569, at 5.
[573] *Id.* at 4.
[574] *See generally* Nancy Leong & Aaron Belzer, *The New Public Accommodations: Race Discrimination in the Platform Economy*, 105 Geo. L.J. 1271 (2017); Pauline T. Kim, *Big Data and Artificial Intelligence: New Challenges for Workplace Equality*, 57 U. Louisville L. Rev. 313 (2019); Ifeoma Ajunwa, *The Paradox of Automation as Anti-Bias Intervention*, 41 Cardozo L. Rev. 1671 (2020); Allyson E. Gold, *Redliking: When Redlining Goes Online*, 62 Wm. & Mary L. Rev. 1841 (2021).

Commission should use its unfairness authority to supplement and backstop these protections across the U.S. economy, including in areas where Congress has already specifically legislated.[575]

Existing civil rights laws leave gaps that the Commission should not hesitate to fill with its unfairness authority. The legal standards that govern discrimination have not entirely kept pace with technology. "The tools currently available to policymakers, legislators, and courts were developed primarily to oversee human decisionmakers."[576] Today, algorithms, not humans, make many of our everyday decisions.[577] But these choices, as when made by humans, have the capacity to discriminate, in part because they embed and amplify human bias.

First, humans may be constantly "in-the-loop" with their creations, working together with the machine either at the initial design stage, or along the way teaching and correcting its decisional process.[578] Second, even when algorithms are not explicitly programmed to take protected characteristics into consideration, they still may use neutral factors as proxies or embed underlying structural inequality.[579] Third, algorithms can amplify discrimination, in part because they can process a

[575] Congress has barred discrimination in specific sectors, such as housing (under the Fair Housing Act), employment (under the Civil Rights Act of 1964, Title VII), and consumer finance (under the Equal Credit Opportunity Act). Notably, Congress has also barred race discrimination in public accommodations (under the Civil Rights Act of 1964, Title VII), race and ethnic discrimination in all federal funded programs (under the Civil Rights Act of 1964, Title VI), sex discrimination in all federally funded and vocational programs (under the Education Amendments of 1972, Title IX), and discrimination against individuals with disabilities in several sectors spanning employment, transportation, public accommodations and more (under the Americans with Disabilities Act).
[576] Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. Pa. L. Rev. 633, 636 (2017).
[577] *See* Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 Wake Forest L. Rev. 393, 393 (2014) (describing how "large datasets are being mined for important predictions and often surprising insights").
[578] Eduardo Mosqueira-Rey et al., *Human-in-the-Loop Machine Learning: A State of the Art*, 7 A.I. Rev. 1, 10 (2022); *see also* Citron & Pasquale, *supra* note 315, at 4.
[579] Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 Wm. & Mary L. Rev. 857, 877 (2017) ("Data models may also discriminate when neutral factors act as 'proxies' for sensitive characteristics like race or sex."); Prince & Schwartz, *supra* note 272, at 1283–89 (describing how "proxy discrimination by AIs is a substantial, and nearly inevitable, risk," in sectors including employment, housing, and lending).

greater volume of information and with greater speed, but also take in data that may or may not be reliable (i.e., the volume, velocity, veracity problem).[580]

Below, we provide examples of algorithmic discrimination in the housing and employment sectors which demonstrate the new challenges algorithmic decision-making brings and illustrate the need for the Commission to adopt new rules that fill in the gaps left by existing civil rights laws.

Housing. The Fair Housing Act was adopted in 1968, after the end of formal Jim Crow, but during an era characterized by racially restrictive covenants, racial steering by real estate agents, and persistent stereotypes in the minds of homeowners, buyers, landlords, and tenants alike.[581] The FHA forbids discrimination in the sale, rental, or advertising of housing, based on race, color, religion, sex, familial status, or national origin (collectively, "FHA-protected characteristics").[582] It also includes a ban on discriminatory advertising, making it illegal:

> [t]o make, print, or publish, [or cause to be made, printed, or published] any notice, statement, or advertisement, with respect to the sale or rental of a dwelling that indicates any preference, limitation, or discrimination based on race, [… color, religion, sex, handicap, familial status, or national origin, or an intention to make any such preference, limitation, or discrimination].[583]

Little did Congress know at the time this law was enacted that someone's "likes" on a social media website could also be used to discriminate in housing.

---

[580] Maddalena Favaretto et al., *Big Data and Discrimination: Perils, Promises and Solutions. A Systematic Review*, 6 J. Big Data 1, 2 (2019) ("[S]ince Big Data technologies are dealing with high volume, velocity and great variety of qualitatively very heterogeneous data, it is highly improbable that the resulting data set will be completely accurate or trustworthy, creating issues of veracity.").
[581] *See* Douglas S. Massey, *The Legacy of the 1968 Fair Housing Act*, 29 Socio. F. 571 (2015).
[582] 42 U.S.C. § 3604(a) (for sale or rental).
[583] 42 U.S.C. § 3604(c).

Social networks are increasingly used to facilitate economic transactions like purchasing, selling, and renting homes[584]—and are increasingly under fire for enabling discriminatory advertising. In 2018, the National Fair Housing Alliance and other fair housing advocacy organizations sued Facebook, alleging that their advertising platform allowed housing, employment, and credit card advertisers to "exclude" audiences based on racial or ethnic characteristics.[585] As part of a settlement, Facebook agreed to change its system to address discrimination.[586]

In that same year, HUD filed an investigation and charge of discrimination against Facebook, alleging that it was still violating the FHA.[587] In 2022, the Department of Justice brought its "first case challenging algorithmic bias under the Fair Housing Act."[588] The complaint alleged that Meta's advertising tool, "Lookalike Audience," was using a machine-learning algorithm to find users who "look like" an advertiser's intended audience, based in part on FHA-protected characteristics.[589] To generate a Lookalike Audience, the complaint alleged that Meta considered

---

[584] *See 2021 Technology Survey,* Nat'l Ass'n of Realtors, https://www.nar.realtor/sites/default/files/documents/2021-technology-survey-08-03-2021.pdf (last visited Nov. 16, 2022) (noting that in 2021, 90% percent of realtors used Facebook in their real estate business, 52% used Instagram, 48% used LinkedIn, and 24 percent used YouTube); Michael Bailey et al., *The Economic Effects of Social Networks: Evidence from the Housing Markets*, 126 J. Pol. Econ. 2224 (2018) (analyzing data from social networking services effects on economic decision making).

[585] First Am. Complaint, *Nat'l Fair Hous. All. v. Facebook*, No. 1:18-cv-02689-JGK, 34 (S.D.N.Y. June 25, 2018).

[586] *Facebook Settlement: Civil Rights Advocates Settle Lawsuit with Facebook: Transforms Facebook's Platform Impacting Millions of Users*, Nat'l Fair Hous. All., https://nationalfairhousing.org/facebook-settlement/ (last visited Nov. 16, 2022).

[587] Charge of Discrimination, *United States Dep't of Hous. & Urban Dev. v. Facebook*, FHEO No. 01-18-0323-8 (HUD Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf. ("[B]y grouping users who 'like' similar pages (unrelated to housing) and presuming a shared interest or disinterest in housing-related advertisements, [Facebook]'s mechanisms function just like an advertiser who intentionally targets or excludes users based on their protected class.").

[588] Press Release, Dep't of Just., *Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising*, DOJ (June 21, 2022), https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known [hereinafter Facebook Lookalike Audience Settlement].

[589] Complaint, *United States v. Meta Platforms*, No. 1:22-cv-05187 (S.D.N.Y. June 21, 2022).

proxies such as a user's "likes," "avatars," or "friends."[590] Meta settled again, agreeing to stop using its discriminatory advertising tools.[591]

Airbnb also facilitates housing rentals and has exhibited algorithmic discrimination based on FHA-protected characteristics. Initially, Airbnb required users to post their names and photos of themselves, features that soon permitted landlords and renters to make decisions based on race discrimination.[592] One study found that "guests with distinctively African American names [were] 16 percent less likely to be accepted relative to identical guests with distinctively [W]hite names."[593] Another that study found that "the more trustworthy the host is perceived to be from her photo, the higher the price of the listing and the probability of it being chosen."[594] Racial bias and determinations of "trustworthiness" are highly correlated.[595] In 2018, Airbnb settled a lawsuit in which guests alleged that hosts had the capacity to discriminate against them by viewing their full name and photos.[596] This case was brought under Oregon's public accommodations law, which raises the question of whether federal public accommodations law would have led to the same result.[597]

---

[590] *Id.* at 7–13.
[591] Facebook Lookalike Audience Settlement, *supra* note 588.
[592] *See* Michael Luca & Max H. Bazerman, *What Data Experiments Tell Us About Racial Discrimination on Airbnb*, Fast Co. (June 19, 2020), https://www.fastcompany.com/90460723/airbnbwhileblack-the-inside-story-of-airbnbs-racism-problem.
[593] Benjamin Edelman et al., *Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment*, 9 Am. Econ. J.: Applied Econ. 1, 1–2 (2017).
[594] Viva Sarah Press, *Airbnb Host Profile Pic Affects Consumer Booking,* ISRAEL21c (Apr. 28, 2016), https://www.israel21c.org/airbnb-host-profile-pic-affects-consumer-booking/#:~:text=The%20study%20found%20that%20the,or%20likelihood%20of%20consumer%20booking.
[595] Damian A. Stanley et al., *Implicit Race Attitudes Predict Trustworthiness Judgments and Economic Trust Decisions*, 108 Proc. Nat'l Acad. Sci. 7710 (2011) (finding that people's "economic decisions to trust is predicted by that person's bias in implicit race attitude).
[596] *Harrington v. Airbnb*, 348 F. Supp. 3d 1085 (D. Or. 2018); Elliot Nijus, *Airbnb Settles Oregon Discrimination Suit*, Oregonian, (Aug. 13, 2019), https://www.oregonlive.com/business/2019/08/airbnb-settles-oregon-discrimination-suit.html.
[597] *Harrington*, 348 F. Supp. 3d at 1086–87 (finding that the plaintiffs adequality pleaded circumstantial of discriminatory intent and that Airbnb is a place of public accommodations under the Oregon Public Accommodations Act (OPPA). The case was removed to federal court based on diversity jurisdiction.); *see* Leong & Belzer, *supra* note 574, at 1304 ("[S]tate public accommodation laws are sometimes more useful than federal laws because they are more expansive in scope.").

Applying the FHA to housing platforms like Airbnb is more complicated. Under the FHA, landlords cannot discriminate when renting out a "dwelling," which has been "narrowly defined as any part of a building or structure to be occupied as a 'residence'."[598] There is no statutory definition of "residence," but some courts have interpreted it to mean "a sense of a home, as opposed to a temporary destination."[599] While Airbnb's long-term sublets would likely have FHA applications,[600] can their short-term rentals be considered residences? If so, would hosts occupying the rental have access to particular exemptions?[601] How long do they need to occupy the home to be considered "occupants" under the act? Or, as Professor Nancy Leong and Aaron Belzer argue, would these rentals be more akin to hotel rooms, falling under public accommodations law?[602]

By establishing in its commercial surveillance rule that discrimination by platforms like Airbnb is unfair and unlawful,[603] the Commission has the power to remove all doubt in this sector—and to unlock significant enforcement authority to give effect to anti-discrimination protections.

Employment. According to EEOC Chairwoman Charlotte Burrows, more than 80% of employers are using AI in some form of their work and employment decision-making.[604] While employers increasingly rely on algorithms to make

---

[598] 42 U.S.C. § 3604(a) ("It shall be unlawful ... [t]o refuse to sell or rent after the making of a bona fide offer, or to refuse to negotiate for the sale or rental of, or otherwise make unavailable or deny, a dwelling to any person because of race, color, religion, sex, familial status, or national origin."); Gold, *supra* note 574, at 1873.

[599] *Weisenberg v. Town Bd. of Shelter Island*, 404 F. Supp. 3d 720, 728 (E.D.N.Y. 2019) (citing *Schwarz v. City of Treasure Island*, 544 F.3d 1201, 1215 (11th Cir. 2008); *United States v. Columbus Country Club*, 915 F.2d 877, 881 (3d Cir. 1990)).

[600] Michael Todisco, *Share and Share Alike? Considering Racial Discrimination in the Nascent-Room Sharing Economy*, 67 Stan. L. Rev. 121, 126 (2015); *see Monthly Stays Made Easy with Airbnb Sublets*, Airbnb, https://www.airbnb.com/sublets (last visited Nov. 16, 2022).

[601] 42 U.S.C. § 3603(b)(2) (exempting from FHA liability owners of dwellings intended to be occupied by four or fewer families if the owner lives in one of the units).

[602] *See* Leong & Belzer, *supra* note 574.

[603] *Cf.* Complaint and Request for Investigation, Injunction, and Other Relief, *In re Airbnb* (Feb. 26, 2020), https://epic.org/privacy/ftc/airbnb/EPIC_FTC_Airbnb_Complaint_Feb2020.pdf.

[604] Lindsey Wagner, *Artificial Intelligence in the Workplace*, ABA (June 10, 2022), https://www.americanbar.org/groups/labor_law/publications/labor_employment_law_news/spring-2022/ai-in-the-workplace/.

decisions, Title VII's prohibition of employment discrimination is "not equipped to deal" with the modern problems that arise.[605]

Under Title VII, discrimination claims can be categorized into two broad categories: disparate treatment and disparate impact.[606] Disparate treatment seeks to punish intentional discrimination, as courts often will look for a "smoking gun" showing "discriminatory motive " or discriminatory purpose[607] By contrast, with the disparate impact approach to establishing a discrimination claim, the challenged practice may be neutral on its face (i.e., facially neutral), but have a discriminatory impact. A showing of discriminatory impact can either "smoke out" the underlying discriminatory purpose or help establish structural inequality where purposeful discrimination may not be readily apparent. For example, the discrimination may be embedded in past and present practice, or the challenged party may have more information (i.e., knowledge of the actual basis of an employment decision), may rely on a proxy for discrimination (such as residence, rather than explicitly race), or may make a decision based on unconscious bias.

To bring a claim, the plaintiff must first identify a discriminatory practice.[608] Then, under a burden shifting framework, the employer can defend its practice by showing it is "job related" and "consistent with business necessity."[609] Finally, if the employer succeeds with a business defense, the plaintiff can still prevail by proving the employer failed to adopt a less discriminatory alternative.[610]

This process does not always translate well for plaintiffs discriminated against by algorithms. As employers control all of the data in hiring platforms, "[a] major thread that runs through the dismissed cases on automated hiring is the court's finding of a lack of evidence or the inability of the plaintiff to provide proof

---

[605] Kim, *supra* note 579, at 903 n.167 (finding that "Barocas and Selbst similarly concluded that Title VII is 'not well equipped' to address the various discriminatory features of data mining."); *see* Barocas & Selbst, *supra* note 525, at 674.
[606] *See* Jennifer C. Braceras, *Killing the Messenger: The Misuse of Disparate Impact Theory to Challenge High Stakes Educational Tests*, 55 Vand. L. Rev. 1109, 1140–41 (2019).
[607] Ifeoma Ajunwa, *Beware of Automated Hiring*, N.Y. Times (Oct. 8. 2019), https://www.nytimes.com/2019/10/08/opinion/ai-hiring-discrimination.html.
[608] 42 U.S.C. § 2000e–2(k)(1)(A).
[609] 42 U.S.C. § 2000e–2(k)(1)(A)(i).
[610] 42 U.S.C. § 2000e–2(k)(1)(A)(ii).

of their allegations of discrimination."[611] The lack of transparency in algorithms makes it difficult for programmers to explain what happened, let alone for the individuals who were discriminated against to know and understand.[612] If a plaintiff is able to get past this hurdle, the EEOC's Uniform guidelines "hold that a practice can be justified as a business necessity when its outcomes are predictive of future employment outcomes" and unfortunately "data mining is specifically designed to find such statistical correlations."[613] Automated decision-making tools often rely on "unexplained correlations" that "have no intuitive connection with performance."[614]

The EEOC has recognized these issues and recently launched an initiative focusing on ways "to help ensure that that tech tools used in employment decisions comply with Federal Anti-Discrimination laws[,] " which so far has resulted in the issuance of new guidance on the implications of algorithms for claims based on disability discrimination.[615] But more work remains, and the FTC is well positioned to supplement the safeguards of Title VII and the work of the EEOC.

The Commission should adopt rules on algorithmic discrimination that apply to all firms in the platform economy—and beyond. Traditional sectors are going digital as they join what has been coined the "platform economy."[616] Uber and Lyft have changed the marketplace for transportation services; Etsy and eBay have altered the way we shop; and Airbnb has revolutionized travel and look for homes. In *Race Discrimination in the Platform Economy*, Professor Nancy Leong & Aaron Belzer identify two key features Platform Economy Businesses ("PEBs").[617] First, these platforms make money by connecting service providers to consumers who

---

[611] Ikfeoma Ajunwa, *An Auditing Imperative for Automated Hiring Systems*, 34 Harv. L. Rev. 621, 649 (2021).
[612] *See id.;* Kim, *supra* note 579, at 326.
[613] Barocas & Selbst, *supra* note 525, at 672; Uniform Guidelines on Employee Selection Procedures, 29 C.F.R. § 1607.15 (2020).
[614] Paul Kim & Matthew T. Bodie, *Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy*, 35 ABA J. Lab. & Emp. L. 289, 298 (2021).
[615] Press Release, U.S. Equal Emp. Opportunity Comm'n, *EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairness* (Oct. 28, 2021), https://www.eeoc.gov/newsroom/eeoc-launches-initiative-artificial-intelligence-and-algorithmic-fairness; *see also* EEOC AI Hiring Report, *supra* note 477 (EEOC's first guidance issued regarding employer's use of AI under the ADA).
[616] This has been also coined the "sharing economy", "on-demand economy", "peer-to-peer economy," "gig economy", and more. *See* Leong & Belzer, *supra* note 574, at 1284.
[617] *Id.* at 1275.

need services.[618] Second, for these connections to be efficient, PEBs operate on digital platforms that use machine learning algorithms, not in physical spaces.[619] While sharing assets and services is not new, internet facilitation of these transactions leads to a host of new questions for regulators, as "laws governing activities in the physical world do not always apply identically to activities initiated in cyberspace."[620] The unique structures of PEBs that make it challenging to apply traditional civil rights protections and illustrate the need for the Commission to consider new rules addressing discrimination in the platform economy.

PEBs usually require users to create profiles, typically including their names and photos. This is encouraged for practical reasons, as Lyft claims it makes it easier for a driver to recognize who they are going to pick up.[621] Additionally, PEBs generally ask users to comply with a rating system after their transactions.[622] After the rating, the PEB's algorithm aggregates the score and disseminates this average to participants, "encouraging them to rely on it to determine whether, and to whom, to transact businesses."[623] Uber claims that this system is designed as a measure of keeping "the rider and driver experience safe."[624] While it's understandable that users would want to know about the parties they transact with, these features can lead to discriminatory outcomes.

Research shows that discrimination in the platform economy takes place in several ways. For Uber, "[b]ecause drivers can reject riders for any reason, you have

---

[618] *Id.*
[619] *Id.*
[620] *Id*. at 1276; Johanna Interian, *Up in the Air: Harmonizing the Sharing Economy Through Airbnb Regulations*, 39 B.C. Int'l & Comp. L. Rev. 129, 151–52 (2016) ("Prosumers who use the services of sharing economy companies often are able to evade liability because of the difficulty in applying laws—which were written for the offline world—to virtual spaces.").
[621] *ID Submission*, Lyft, https://help.lyft.com/hc/en/all/articles/115012926958-id-submission (last visited Nov. 16, 2022) ("Take and submit a photo of yourself. This will become your profile photo to help drivers identify you").
[622] *See, e.g.*, *How Do I Leave a Review?,* TaskRabbit, https://support.taskrabbit.com/hc/en-us/articles/213301766-How-Do-I-Leave-a-Review (last visited Nov. 16, 2022) (noting that after the service is completed, users are emailed an invoice with a "Don't forget to review your Tasker" link in that email).
[623] Leong & Belzer, *supra* note 574, at 1287–88.
[624] *How the Uber Rating System Works*, Uber, https://www.uber.com/en-EG/blog/how-the-uber-rating-system-works/ (last visited Nov. 16, 2022).

no way of knowing whether it's because of your rating, your name (from which race can often be inferred), or the neighborhood you're in."[625] Rating systems can be particularly dangerous, as users can impute bias into assigning a rating, which will in turn be factored into future users' decisions. Empirical research suggests that "[c]onsumer-sourced ratings … are highly likely to be influenced by bias on the basis of factors like race or ethnicity."[626] Further, these ratings can "self-perpetuate."[627] If an Uber driver picks up someone with a low rating, "he may be primed to draw negative conclusions about the passenger on the bias of innocuous or ambiguous behavior."[628] These negative conclusions can factor into lower ratings again, creating a "snowball effect." [629] Lower ratings then translate to a worse user experience, "interfer[ing] with the 'full participation in an equal society' that the Civil Rights Act of 1964 was intended to guarantee for all people."[630]

Scholars and advocates have identified existing legal mechanisms that may apply to algorithmic discrimination in the platform economy. Professor Nancy Leong & Aaron Belzer find that in many circumstances, public accommodation laws under Title II of the Civil Rights Act of 1964 may be used to address discrimination in sectors moved to the platform economy, but also note difficulties in this application.[631] Public accommodations law prohibits discrimination in places of traditional physical locations like hotels, restaurants, theaters.[632] PEBs "function as substitutes for sectors of the traditional economy," but move sectors away from the physical world to the Internet.[633]

---

[625] Jenna Wortham, *Ubering While Black*, Medium (Oct. 23, 2014), https://medium.com/matter/ubering-while-black-146db581b9db.
[626] Gold, *supra* note 574, at 1907 (quoting Alex Rosenblat, *Uberland: How Algorithms Are Rewriting the Rules of Work* 112–13 (2018)).
[627] Leong & Belzer, *supra* note 574, at 1294.
[628] *Id.*
[629] *Id.*
[630] *Id.*
[631] *See generally id.*
[632] *Id.*; Tara E. Thompson, Comment, *Locating Discrimination: Interactive Web Sites as Public Accommodations Under Title II of the Civil Rights Act*, 2000 U. Chi. Legal F. 409, 412 (2002) ("The courts, however, have not reached a consensus as to under what circumstances "non-physical" establishments can be Title II public accommodations").
[633] Leong & Belzer, *supra* note 574, at 1275.

While some courts have adopted an expansive view of Title II, "[n]either Congress nor the courts has addressed how Title II should apply in today's new economy," leaving consumers unsure of their protections.[634] As Professor Leong's article points out, if an Airbnb host who never occupies his property discriminates against a guest, it would likely be captured by Title II.[635] But what about a host who rents out his home while he is traveling across the country—is that considered occupying the rental property enough for his guests to garner Title II's protection? The ridesharing sector may track even less clearly with Title II, as the act is silent as to whether taxicabs are covered, "much less, emerging algorithmic transportation models."[636] Under common carrier doctrine, commentators have found taxis to be public accommodations.[637] But even if they were to be classified as such, "litigation of such cases is rare because prospective litigants often lack [] resources . . . and suffer from imperfect information."[638]

As these examples illustrate, PEBs present a host of difficult legal considerations. With its broad authority to regulate unfair and deceptive trade practices across virtually the entire U.S. economy, the Commission is uniquely positioned to fill in the legal gaps that PEBs and other businesses may exploit to escape accountability for discriminatory algorithmic practices. By declaring that it is an unfair practice to discriminate in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of protected characteristics, the FTC would unlock significant new enforcement authority and provide an essential backstop to existing civil rights law.

---

[634] *Id.* at 1296.
[635] Leong & Belzer, *supra* note 574, at 1297.
[636] Bryan Casey, *Title 2.0: Discrimination Law in a Data-Driven Society*, 2019 J.L. & Mob. 36, 48 (2019).
[637] *See* Leong & Belzer, *supra* note 574, 1297–98; Sylvia A. Law, *White Privilege and Affirmative Action*, 32 Akron L. Rev. 603, 605–06 (1999) ("Since ... Congress passed the Civil Rights Act of 1964, it has been illegal for common carriers, including taxis to discriminate on the basis of race."); Danita L. Davis, *Taxi! Why Hailing a New Idea About Public Accommodation Laws May Be Easier than Hailing a Taxi*, 37 Val. U. L. Rev. 929 (2003).
[638] Leong & Belzer, *supra* note 574, at 1298.

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

As noted above, section 45(n) of the FTC Act defines unfairness[639] with a three-part analysis: (1) whether the "act or practice causes or is likely to cause substantial injury to consumers," (2) "which is not reasonably avoidable by consumers themselves," and (3) is "not outweighed by countervailing benefits to consumers or to competition."[640] Additionally, the Commission may consider whether an act or practice violates "well established" public policies.[641]

Within these bounds, unfairness authority is quite expansive and has significant potential to reach conduct beyond the scope of traditional anti-discrimination laws. Congress intentionally provided for flexibility in the unfairness framework so that the Commission could continually develop its legal contours as the contexts of unfairness evolve over time. This is one such circumstance.

Lessons to draw from traditional anti-discrimination law. Traditional civil rights laws prohibit discrimination in a range of areas. For instance, there are federal laws that protect discrimination in employment, credit, and housing. Title VII protects employees and job applicants against discrimination based on race, color, sex, religion, and national origin.[642] The Fair Housing Act prohibits discrimination in the sale or rental of housing based on race, color, religion, sex, familial status, or national origin.[643] The Equal Credit Opportunity Act makes it unlawful to discriminate an applicant on the basis of race, color, religion, national origin, sex, marital status, age, or because someone receives public assistance.[644]

---

[639] While the FTC has authority to prohibit both unfair *and* deceptive acts or practices, this section focuses on the FTC's unfairness authority, as reflected in the Commission's question.
[640] 15 U.S.C. § 45(n) (as included in the FTC Act Amendments of 1994); *see FTC v. Wyndham Worldwide Corp.*, 799 F.3d at 244; *LabMD, Inc. v. FTC*, 894 F.3d at 1229 (11th Cir. 2018).
[641] 15 U.S.C. § 45(n).
[642] 42 U.S.C. § 2000e-2.
[643] 42 U.S.C. § 3604. *See, e.g.*, Facebook Lookalike Audience Settlement, *supra* note 588 (announcing that the DOJ had settled with Meta Platforms, Inc. regarding allegations that the company engaged in unlawful algorithmic discrimination in violation of the Fair Housing Act).
[644] 15 U.S.C. § 1691.

The Commission should use these laws as a starting point for rulemaking with respect to digital discrimination, but there are several lessons to be mindful of when carrying over these frameworks to the problem of algorithmic and digital discrimination.[645]

The problem of proxies. While discrimination doctrine is well developed, it needs to be updated to tackle today's world of technology, big data, and AI. While traditional civil rights law has in some cases been interpreted to address the use of proxies for protected categories (for example, restrictions based on residency rather than race), the use of proxies by algorithms may be harder to detect. What if an algorithm categorizes based on name, location, or language instead of a protected characteristic?[646] The use of proxies can subtly embed implicit and historic biases that are invisibly factored into decision-making by automated systems. In the aggregate, such practices can substantially harm consumers.

Take the Amazon hiring tool as an example.[647] As noted above, Amazon's recruiting system used an algorithm that "learned" to discriminate against women "by observing [and prioritizing the] patterns in resumes submitted to the company over a 10-year period"—most of which had come from men.[648] As a result, the tool used proxies such as attendance at a historically women's college, women's chess club membership, and other forms of "feminine" language to identify inferior applications.[649] It taught itself that male candidates were preferable, and dismissed the female applicants.[650]

Even if these machine learning systems do not rely on protected categories, proxies still may disadvantage a segment of the population. And once algorithmic bias exists, a system can perpetuate that bias through continual reinforcement. These

---

[645] *See Joined By Commissioner Rebecca Kelly Slaughter In the Matter of Napleton Automotive Group Commission File No. 2023195*, 2022 WL 1039797, *2 (FTC Mar. 31, 2022) ("[D]iscrimination based on protected status is a substantial injury to consumers.").
[646] *See Airbnb Will Change Process to Fight Discrimination in Oregon*, U.S. News (Jan. 6, 2022), https://www.usnews.com/news/business/articles/2022-01-06/airbnb-will-change-process-to-fight-discrimination-in-oregon.
[647] Dastin, *supra* note 339.
[648] *Id.*
[649] *Id.*
[650] *Id.*

proxies could be unknown to the creators themselves, yet the harm is the same: individuals lose out on opportunities because the system finds it not salient to them. Disparities are entrenched, and those excluded cannot seek redress because they are likely unaware that it is happening to them.

Disparate impact versus disparate treatment analysis. The Commission's rule on commercial surveillance must establish that algorithmic and digital disparate impact—not merely disparate treatment—is unfair. Under federal civil rights law, disparate treatment analysis utilizes evidence of intentional discrimination, whereas disparate impact indicates an action that is neutral on its face but has a "'disproportionately adverse effect on minorities.'"[651] Laws that recognize disparate impact typically have a three-part test.[652] Since machine learning creates outputs based on collected data that inherently reflect existing biases in society, disparate impact doctrine is more helpful to combat discrimination online—yet it is not always a cause of action under existing law. While plaintiffs can assert disparate impact claims under Title VII[653] and the FHA,[654] disparate impact is not cognizable under section 1981 of the Civil Rights Act of 1866.[655]

Additionally, these laws scrutinize particular decisions or actions in relationship to sectors they regulate—with disparate treatment being the common focus.[656] Even the laws that permit disparate impact claims cannot necessarily reach the decisions made by a complex array of upstream actors.[657] For example, there is arguably no federal anti-discrimination law that would directly protect against systematic disparities in facial recognition and speech recognition performance by

---

[651] *Inclusive Communities Project*, 576 U.S. at 524. Disparate impact does not require a showing of intent. *See* Hayes & Schellenberg, *supra* note 569, at 15.
[652] Hayes & Schellenberg, *supra* note 569, at 8 ("Generally, unlawful disparate impact occurs when a (1) facially neutral policy or practice disproportionately harms members of protected classes, and either (2) the policy or practice does not advance a legitimate interest, or (3) is not the least discriminatory way to serve that interest.").
[653] *See* 42 U.S.C. § 2000e-2(k).
[654] *See generally Inclusive Cmtys. Project*, 576 U.S. at 519.
[655] *See* Hayes & Schellenberg, *supra* note 651, at 9.
[656] Selbst & Barocas, *supra* note 334, at 7.
[657] *Id.* ("Many commercial applications of AI take place in domains outside those regulated by discrimination law or upstream from the regulated decision, yet nonetheless create discriminatory harms.").

smartphones based on race because they are not directly related to the regulated decision-making process.[658] As Commissioner Rebecca Kelly Slaughter puts it: "'Because AI' is neither an explanation nor an excuse" in anti-discrimination law.[659] However, this is clearly a consumer protection harm with discriminatory consequences—which is within the scope of the FTC's authority.

Drawing the line of unfairness. The Commission can use its unfairness authority to fill in the gaps that exist in traditional anti-discrimination law and reach a broader scope of actors and methods of commercial surveillance that lead to discriminatory outcomes. The hope is to address these harms ex ante by providing notice as to what is unfairness in the context of discrimination and preventing data-driven harms before they occur. Civil rights laws should guide the Commission in building the framework for rules that squarely address such consumer harms. However, the FTC must be creative to effectively address discrimination in digital settings. Most importantly, it must redefine harm in anti-discrimination law.

Defining discrimination harms and "substantial injury." Andrew Selbst and Solon Barocas have put forward a comprehensive approach to understanding discrimination harms.[660] To begin, they identify three types of harms: allocative, quality of service, and representational harms.[661] The Facebook Lookalike Audience case exemplifies the concept of allocative harm, as those targeted based on their protected characteristics were denied housing opportunities.[662] Quality of service harms fit neatly in the FTC's scope of authority: consumers who cannot redeem the value of something they paid for suffer economic harm—such as by means of faulty

---

[658] *Id.* at 8. *See* Allison Koenecke et al., *Racial Disparities in Automated Speech Recognition*, 117 Proc. Nat'l Acad. Sci. 7684 (2020).
[659] Slaughter et al., *supra* note 245, at 38.
[660] Selbst & Barocas, *supra* note 334.
[661] *Id.* at 13 ("Allocative harms are those that concern the distribution of a desirable resource or opportunity, such as a job, credit, or a home. These are the types of harms that are the concerns of traditional discrimination law. Quality-of-service harms are the injuries caused by consumer products and services that simply work less well for certain demographic groups than others. Representational harms capture cases where certain demographic groups are represented in a stereotypical or demeaning manner or where they are not acknowledged at all, harming their social standing in society.").
[662] *See* Facebook Lookalike Audience Settlement, *supra* note 643.

facial recognition technology.[663] Representational harms are the most difficult to address under section 5 because they refer to emotional or dignitary harms, rather than tangible or economical ones.[664] However, all unlawful discrimination inevitably elicits "shame and stigma as well as social consequences of further entrenching disadvantages to marginalized groups."[665] While perhaps not an immediate, concrete harm, representational harm affects an entire class of consumers (and hence, it is substantial). Further, these harms are typically triggered by acts that constitute unlawful discrimination, which are *per se* unfair.[666]

The misuse of personal data can fall into more than one category of harms, such as Amazon's AI hiring tool that discriminated against women in the applicant pool.[667] It denied female candidates job opportunities *and* reinforced degrading stereotypes regarding women's second-class status in male-dominated professions.[668] These allocative and representational harms also demonstrate how powerful actors can use proxies (here, candidate qualifications) that are difficult for the injured party to recognize or establish as discriminatory.[669]

Notably, disparate treatment claims commonly "define[] discrimination and [what] makes it wrongful" through the employer's intent and decision-making process, absorbing the claim of injury into the question of liability without much emphasis on the injury itself.[670] By contrast, section 5 requires a "substantial injury" to consumers to find unfairness.[671] Discrimination law's "perpetrator perspective" is not compatible with section 5's central concern of consumer harm.[672] To this point,

---

[663] Selbst & Barocas, *supra* note 334, at 27 (expanding on the example of performance disparities in facial and speech recognition software based on demographic groups).
[664] *Id.* at 28–29.
[665] Citron & Solove, *supra* note 18, at 855–59.
[666] *See* Selbst & Borocas, *supra* note 334, at 28–29.
[667] Rachel Goodman, *Why Amazon's Automated Hiring Tool Discriminated Against Women*, ACLU (Oct. 12, 2018), https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against.
[668] *Id.*
[669] *See* Solove & Citron, *supra* note 665, at 56 (providing another example: "If an employer used a third-party hiring service to score candidates, then rejected applicants will have no way to know that the hiring service relied upon their intimate information (like their painful periods or infertility).").
[670] Noah D. Zatz, *Disparate Impact and the Unity of Equality Law*, 97 B.U. L. Rev. 1357, 1372 (2017).
[671] 15 U.S.C. § 45(n).
[672] *See* Zatz, *supra* note 670, at 1367.

Professor Noah Zatz argues that disparate treatment and nonaccomodation "share two fundamental elements: status causation" and "responsibility for the injury." [673] Zatz asserts that the injury of "status causation," which arises when an individual suffers harm because of their protected status, is the common thread in all discrimination.[674]

Applying this framework to unfairness, the Commission should sever the inquiry of responsibility for the harm from the inquiry of the injury itself. It then may apply Zatz's definition of injury—status causation—to determine whether there is substantial injury.[675] In the alternative, the Commission may itself define injury in the context of discrimination. The Commission should attempt to capture the essence of discrimination harms, similar to Zatz's formation of "status causation." This can be applied to various factual scenarios under the substantial injury inquiry. Ultimately, responsibility for the injury would be implied in both cases since the unfairness test centers on the consumer rather the covered entities' actions or intentions that led to such harm.

Reasonable avoidability, cost-benefit analysis, and public policy concerns. Under unfairness jurisprudence, an injury is "not reasonably avoidable"[676] when consumers do not have a "free and informed choice."[677] Under all three types of harms, it is difficult to argue that this prong is not met. Consumers are typically not aware of whether a product contains algorithmic biases, as there is no standard auditing system. Even if the former wasn't a concern, audits would be difficult for a typical consumer to understand, and consumers don't have alternatives to avoid biased AI in this commercial surveillance economy.[678] In all, "discrimination is an

[673] *Id.* at 1375. Nonaccomodation occurs when the "protected status enters the causal chain outside the employer's decision-making process, but it nonetheless affects the ultimate outcome of that process. Such 'external' status causation occurs when disability affects tool use and tool use is the employer's basis for decision." *Id.* at 1370.
[674] Zatz, *supra* note 670, at 1359, 1375.
[675] *See id.* at 1378.
[676] 15 U.S.C. § 45(n).
[677] *Neovi, Inc.*, 604 F.3d at 1158.
[678] Selbst & Barocas, *supra* note 334, at 36.

'obstacle to the free exercise of consumer decision-making,' because consumers are almost never in a position to take action to avoid the injury."[679]

Moreover, the cost-benefit analysis requires the Commission to weigh the harm against any benefits to consumers or competition.[680] Both intentional discrimination and disparate impact claims are unlikely to be outweighed by countervailing benefits to consumers or competition.[681] Disparate impact claims have a three step analysis, with the second prong asking "whether a practice with a disparate impact satisfies a legitimate business need."[682] If the answer is no, "there likely is no reasonable argument that a discriminatory practice with no business justification benefits consumers or competition."[683] The third prong requires a similar cost-benefit analysis: whether the business needs could be achieved with a less discriminatory alternative.[684] Chairwoman Lina Khan has noted that "[a]ny purported benefit that can be achieved without engaging in the conduct causing substantial injury is not countervailing, and does not overcome the costs associated with discrimination."[685]

Finally, public policy considerations weigh in favor of finding discriminatory practices to be unfair. [686] Traditional anti-discrimination laws have been embedded in our country's legal structure for decades. Over time, society has developed a collective recognition of anti-discrimination principles and protected classes associated with such prohibition.[687] With an "existing policy for the recognition of

---

[679] Hayes & Schellenberg, *supra* note 651, at 15; *Joined By Commissioner Rebecca Kelly Slaughter In the Matter of Napleton Automotive Group Commission File No. 2023195*, 2022 WL 1039797, *2 ("[I]njuries stemming from disparate treatment or impact are unavoidable because affected consumers cannot change their status or otherwise influence the unfair practices.").
[680] 15 U.S.C. § 45(n).
[681] Hayes & Schellenberg, *supra* note 651, at 15; *see Joined By Commissioner Rebecca Kelly Slaughter In the Matter of Napleton Automotive Group Commission File No. 2023195*, 2022 WL 1039797, *2.
[682] Hayes & Schellenberg, *supra* note 651, at 15.
[683] *Id.*
[684] *Id.* at 16.
[685] *Joined By Commissioner Rebecca Kelly Slaughter In the Matter of Napleton Automotive Group Commission File No. 2023195*, 2022 WL 1039797, *3.
[686] 15 U.S.C. § 45(n).
[687] Hayes & Schellenberg, *supra* note 651, at 16.

the injury," along with codified law, the Commission has a strong argument that public policy supports a finding of unfairness.

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

In its notice of proposed rulemaking, the Commission asks how its expertise and authorities can complement the work of civil rights agencies and how it can ensure interagency collaboration. We note many of the answers to this question may fall outside the four corners of the Commission's rule on commercial surveillance. With that caveat, we recommend that the FTC: (1) create an Office for Civil Rights; and (2) advise the White House to create an interagency working group on algorithmic discrimination, commercial surveillance, and civil rights, which should be co-chaired by the FTC and a White House official with sufficient seniority and authority to effectively coordinate agencies and departments across the inter-agency.

The Commission should create an Office for Civil Rights. EPIC and a broad spectrum of civil rights and consumer protection organizations have previously called on the Commission to create an Office for Civil Rights (OCR) in order to assess the inequities of digital surveillance and to protect civil rights in data-driven commerce.[688] There are currently more than thirty civil rights offices within other federal agencies.[689] An OCR is a sub-agency of an agency that enforces civil rights laws and is dedicated to promoting civil rights and liberties in the agency's programs and activities.[690] OCRs are often led by directors or officers who are in an

---

[688] *Civil Society to U.S. FTC: Fight for Civil Rights and Privacy*, Access Now (Aug. 4, 2021), https://www.accessnow.org/ftc-data-protection-civil-rights/.
[689] *See Civil Rights Offices of Federal Agencies*, Dep't of Just., https://www.justice.gov/crt/fcs/Agency-OCR-Offices (last visited Nov. 21, 2022).
[690] *See* DHS, *Office for Civil Rights and Civil Liberties*, Dep't of Homeland Sec. (Aug. 18, 2017), https://www.dhs.gov/sites/default/files/publications/CRCL%20Handout_Updated%208-18-17.pdf ("[The Office for Civil Rights and Civil Liberties (CRCL)] integrates civil rights and civil liberties considerations into all of the Department's activities by… investigating civil rights and civil liberties complaints…[and] communicating with individuals and communities whose civil rights and liberties may be affected by the Department's activities."); *About OCR*, U.S. Dep't of Com.,

assistant-secretary level position and who report directly to the top authority in an agency.[691] The director or officer provides overall leadership and direction to the agency's civil rights programs and advises the agency on its responsibilities under civil rights laws.[692]

For example, the Department of Homeland Security (DHS) Office for Civil Rights and Civil Liberties (CRCL) was established by the Homeland Security Act of 2002[693] and supports the DHS in promoting civil rights law in its policy development by advising Department leadership and local partners.[694] The CRCL is led by the Officer for CRCL, who is an assistant, non-Senate confirmed Presidential appointee and is supported by two Deputy Officers.[695] In addition to being a civil rights advisor, the CRCL is also responsible for investigating civil rights complaints filed by the public in connection with the DHS's policies or activities, including disability discrimination or racial or ethnic profiling.[696] The CRCL is made up of several sub-divisions to address a variety of areas that may raise civil rights violations.[697] Its Compliance Branch investigates complaints from the public in DHS activities, and its Programs Branch provides policy advice to the DHS on civil liberties issues including anti-discrimination, immigration, and security, intelligence, and information policy.

The Commission should establish its own OCR so that it can effectively support and advise the Commission on its policies and regulations. Establishing an OCR would allow the Commission to center anti-discrimination in its efforts to

---

https://www.commerce.gov/cr/about-us/about-ocr (last visited Nov. 21, 2022) ("The Office of Civil Rights (OCR) coordinates the enforcement of equal opportunity and accessibility for Commerce employees, job applicants, and users of programs and services operated or funded by the Department.").

[691] *See* Dep't of Homeland Sec., *supra* note 690; U.S. Dep't of Com., *supra* note 690; *Office of the Assistant Secretary for Civil Rights,* U.S Dep't of Educ., https://www2.ed.gov/about/offices/list/ocr/contactus2.html (last visited Nov. 21, 2022). For example, Catherine Elizabeth Lhama is the Assistant Secretary for Civil Rights at the Department of Education. *See id.*

[692] *See id*.

[693] 6 U.S.C. § 245.

[694] *See* Dep't of Homeland Sec., *supra* note 690.

[695] *Id.*

[696] *Id.*

[697] *Id.*

regulate the digital consumer space.[698] Similar to the DHS, the FTC could seek to establish its own compliance branch that would manage or assist in the investigation of complaints concerning discriminatory algorithmic practices. It should also establish a program branch or subdivision with the expertise to advise the Commission on how to respond to emerging issues. The OCR would be able to advise the Commission on its actions and efficiently respond to emerging industry practices that may result in disparate impact.[699] Further, it would be able to coordinate with other agencies and their OCRs to ensure that the agencies' regulations and standards adequately protect individuals' civil rights. An OCR that is specifically devoted to civil rights protection will ensure that the Commission remains fully committed to civil rights as the agency continues to create and implement policies.

The Commission should recommend that the White House create an interagency task force. The FTC can collaborate with other civil rights agencies by recommending that the White House create an interagency task force on algorithmic discrimination, commercial surveillance, and civil rights. An interagency task force would help ensure coordination and cooperation between federal agencies and departments.

To take a recent example, President Biden established the Gender Policy Council (GPC) by executive order to implement and develop domestic and foreign policies based on gender equity and equality.[700] The GPC was created to advance equity for those who face discrimination and bias, including members of the BIPOC and LGBTQI+ communities and persons with disabilities.[701] The GPC is led by a Director who also serves as an assistant to the president.[702] The GPC is also staffed by a variety of domestic and international gender policy experts, including an

[698] *See* Access Now et al., *Letter from Civil Rights and Privacy Groups to the FTC* 9 (July 29, 2021), https://www.accessnow.org/cms/assets/uploads/2021/08/FTC-civil-rights-and-privacy-letter-Final.pdf.
[699] *See id*.
[700] *See Gender Policy Council*, White House, https://www.whitehouse.gov/gpc/ (last visited Nov. 21, 2022).
[701] *Id*.
[702] *Id*.

Advisor on Gender-Based Violence.[703] It currently coordinates its work with other White House policy councils and across all federal agencies as part of a "whole-of-government approach" to promoting gender equality and equity.[704]

In view of the Commission's special expertise, the FTC should advise the White House to establish an analogous task force on algorithmic discrimination and privacy harms co-chaired by the Commission and a White House official with sufficient seniority and authority to effectively coordinate agencies and departments across the inter-agency. An interagency task force would provide a vehicle for the Commission to collaborate with the Federal Communications Commission, Department of Health and Human Services, Department of Justice, the Securities and Exchange Commission, and other relevant agencies which share overlapping responsibilities and goals of promoting privacy and civil rights.

The right to privacy is a matter of survival.[705] In our data-driven world, marginalized groups stand at the intersection of unregulated commercial data practices and discriminatory harms. The Commission is equipped with the tools to address the harmful impacts of digital surveillance and algorithmic decision-making systems. The FTC's commercial surveillance rule can secure the necessary privacy and civil rights protections that individuals, especially those from marginalized communities, must be afforded. But the Commission should go further to address the barriers to effective interagency collaboration by creating an Office for Civil Rights and recommending that the White House establish an interagency task force. Doing so will allow the Commission and its fellow civil rights agencies to ensure that consumers are protected from discriminatory data practices and to better adapt to a rapidly evolving digital environment.

---

[703] *Id.*

[704] *Id.*

[705] 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/.

4. Notice and Transparency

Responsive to questions 83–93.

Half a century ago, the landmark report *Records, Computers, and the Rights of Citizens* cemented the role of notice and transparency as critical safeguards for the protection of personal data.[706] Wary of the threats posed by the secret processing of personal information—and mindful of "the principle of mutuality necessary for fair information practice"[707]—the Advisory Committee on Automated Personal Data Systems set out baseline disclosure requirements for any organization maintaining such a data system.[708] Among these were the obligations to "give public notice of the existence and character" of each system at least once a year;[709] to inform individuals whether and for what purpose their personal information was being processed;[710] to "make such data fully available to the individual upon [the individual's] request" in a "comprehensible form"; and to "permit data to be corrected or amended when the individual to whom they pertain so requests."[711]

Five decades later, the importance of transparency to the protection of personal information has only grown. The volume, complexity, and stakes of personal data processing far exceed what was known in the 1970s. With the rise of automated decision-making technologies, pervasive tracking and profiling, devices that collect data from our homes and persons, and other vectors of commercial surveillance, it is even more essential that businesses be required to disclose the how, what, when, and why of their processing activities.[712] But meaningful transparency in today's surveillance economy must go beyond the rote disclosure of

[706] Advisory Comm. on Automated Pers. Data Sys., U.S. Dep't of Health, Educ., & Welfare, *Records, Computers and the Rights of Citizens* (1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf.
[707] *Id.* at 60.
[708] *Id.* at 57, 99.
[709] *Id.*
[710] *Id.* at 59, 62.
[711] *Id.* at 59.
[712] *See* Citron & Pasquale, *supra* note 315, at 33.

this information. As the Commission's guidance[713] and enforcement actions[714] reflect, companies that exercise control over our personal data must demonstrate that they have carefully evaluated the risks of the processing they undertake and that such processing is justified in light of those risks. An individual must also have a straightforward mechanism to learn what personal data a company collects and retains from them, which in turn enables the consumer to demand its correction or deletion.

To be clear, even the most effective notice and transparency requirements cannot, by themselves, fully protect against the abuse of personal data.[715] We have moved beyond the notion that notice and consent alone can legitimize commercial surveillance practices when those practices are too complex and numerous for even the most sophisticated consumer to understand. That is why it is critical that the Commission establish the substantive limits on data collection and processing set out elsewhere in these comments.

Still, notice and transparency remain essential components of an effective data protection regime, and the Commission should recognize that their absence from the commercial processing of personal data constitutes an unlawful trade practice. Consumers are routinely harmed by data processing activities that are unvetted or undisclosed by businesses, and consumers certainly cannot avoid harm which they "have no reason to anticipate."[716] There are no plausible benefits to consumers or competition from secret, unaccountable processing of personal

---

[713] *See generally* FTC, *Mobile Privacy Disclosures: Building Trust Through Transparency* (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.
[714] *See, e.g.*, Decision and Order at 4, *In re Residual Pumpkin*, FTC File No. 192-3209 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Residual%20Pumpkin%20Agreement%20Containing%20Consent%20Order.pdf (requiring respondent to "[a]ssess, at least once every twelve (12) months … the sufficiency of any safeguards in place to address the internal and external risks to the privacy, security, confidentiality, or integrity of Personal Information, and modify the Information Security Program based on the results"); *see also* Megan Gray, *Understanding and Improving Privacy "Audits" under FTC Orders* (2018), https://cyberlaw.stanford.edu/sites/default/files/blogs/white%20paper%204.18.18.pdf (recommending steps to strengthen the privacy audits required under many consent decrees).
[715] *See* Philipp Hacker & Bilyana Petkova, *Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers*, 15 Nw. J. Tech. & Intell. Prop. 1, 16–9 (2017) (discussing limits of transparency as accountability and consumer disclosure involving Big Data).
[716] *IFC Credit Corp.*, 543 F. Supp. 2d at 948 (N.D. Ill. 2008).

information—and if there were, they would be readily outweighed by the injuries that such processing inflicts on consumers.

4.1. It is an unfair and deceptive practice to collect, use, retain, or transfer personal data without first assessing, justifying, and providing adequate notice of such collection, use, retention, or transfer.

Responsive to questions 73, 74, 83–85, 89–92.

A business's processing of personal data cannot be considered fair or honest if that business fails to thoroughly evaluate the risks that its processing presents to individuals; fails to establish the necessity of its processing in light of the risks; or fails to provide adequate notice of its processing. The excessive, unjustifiable, and secret exploitation of personal data by businesses has helped to produce the "information and power asymmetry" at the heart of the modern surveillance economy.[717] Although "data-driven companies collect much more personal data than the consumer knows or can reasonably oversee,"[718] transparency—despite its limitations—remains "an essential tool for consumers to exercise their rights" and to maintain a degree of "control and autonomy over their privacy."[719] The Commission's trade rule on commercial surveillance must reflect this.

Undisclosed and unaccountable commercial processing of personal data is a deceptive trade practice. If the reasonable consumer is to have any ability to exercise "choice . . . regarding a [digital] product,"[720] the consumer must, at a minimum, be provided with notice that the product exists in the first place; information about how and why the product operates as it does; and fair warning of the risks that the product presents to the consumer. When a company conducts commercial processing of personal data without ascertaining and disclosing these

[717] Pub. Citizen et al., *Privacy and Digital Rights For All* 2 (2020), https://epic.org/wp-content/uploads/privacy/policy/Privacy-And-Digital-Rights-For-All-A-blueprint-for-the-next-Administration.pdf.
[718] Peter J. van der Waerdt, *Information Asymmetries: Recognizing the Limits of the GDPR on the Data-Driven Market*, 2020 Comput. L. & Sec. Rev. 38, 38 (2020).
[719] *Id.* at 51.
[720] FTC Deception Statement, *supra* note 104, at 5–6.

basic parameters, it engages in an omission of material fact—and thus a deceptive trade practice.

This premise is embodied in the Commission's enforcement actions targeting the use of malware, stalkerware, and other forms of surreptitious tracking and processing.[721] The Commission rightly considers it a deceptive trade practice for a business to engage in processing of personal data that it has not disclosed, even if the business has been forthright about other processing it performs on the same data. For example, the Commission recently determined that Twitter deceived consumers by using email addresses and phone numbers collected for one purpose (account security) for an undisclosed purpose (targeted advertising).[722]

Moreover, the omission of key information about a business's processing of personal data is likely to affect consumer choice and conduct. In the (regrettably rare) instance that consumers are given notice that their data will be commercially exploited and provided a frictionless mechanism to opt out, they do so at a high rate. For example, when Apple provided iOS users with the opportunity to opt out of cross-app tracking by advertisers in 2021, more than 90% of users exercised that opt-out.[723]

Undisclosed and unevaluated commercial processing of personal data is an unfair trade practice that causes substantial injury to consumers. Commercial processing of personal data that is kept secret or conducted without ascertaining the risks to consumers can cause a virtually limitless range of harms—everything from discriminatory treatment to emotional and psychological harms to the breach, wrongful disclosure, or improper secondary use of personal data.[724] In many cases

[721] *See, e.g.*, *In re Support King, LLC (SpyFone.com)*, FTC File No. 192-3003 (2021); *In re Sears Holdings Mgmt. Corp.*, FTC File No. 082-3099 (2018); *In re Lenovo*, FTC File No. 152-3134 (2018).
[722] *In re Twitter*, FTC File No. 202-30623 (2022).
[723] *See* Estelle Laziuk, *iOS 14.5 Opt-in Rate - Daily Updates Since Launch*, Flurry (Apr. 29, 2021), https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/.
[724] Citron & Solove, *supra* note 18, at 830–861.

these harms are economically quantifiable,[725] and in many cases consumers are forced bear the cost of unrevealed risks to their personal information.[726]

Even where the undisclosed or incautious processing of personal data does not produce downstream harms, the fact that such processing occurs in the first place is a source of substantial injury to consumers in at least three ways. First, surreptitious processing inherently deprives a consumer of autonomy by causing a loss of control over one's personal data—i.e., an "inability to make certain choices about one's personal data or to be able to curtail certain uses of the data."[727] Being stripped of control over the use of personal or confidential information is a well-established form of injury, as in the torts of misappropriation of name or likeness[728] and wrongful appropriation of trade secrets.[729]

Second and relatedly, a consumer's autonomy is inherently diminished by a business's "failure to inform" them about the processing of their personal data.[730] "When individuals are not informed of their rights or not given important

---

[725] *See generally* Robert L. Rabin, *Intangible Damages in American Tort Law: A Roadmap* (July 2016), https://law.stanford.edu/wp-content/uploads/2016/07/R.L.RABIN-SSRN-Rotterdam-Conf-paper-revised-for-ssrn-2727885-Intangible-Damages-in-American-Tort-Law.pdf.
[726] *See, e.g.*, IBM, *Cost of a Data Breach Report 2022* 13 (2022), https://www.ibm.com/reports/data-breach ("A majority [60%] of organizations in the study said they increased the price of their products and services as a result of the data breach."); Alex Scroxton, *Consumers left out of pocket as security costs soar*, Comput. Wkly. (July 27, 2022), https://www.computerweekly.com/news/252523222/Consumers-left-out-of-pocket-as-security-costs-soar ("As it becomes increasingly difficult to obtain cyber insurance coverage and/or pay-outs following cyber incidents, companies will certainly look to pass these costs on to their customers, who will end up not only footing the bill for the breach, but also paying the price for having their data in the hands of criminal gangs or for sale on the dark web[.]").
[727] Citron & Solove, *supra* note 18, at 846; *see also* Alan F. Westin, *Privacy and Freedom* 7 (1967) (defining privacy as the right of individuals "to control, edit, manage, and delete information about themselves and decide when, how, and to what extent information is communicated to others").
[728] Restatement (Second) of Torts § 652C; *see also Long v. Southeastern Pa. Transp. Auth.*, 903 F.3d 312, 324 (3d Cir. 2018) ("These latter three types of privacy torts represent interference with an individual's ability to control his personal information. That is analogous to the injury here, which is the use of Plaintiffs' personal information—their consumer reports—without Plaintiffs being able to see or respond to it.").
[729] Restatement (Third) of Unfair Competition § 40.
[730] Citron & Solove, *supra* note 18, at 849; *see also Long*, 903 F.3d at 324; *Robertson v. Allied Sols., LLC*, 902 F.3d 690, 697 (7th Cir. 2018) ("Respondents' injury consequently seems concrete and particular. . . . [W]hat matters is that Robertson was denied information that could have helped her craft a response to Allied's concerns.") (cleaned up).

information, they are harmed because they lose their ability to assert their rights at the appropriate times, to respond effectively to issues involving their personal data, or to make meaningful decisions regarding the use of their data."[731]

Finally, a business's failure to evaluate and disclose the details of its personal data processing creates "an imbalance in information between buyers and sellers, which can potentially lead to inefficient market outcomes."[732] Not only does this practice foist the burden of identifying and mitigating the risks of processing onto the consumer—who is almost always in a worse position to do so—but it can also "lead to an 'adverse selection' or 'lemons' problem, where higher quality goods (e.g., more privacy protective goods and services) are driven out of the market."[733] These inefficiencies cause substantial economic injuries to consumers.

Undisclosed and unevaluated commercial processing of personal data is not reasonably avoidable by consumers. Although notice alone is often insufficient to make a business's processing of personal data reasonably avoidable by a consumer, it is self-evident that a consumer cannot reasonably avoid something if they are not made aware of it. "Having no reason to anticipate the harm" associated with undisclosed and unevaluated processing of their personal data, "there [is] no occasion for the consumers even to consider taking steps to avoid it."[734] Even the most sophisticated and well-resourced consumers cannot protect themselves against the exploitation of their personal information by third-party data brokers that operate in the shadows,[735] app developers and SDKs that covertly collect location data,[736] or platforms that collect and process personal information to a far greater extent than they disclose.[737]

---

[731] Citron & Solove, *supra* note 18, at 849.
[732] OECD, *Consumer Data Rights and Competition - Background Note* 23 (2020), https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf.
[733] *Id.*
[734] *IFC Credit Corp.*, 543 F. Supp. 2d at 948; *see also Orkin Exterminating Co.*, 849 F.2d at 1365 ("[C]onsumers may act to avoid injury before it occurs *if they have reason to anticipate the impending harm and the means to avoid it*[.]") (emphasis added).
[735] *See, e.g.*, Complaint for Permanent Injunction & Other Relief, *FTC v. Kochava, Inc.*, No. 2:22-cv-377 (D. Idaho filed Aug. 29, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf.
[736] *See, e.g.*, *In re Goldenshores Technologies, LLC*, FTC File No. 132-3087 (2013).
[737] *See, e.g.*, *In re Facebook, Inc*, FTC File No. 092-3184 (2011, 2019).

Undisclosed and unevaluated commercial processing of personal data is not justified by any benefits to consumers or competition. There is no credible benefit to consumers from commercial processing of personal data conducted without adequate notice and an assessment of the risks. Transparency is just one piece of an effective data protection framework, but it unquestionably benefits individuals and maximizes consumer choice and control. Of course, it is also important to ensure that notice concerning the processing of personal information is presented in an accessible fashion and does not bombard or overwhelm consumers.[738] But no reasonable consumer would contend that key information about the commercial use of their personal data should be affirmatively withheld if they seek it out or that businesses should process their data oblivious to the injuries that may result.

And as noted, opaque and unaccountable data processing tends to create *less* efficient markets by introducing information asymmetries, increasing transaction costs for the consumer, unfairly entrenching the market position of unscrupulous data holders, and excluding less privacy protective alternatives from the market.[739] "[Online] transactions appear to take place in an inefficient market hampered by steep information asymmetries, which are further aggravated by big data. Transacting with a big data platform is like a game of poker where one of the players has his hand open and the other keeps his cards close."[740] Individual firms may benefit enormously from the undisclosed processing of personal data. Competition does not.

Undisclosed and unevaluated commercial processing of personal data is prevalent. To begin with, the commercial processing of personal data is a definitively prevalent trade practice. U.S. spending on digital advertising alone—a sector heavily reliant on the tracking and targeting of individual consumers—

[738] *See* Consumer Reps. & EPIC, *supra* note 3, at 24–25.
[739] *See* OECD, *supra* note 732, at 23; EPIC et al., *Comments on Competition and Consumer Protection in the 21st Century Hearings* 19 (2018), https://epic.org/wp-content/uploads/apa/comments/EPIC-FTC-CompetitionHearings-August2018.pdf ("Privacy—or a lack thereof—is at the very heart of why the digital platforms have been able to entrench their dominance. Access to consumer data gives firms a competitive edge that did not exist prior to the age of big data.").
[740] Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 Nw. J. Tech. & Intell. Prop. 239, 255 (2013).

reached at least $189 billion in 2021[741] (and is by some accounts more than twice that high).[742] Data brokerage is a more than $200 billion industry,[743] and the location data market is estimated at $14 billion.[744] The breathtaking scale of the surveillance economy is beyond doubt.

But while commercial processing of personal data is abundant, there is a widespread failure to thoroughly evaluate the risks that such processing presents to individuals and to provide adequate notice. A 2020 survey found that just 57% of businesses had conducted a data security risk assessment.[745] That means 43% of businesses failed to conduct even a baseline analysis of security threats to the data they collect, use, store, or transfer—let alone a comprehensive evaluation of the privacy risks that their processing poses. Fewer businesses still publish the results or contents of those risk assessments, even in a redacted or summarized form.

A 2019 survey of 150 privacy policies—the mechanism by which many companies would ostensibly disclose the details of their data processing activities—found the policies "inscrutable," "vague," "opaque[]," and an "incomprehensible disaster."[746] This systematic ambiguity "undermines the purpose and value of a

---

[741] Press Release, Interactive Advert. Bureau, *Digital Advertising Soared 35% to $189 Billion in 2021 According to the IAB Internet Advertising Revenue Report* (Apr. 12, 2022), https://www.iab.com/news/digital-advertising-soared-35-to-189-billion-in-2021-according-to-the-iab-internet-advertising-revenue-report/.

[742] Patience Haggin, *Personal Data Is Worth Billions. These Startups Want You to Get a Cut*, Wall St. J. (Dec. 4, 2021), https://www.wsj.com/articles/personal-data-is-worth-billions-these-startups-want-you-to-get-a-cut-11638633640 ("Personal data is behind the $455.3 billion digital-ad market.").

[743] MMR, *Data Broker Market: Global Industry Forecast (2022-2029) by Data Category, Data Type, Pricing Model, End Use Sector, and Region* (2022), https://www.maximizemarketresearch.com/market-report/global-data-broker-market/55670/.

[744] Grand View Rsch., *Location Intelligence Market Size, Share & Trends Analysis Report by Application (Sales & Marketing Optimization, Remote Monitoring), By Service, By Vertical, By Region, and Segment Forecasts, 2022 - 2030* (2022), https://www.grandviewresearch.com/industry-analysis/location-intelligence-market.

[745] *78% Lack Confidence in Their Company's Cybersecurity Posture, Prompting 91% to Increase 2021 Budgets*, BusinessWire (Feb. 24, 2021), https://www.businesswire.com/news/home/20210224005176/en/78-Lack-Confidence-in-Their-Company%E2%80%99s-Cybersecurity-Posture-Prompting-91-to-Increase-2021-Budgets.

[746] Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.*, N.Y. Times (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html; *see also Social Media Privacy*, EPIC (2022),

privacy policy for website users" and fails to achieve the "clarity in privacy practices [that] is a necessary prerequisite to empowering users to make informed decisions."[747]

The failure of current notice and accountability mechanisms is apparent from consumers themselves. In a 2021 industry survey of consumers in twelve countries (including the United States), 46% of respondents reported being unable "to effectively protect [their] personal data today," and 76% of those cited the difficulty of "figur[ing] out what companies are doing with my data" as a reason.[748] Not surprisingly, 59% of Americans reported in a 2019 Pew Research Center survey that they "underst[oo]d very little or nothing" about what companies do with the personal data they collect.[749]

And the fact that the Commission has taken significant steps to ensure that businesses thoroughly evaluate and disclose their processing of personal data reflects the systemic nature of the problem. For example, the Safeguards Rule already requires financial institutions to "identif[y] reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks."[750] This same requirement has been incorporated into multiple consent decrees premised on unfair and deceptive data practices.[751]

To prevent undisclosed and unevaluated commercial processing of personal data, the Commission should establish robust assessment, disclosure,

---

https://epic.org/issues/consumer-privacy/social-media-privacy/ ("[T]hese policies are often vague, hard to interpret, full of loopholes, subject to unilateral changes by the platforms, and difficult or impossible for injured users to enforce.").

[747] Joel R. Reidenberg et al., *Ambiguity in Privacy Policies and the Impact of Regulation*, 45 J. Legal Stud. S163, S164 (2016).

[748] Cisco, *Building Consumer Confidence Through Transparency and Control* 4 (2021), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf.

[749] Brooke Auxier et al., *supra* note 219.

[750] 16 C.F.R. § 314.4.

[751] *See, e.g.*, Decision & Order at 7, *In re Lenovo*, FTC File No. 152-3134 (2018); Stipulated Final Order for Permanent Inj., *FTC v. Bayview Solutions, LLC*, FTC File No. 142-3226 (D.D.C. Apr. 21, 2015).

and access requirements. This should include both a requirement to conduct privacy impact assessments and individual rights for consumers to access, correct, or delete their personal information.

The Commission should require businesses to conduct and disclose a privacy impact assessment prior to processing personal data or substantially modifying their processing of personal data. A privacy impact assessment, also known as a data protection impact assessment or privacy risk assessment, is an analysis of how and why personally identifiable information will be collected, processed, stored, and transferred. When implemented properly, privacy impact assessments force institutions to carefully evaluate and disclose the privacy risks of a proposed action, system, or project—and to mitigate those risks. We urge the Commission to require businesses that intend to process personal data to conduct and publish a robust privacy impact assessment prior to initiating or substantially modifying such processing.

The object of a privacy impact assessment is to "anticipate[] problems, seeking to prevent, rather than to put out fires."[752] When a business is deciding whether to initiate a collection of personal data or to adopt a system that will process personal data, it is the responsibility of that business to conduct a privacy impact assessment before proceeding. An impact assessment enables the business to identify privacy risks, to determine how and if those risks can be mitigated, and to make an informed decision on whether the proposed collection or system can be justified in light of its privacy impact. An impact assessment can also provide the public with vital information about a data collection or a data system that poses a threat to privacy. Privacy impact assessments are analogous to the environmental impact statements that federal agencies and other entities must complete before initiating projects that will significantly affect the environment.[753]

An impact assessment should not be a simple box-checking exercise or a static, one-off undertaking. Rather, it is "a process which should begin at the earliest

[752] *Privacy Impact Assessment* v (David Wright & Paul de Hert, eds., 2012) (foreword by Gary T. Marx).
[753] *See National Environmental Policy Act Review Process*, EPA (Oct. 5, 2022), https://www.epa.gov/nepa/national-environmental-policy-act-review-process.

possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should continue until and even after the project has been deployed."[754] As the Office of Management and Budget warns federal agencies, a privacy impact assessment "is not a time-restricted activity that is limited to a particular milestone or stage of the information system or [personally identifiable information] life cycles. Rather, the privacy analysis shall continue throughout the information system and PII life cycles."[755]

Privacy impact assessments have been in use for more than thirty years[756] and are a key component of leading data protection frameworks. Impact assessments are required of federal agencies (including the FTC)[757] under section 208 of the E-Government Act of 2002;[758] are mandated by the European Union's General Data Protection Regulation (GPDR) for projects that are "likely to result in a high risk to the rights and freedoms of natural persons";[759] and feature in both the California Consumer Privacy Act (CCPA)[760] and the Colorado Privacy Act (CPA).[761] Impact assessments are also an important element of the Commission's consent decrees arising from unlawful data protection and data security practices.[762]

These existing frameworks offer a blueprint for the Commission to develop effective privacy impact assessment requirements. But four principles are worth highlighting here. First, the Commission must ensure that it sets an inclusive threshold for the obligation to complete an impact assessment. Even relatively limited processing of personal data can pose a significant threat to consumers if a business fails to identify, evaluate, and mitigate the resulting risks. If necessary, the

---

[754] *Privacy Impact Assessment*, *supra* note 752, at 5–6.
[755] Off. of Mgmt. & Budget, Exec. Off. of the President, *OMB Circular A-130: Managing Information as a Strategic Resource* app. II at 10 (2016).
[756] *See* PIAF, *A Privacy Impact Assessment Framework for data protection and privacy* rights 124 (David Wright et al. eds., 2011), https://piafproject.files.wordpress.com/2018/03/piaf_d1_21_sept2011revlogo.pdf.
[757] *Privacy Impact Assessments*, FTC, https://www.ftc.gov/policy-notices/privacy-policy/privacy-impact-assessments (last visited Nov. 16, 2022).
[758] E-Government Act, Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921–23 (2002).
[759] GDPR art. 35.
[760] Cal. Civ. Code. § 1798.185(a)(15)(B).
[761] Colo. Rev. Stat. Ann. § 6-1-1309.
[762] *See, e.g.*, Decision at II.E, *In re Twitter*, FTC File No. 202-30623 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023062C4316TwitterModifiedOrder.pdf.

minimal regulatory burden posed by impact assessments can be calibrated by tying the required scope and depth of assessments to the size, complexity, nature, and sensitivity of the data processing for which they are required. But the baseline assessment requirement should extend to all entities subject to the FTC's jurisdiction that engage or intend to engage in the processing of personal data.

Second, we urge the Commission to require the completion of a privacy impact assessment as soon as a business takes material steps toward data processing that will pose a risk to consumers so that the risks to individuals can be prevented or mitigated *before* processing begins. Allowing impact assessments to be postponed until the last minute (or even until after data processing has begun) threatens to turn the assessments into superfluous paperwork and facilitate the whitewashing of harmful data practices. We also urge the Commission to require covered businesses to review and update privacy risk assessments well in advance of any change to a business's data processing activities that might alter the resulting risks to individuals' privacy, but in any event no less than once per six-month period.

Third, although the categories of information suggested by the Commission's ANPR are essential to effective impact assessments, additional disclosures should be included. The Commission asks whether companies should be required to explain:

- The data [companies] use;
- How they collect, retain, disclose, or transfer that data;
- How they choose to implement any given automated decision-making system or process to analyze or process the data, including the consideration of alternative methods;
- How they process or use that data to reach a decision;
- Whether they rely on a third-party vendor to make such decisions;
- The impacts of their commercial surveillance practices, including disparities or other distributional outcomes among consumers; [and]
- Risk mitigation measures to address potential consumer harms[.][763]

We believe all of these categories should be included in a privacy impact assessment, and we would advise the Commission to also require the following non-exhaustive list of disclosures:

[763] ANPR, *supra* note 1, at 51285.

- The purpose(s) for which the company will collect, process, retain, or make available to third parties each category of personal data;
- The sources of the personal data the company will collect, process, retain, or make available to third parties;
- To which third parties and service providers, if any, the company will make personal data available;
- What notice or opportunities for consent will be provided to consumers concerning the company's collection, processing, or retention of their personal data or the availability of such information to third parties;
- The potential harms that might result from such processing, including but not limited to privacy, physical, economic, psychological, autonomy, and discrimination harms;
- The company's asserted need to engage in such collection, processing, retention, or transfer of personal information;
- Any alternatives to such collection, processing, retention, or transfer of personal information seriously considered by the company and the reason(s) why such alternatives were rejected;
- How the asserted benefits resulting from such collection, processing, retention, or transfer to the business, the consumer, other stakeholders, and the public compare to the risks to the consumer; and
- A plain language summary of the assessment that would be comprehensible to a reasonable consumer.

Finally, it is critical that both the Commission and the business conducting a risk assessment publish the results of that assessment promptly, conspicuously, and by means that are readily accessible to interested members of the public. In addition to forcing a business to evaluate and mitigate the harms of its data processing, a risk assessment also serves to inform the public of a data collection or a data system that poses a threat to privacy—a key corrective to the harms caused by undisclosed processing. We believe the underlying assessments should be presumptively public, subject only to the narrow redactions necessary to protect data security and trade secrets. Such assessments should be both published in a central repository maintained by the Commission and made readily accessible to consumers by the companies themselves. We take no position on whether a single document may be used to disclose a company's assessment of multiple data processing activities, so long as the document includes the required elements and is published well in advance of any new or changed processing activities that might alter the resulting risks to individuals' privacy.

It is worth repeating that even the strongest privacy impact assessment and transparency requirements are insufficient methods to protect privacy alone. They must be paired with substantive limits on data collection and processing set out elsewhere in these comments.[764]

In addition to requiring businesses to evaluate and disclose their processing of personal data to the public at large, the Commission should require businesses to promptly honor an individual's request to access all data the business maintains on them; to have such data corrected if it is in error; and to secure the deletion of all such data. Access, correction, and deletion rights ensure additional accountability, transparency, and user control of businesses' processing of personal data.

Access rights date back at least as far as the Fair Credit Reporting Act in U.S. law;[765] feature prominently in the EU's General Data Protection Regulation,[766] California Consumer Protection Act,[767] Colorado Privacy Act,[768] and other data protection regulations; and are found in the proposed American Data Privacy and Protection Act.[769] These frameworks point to at least four principles for the Commission's implementation of access, correction, and deletion rights.

First, the right of access should extend to substantially all of the individual's personal data collected, maintained, or processed by the business; must enable the individual to learn the identities of any third parties and service providers to which the business has transferred personal data and an explanation of why such transfer(s) occurred; and must require disclosure of the individual's personal data in a human-readable format that a reasonable individual can understand.

Second, the right of correction should require corroborating evidence from the individual only where a business reasonably believes that the individual's proposed correction is erroneous and the accuracy of the personal data in question

---

[764] *See generally* Ari Ezra Waldman, *Industry Unbound* (2021) (demonstrating that many privacy impact assessments have become little more than checkbox forms).
[765] Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*.
[766] GDPR arts. 15–17.
[767] Cal. Civ. Code. §§ 1798.105, 1798.106, 1798.110.
[768] Colo. Rev. Stat. Ann. §§ 6-1-1306(1)(b)–(d).
[769] ADPPA § 203.

is material to the business's operations; should minimize the burden on the individual in circumstances where it is appropriate for a business to request corroborating evidence; and should require a business to make reasonable efforts to ensure that any third parties and service providers to which it has transferred the individual's personal data also correct the identified error(s).

Third, as with the right of correction, the right of deletion should require a business to make reasonable efforts to ensure that any third parties and service providers to which it has transferred the individual's personal data also delete such data. Companies should also be required to delete personal data once that data is no longer necessary for the purpose for which the data was collected, processed, or transferred.[770]

Finally, it is important that the Commission establish frictionless mechanisms for the exercise of these rights. The Commission should consider establishing platform- and technology-neutral standards in its commercial surveillance rule that would enable individuals to easily submit access, deletion, and correction requests to each business. The Commission should also explore requiring businesses to honor global or multi-business access, correction, and deletion requests where appropriate.

Just as privacy impact assessments and transparency alone are not enough to protect privacy, neither are individual rights. As Professor Ari Ezra Waldman has noted: "The practices associated with individual rights of control seem empowering: we can click on links to ask that our data be deleted, corrected, and moved. But although more control sounds like a good thing, individual rights will not solve collective privacy problems."[771] Professor Julie Cohen observes that "Atomistic, post hoc assertions of individual control rights, however, cannot meaningfully discipline networked processes that operate at scale."[772] Individual

[770] Complaint at ¶ 12(e), *FTC v. SkyMed International, Inc.*, FTC File No. 192-3140 (2020), https://www.ftc.gov/system/files/documents/cases/skymed_-_complaint.pdf.
[771] Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 Cal. L. Rev. 1221, 1254 (2022), https://ssrn.com/abstract=3784667 (citing Margot E. Kaminski & Gianclaudio Malgieri, *Algorithmic Impact Assessments Under the GDPR: Producing Multi-Layered Explanations*, 11 Int'l Data Priv. L. 125, 138 (2021), https://ssrn.com/abstract=3456224).
[772] Julie E. Cohen, *How (Not) to Write a Privacy Law*, Knight First Amend. Instit. (2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law.

rights are not meaningful unless combined with the substantive limits on data collection and processing set out elsewhere in these comments.

5. The Privacy of Minors

5.1. It is an unfair practice to collect, process, retain, or transfer the personal data of minors under the age of 18 unless strictly necessary to achieve the minor's specific purpose for interacting with the business or to achieve certain essential purposes.

Responsive to questions 1, 3–5, 8, 10, 12–15, 17, 19–22, 28, 75, 76, 79.

Commercial surveillance causes unique harms for children and teenage consumers that result in substantial injury. From a very young age, minors participate in a broad range of activities online. These online activities can have many benefits—allowing kids to learn about an endless array of topics, participate in school during a pandemic, connect with loved ones around the world, play games, and explore their developing identities. Unfortunately, the lack of adequate rules to protect minors from commercial surveillance leaves them exposed to the same harms suffered by adults described in section 1. In many instances those harms, such as harms to autonomy or security, are magnified by the unique vulnerabilities of minors.[773] Minors are uniquely vulnerable to profiling and other effects of commercial surveillance systems, which are necessarily designed to suggest and shape preferences and beliefs. A rule under the Commission's unfairness authority could protect children and teens online while not significantly impacting competition in the online services, education technology, and advertising industries. Minors can enjoy the benefits of technology without being subject to commercial surveillance.

As noted in section 1, the most widespread injuries to privacy online today come from the sweeping collection and use of personal data to profile and target consumers based on what they read, where they go, who they interact with, and

[773] *See generally Holding Big Tech Accountable: Legislation to Build a Safer Internet: Hearing before the Subcomm. Consumer Protect. of the H. Comm. on Energy & Com.*, 117th Cong. (2021) (testimony of Josh Golin, Exec. Dir., Fairplay), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Witness%20Testimony_Golin_CPC_2021.12.09.pdf [hereinafter Golin Testimony].

how likely they are to click or buy. Current laws such as the Children's Online Privacy Protection Act (COPPA) are not sufficient to protect minors from these harms.

For example, Life360, a family location sharing app, sold collections of families' location data to about a dozen data brokers, which in turn sold it to "virtually anyone who want[ed] to buy it." While marketed as a way for parents to monitor their children's location, Life360 has been one of the largest sources of data in the industry.[774] As a default, Life360 asks users for the broadest permissions possible for functional purposes.[775] The only way a consumer could avoid ceaseless location tracking is to not download the app at all.[776] Life360 provides a disclaimer in small print: "Your location data may be shared with Partners for the purposes of crash detection, research, analytics, attribution and tailored advertising."[777] While Life360 claims that its purpose is to provide a family location sharing and safety app, it has sold vast amounts of location data to brokers who, in turn, have sold it to an untold number of buyers for undisclosed purposes. A lack of regulations and safeguards has allowed Life360 to profit from selling families' location data, a use entirely unrelated to the original purpose that data was collected for (allowing family members to track each other's real-time locations). Life360 has stated that it will change its practice of selling precise location data, but currently no U.S. regulation is stopping similar behavior from other entities.[778] Notably, the minor is not the one choosing to use the Life360 app—their parents are—but it is the minor's location that is being collected, sold, and distributed widely in the online data ecosystem. This could have dangerous downstream effects and lead to physical harm if the location data of a minor is obtained by a bad actor, such as an abusive

---

[774] *Id.*
[775] Jon Keegan & Alfred Ng, *The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users*, Markup (Dec. 6, 2021), 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.
[776] *Id.*
[777] *Id.*
[778] John Keegan & Alfred Ng, *Life360 Says It Will Stop Selling Precise Location Data*, Markup (Jan. 27, 2022), https://themarkup.org/privacy/2022/01/27/life360-says-it-will-stop-selling-precise-location-data.

relative or child groomer.[779] The Commission must issue a rule that prohibits this type of secondary data use that violates the reasonable expectations consumers have when they download and use an app.

The secondary use of minors' data to provide targeted advertising is especially harmful, as described in detail in the Comments of the Center for Digital Democracy and Fairplay. EPIC supports FairPlay and the Center for Digital Democracy's call to ban targeted advertising to minors.

Surveillance practices also make it exceedingly difficult for children and teens to develop a sense of autonomy. When minors are aware of monitoring as they use technology at home or in school, they change their behavior in ways that have chilling effects on their expression, critical thinking, and political participation.[780] A recent report by the Center for Democracy and Technology found that half of students surveyed agreed with the statement "I do not share my true thoughts or ideas because I know what I do online may be monitored."[781] As Professor Julie Cohen notes, "The opportunity to experiment with preferences is a vital part of the process of learning, and learning to choose, that every individual must undergo."[782] The constant surveillance of minors has detrimental effects on their sense of autonomy—and to our society as a whole, as free thought and expression is impeded.

The broad collection of minors' personal data also poses security risks and can cause physical harms. The FBI warned in a 2018 alert that the rapid increase in

---

[779] Girard Kelly et al., Common Sense Media, *Privacy risks and harms* 9 (2019), https://privacy.commonsense.org/content/resource/privacy-risks-harms-report/privacy-risks-harms-report.pdf.
[780] *Id.* at 11; *see also* Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* 180 (2015) (chilling effects can put "the intellectual development of our citizenry at risk.").
[781] Elizabeth Laird et al., *Hidden Harms: The Misleading Promise of Monitoring Students Online* 22 (2022), https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of-monitoring-students-online/.
[782] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1425 (2000) (citing Anita L. Allen, *Coercing Privacy*, 40 Wm. & Mary L. Rev. 723, 754–55 (1999) ("Privacy is a matter of escaping as well as embracing encumbrances of identity. Without adequate privacy, there can be no meaningful identities to embrace or escape, and no opportunities to engage in meaningful reflection, conversation, and debate about the grounds for embracing, escaping, and modifying particular identities.")).

the use of educational technologies and widespread collection of student data could "have privacy and safety implications if compromised or exploited."[783] "Malicious use of sensitive data could result in social engineering, bullying, tracking, identity theft, or other means of targeting children," the FBI warned.[784] These same risks apply when the data is collected for commercial surveillance purposes.

Profiling of children and teens enabled by widespread data collection is particularly harmful, as it places minors in "predetermined categories, very often without their knowledge."[785] The Committee of Ministers of the Council of Europe recently adopted a recommendation on the use of profiling, noting that it "can pose significant risks for individuals' rights and freedoms," particularly for vulnerable persons, including children.[786] A report on children's privacy to the United Nations Human Rights Council also illustrated the harms from profiling of children and teens.[787] In particular, the report discussed the harms of profiling as children increasingly form their personalities and identities in digital settings.[788] "Profiling children limits their potential self-development in childhood, adolescence and possibly adulthood, as behavioural predictions and nudging techniques can predetermine options and choices."[789] Additionally, processing children's personal data can infringe on their privacy, can lead to a loss of autonomy, and can result in economic, emotional and physical harms.[790]

Facebook whistleblower Frances Haugen highlighted the risks of profiling teens in Congressional hearings late last year, saying:

---

[783] Fed. Bureau of Investigation, *Education Technologies: Data Collection and Unsecured Systems Could Pose Risks to Students*, Alert No. I-091318-PSA (Sept. 13, 2018), https://www.ic3.gov/media/2018/180913.aspx.
[784] *Id.*
[785] Council of Eur. Comm. of Ministers, *Recommendation No. R (8) of the Committee of Ministers to members states on the protection of individuals with regard to automatic processing of personal data in the context of profiling* (Nov. 3, 2021), https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a46147.
[786] *Id.*
[787] Joseph A. Cannataci (Special Rapporteur on the Right to Privacy), *Artificial Intelligence and Privacy, and Children's Privacy*, 12–17, U.N. Doc. A/HRC/46/37 (Mar. 19, 2021).
[788] *Id.* at 14 ("[C]hildren must be able to enjoy, unimpaired by commercial practices, their rights to unhindered development of personality.").
[789] *Id.*
[790] *Id.*

> The second question is around things like search, like how do those interests then percolate into spirals like down rabbit holes? When you engage with any content on Instagram, Facebook learns little bits of data about you—they learn what kinds of content you might like, and then they try to show you more. But they don't show you random content, they show you the content most likely to provoke a reaction for you. And Facebook has demonstrated that in the case of things like teenagers, you can go from a search query like healthy eating to anorexia content within less than two weeks, just by engaging with the content that you're given by Facebook.[791]

In order to drive its engagement-optimizing algorithms (discussed in section 5.2), Facebook was collecting data points on every click, every piece of content viewed, and every search query to build profiles about teenagers in order to keep them online for longer, to keep the commercial surveillance cycle going, and to optimize Facebook's profits. A data minimization rule that limited the use of personal data to that which is strictly necessary to provide a service, as we propose below, would curtail this kind of harmful profiling and targeting.

The substantial injuries resulting from commercial surveillance are not reasonably avoidable by minors. This is due to the fact that (1) children and teens are a class of consumers with unique vulnerabilities and (2) society has progressed to a point where kids and teens cannot avoid going online if they want to participate in both educational and social activities.

Where informational asymmetry exists in the relationship between sellers and adult consumers, that asymmetry is only exacerbated when it comes to child or teen consumers. The primary driver of informational asymmetry regarding commercial surveillance is that it is non-obvious to the user. This is especially true for children and teens, who are still developing critical thinking skills and cannot easily distinguish advertisements or influencer content from non-commercial content.[792] Only 25% of 8- to 15-year-olds, for example, were able to identify the top results

---

[791] *Holding Big Tech Accountable: Targeted Reforms to Tech's Legal Immunity: Hearing before the Subcomm. on Comms. & Tech. of the H. Comm. on Energy & Com.*, 116th Cong. (2021) (testimony of Frances Haugen, 2:08:42), https://www.youtube.com/watch?v=UwKUx-Io-_E.

[792] Ofcom, *Children and Parents: Media Use and Attitudes Report* 12–13 (2017), https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf.

from a Google search as advertisements, despite them being labeled with the term "ad."[793] Because minors generally do not know how and when they are tracked, they have no way to avoid such tracking. They are less likely understand how their data is being used for surveillance purposes.[794] A recent UNICEF manifesto called for improved governance of children's data because children are generally more vulnerable consumers than adults and less likely to appreciate the longer-term implications of the commercial surveillance directed at their online presence.[795]

Another aspect of reasonable avoidance relates to consent. As discussed above, children and teens are more vulnerable and likely to unknowingly or unwillingly consent to data collection or surveillance. COPPA requires some websites and apps to obtain verifiable parental consent before collecting, using, or disclosing personal information from children under the age of thirteen.[796] Operators must comply with COPPA if they direct content to children or if they know they are collecting, using or disclosing information from children under 13.[797] Despite COPPA's protections, commercial surveillance of children persists at an expansive scale.[798] One recent study found that 67% of apps used by preschool-aged children collected persistent digital identifiers and transmitted them to third-party

---

[793] *Id.*

[794] *See, e.g.*, Duncan McCann, New Econ. Found., *I-Spy: The Billion Dollar Business of Surveillance Advertising To Kids* 16 (2021), https://neweconomics.org/uploads/files/i-Spy__NEF.pdf; UNICEF, *The Case for Better Governance of Children's Data: A Manifesto* 5 (2021), https://www.unicef.org/globalinsight/media/1771/file/UNICEF%20Global%20Insight%20Data%20Governance%20Summary.pdf [hereinafter UNICEF Manifesto on Children's Data] ("Children and adolescents have differing awareness of what information is collected online and for what purposes.").

[795] *See id.* at 2–3 ("The implications of surveillance and tracking are also more significant for children due to greater exposure over their lifetime[.]").

[796] 15 U.S.C. §§ 6501–06.

[797] *Id.*

[798] *See* Geoffrey A. Fowler, *Your kids' apps are spying on them*, Wash. Post (June 9, 2022), https://www.washingtonpost.com/technology/2022/06/09/apps-kids-privacy/ ("More than two-thirds of the 1,000 more popular iPhone apps likely to be used by children collect and send their personal information to the advertising industry[.] On Android, 79 percent of popular kids apps to the same."); Pixalate, *Mobile Apps: Google v. Apple COPPA Scorecard (Children's Privacy)* (2022), https://www.pixalate.com/hubfs/Reports_and_Documents/Mobile%20Reports/2022/App%20Reports/Active%20Apps/Child-Directed%20Apps/Q1%202022%20-%20Apple%20vs.%20Google%20COPPA%20Scorecard%20Report%20-%20Pixalate.pdf.

companies.[799] Many of these apps were "child directed" and likely in violation of COPPA,[800] while in other cases COPPA did not apply because the preschooler was using a general audience app.[801] In 2017, researchers found that by the time a child turns 13, over 72 million data points have been collected about them (and that excludes trackers used by Facebook, Twitter, YouTube, and other embedded social widgets).[802] This number is assuredly even higher five years later. Moreover, child-directed websites and applications used by children are not always listed in kids' sections or otherwise identified as being directed at children.[803] Many websites and apps used by children are not "child-directed," or claim not to verify the age of users as under 13 to evade COPPA enforcement completely.[804] Just as consumer surveillance harms are not reasonably avoidable for consumers that are children and teens, they are also unavoidable for parents trying to maintain their children's privacy online, as the parental consent mechanisms of COPPA either are not

---

[799] Fangwei Zhao et al., *Data Collection Practices of Mobile Applications Played by Preschool-Aged Children*, JAMA Pediatrics, 2020, at 4, https://jamanetwork.com/journals/jamapediatrics/fullarticle/2769689.

[800] *Id.* at 2 ("Binns and colleagues used static app analysis (i.e., analyzing app source code to find code that directs data collection to third parties) on 959,000 apps from the US and UK Google Play stores. They found that apps targeting children had among the highest number of third-party trackers. Reyes et al. used dynamic analysis to track the data transmissions from 5855 of the most popular free Android children's apps and showed that the majority had potential COPPA violations.").

[801] *Id.* at 6 ("some children in our study used apps that transmit geolocation data, such as the McDonald's app, and games such as hole.io and SpeedBall. Children may easily download general audience apps from Google Play when parental controls are not enabled. It is also possible that children install adult-directed apps through advertisements that appear in children's apps,10 where they can easily be clicked and installed.").

[802] Fowler, *supra* note 798; *see also* SuperAwesome, *How much data do adtech companies collect on kids before they turn 13?* (Dec. 13, 2017), https://web.archive.org/web/20180309203314/https://blog.superawesome.tv/2017/12/13/how-much-data-do-adtech-companies-collect-on-kids-before-they-turn-13/.

[803] Fowler, *supra* note 798 (There are more than 391,000 child-directed apps between Google and Apple App stores—more than the offerings in the "kids sections" of the app stores.).

[804] *See* Craig Timberg, *Sex, drugs, and self-harm: where 20 years of child online protection law went wrong*, Wash. Post (June 13, 2019), https://www.washingtonpost.com/technology/2019/06/13/sex-drugs-self-harm-where-years-child-online-protection-law-went-wrong/ (detailing how COPPA "actual knowledge" standard is ineffective because it is easy for kids to represent that they are older than 13).

enforced or not triggered due to the "general audience" nature of the site the minor is using.[805]

Children and teens are tracked and profiled as they spend much of their lives online, from toys to educational technology to social media. "In the two years from 2019 to 2021, screen use increased far faster than it had in the previous four years. In fact, the increase in screen use among tweens was six times as large in the past two years as it had been in the four years before that."[806] Research confirms that young people are increasingly online to socialize, read, create content, and play games.[807] Their constant online presence and unique vulnerabilities as minors make consumer surveillance harms unavoidable. "The digital ecosystem is so complex and data processing so seamless," that children and their parents cannot truly understand the benefits or avoid the risks and harms.[808] Facebook's own research has shown that "young people are acutely aware that Instagram can be bad for their mental health, yet are compelled to spend time on the app for fear of missing out on cultural and social trends."[809]

The proliferation of educational technology ("edtech") tools in recent years has made online tracking even more unavoidable for children and teens. If a certain app or website is used in the classroom, parents do not typically have the opportunity to review that edtech tool or its privacy policy. Even if parents were given advance notice and the ability to review these tools, the amount of time required would be staggering and not feasible for the average parent. And if a website or app is required to be used for homework, test taking, school communication, or storage of educational files, students and parents are left with no meaningful choice but to use the service. This was especially true during the

---

[805] Fowler, *supra* note 798 ("Bottom line: If you're a parent who wants to make sure your kids' apps respect their privacy, it takes work."); *see also* Cannataci, *supra* note 787, at 17 ("Most children and parents do not have the capacity to challenge educational technology companies' privacy arrangements or to refuse to provide data, as education is compulsory.").
[806] Victoria Rideout et al., Common Sense Media, *The Common Sense Census: Media Use by Tweens and Teens* 43 (2021), https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf.
[807] *Id.*
[808] UNICEF Manifesto on Children's Data, *supra* note 794.
[809] *See Teen Mental Health Deep Dive*, Wall St. J. (Sept. 29, 2021), https://s.wsj.net/public/resources/documents/teen-mental-health-deep-dive.pdf.

COVID-19 pandemic, as online learning was often the only option children had to "attend" school—the "choice" was to log on to an edtech product or be marked as absent. Researchers at Human Rights Watch analyzed 164 edtech products endorsed by 49 countries during the pandemic.[810] Of the 164 products, 146 (89%) were found to have "put at risk or directly violated children's privacy and other children's rights, for purposes unrelated to their education."[811] The researchers also found over 700 third-party trackers embedded in 112 edtech websites and estimated that a child logging into a single one of those sites to "attend" school would be tracked by an average of six third-party trackers per day.[812] Commercial surveillance has become unavoidable to minors who need to attend school remotely or simply want to be online for social, research, or other purposes.

The injuries to minors caused by commercial surveillance are not outweighed by countervailing benefits to consumers or competition.[813] The Commission must give special consideration to commercial transactions involving children. Children and teens are not typical "bargaining" consumers—they often do not have full agency or understanding to consent to the collection of their personal data. While some degree of data collection may be necessary to provide or personalize a specific service, the use of that data for secondary commercial purposes is not necessary to provide the service.

The serious harms to children and teens online are also not outweighed by benefits to competition in the consumer surveillance realm. Personal data about children and teens, which is necessarily sensitive data, is "packaged up into profiles for commercial advertising purposes. This sort of profiling creates an online experience where advertisers are allowed to target potentially vulnerable young people for commercial gain, and places huge power in the hands of unknown

[810] Hye Jung Han, Human Rights Watch, *"How Dare They Peep into My Private Life?": Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic* (2022), https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments.
[811] *Id.*
[812] *Id.*
[813] 15 U.S.C. § 45(n).

advertisers."[814] Below, we propose a rule dictating that the personal data of individuals under 18 may only be collected, processed, or transferred if strictly necessary to achieve the minor's specific purpose for interacting with the business or strictly necessary to achieve certain essential purposes. This rule would apply evenly, and no one firm would have the upper hand. Moreover, privacy measures tend to distribute market power and improve competition.[815]

The Commission has the authority to issue a rulemaking addressing commercial surveillance harms to kids and teens because mass collection of their data is prevalent. One way to establish prevalence is through evidence that indicates a widespread pattern of unfair or deceptive practices.[816] From educational settings to toys, gaming, and social media, kids and teens live much of their lives online. Their online presence is constantly monitored, often without their knowledge or consent.[817] Not only has there been "an uptick in daily teen internet users, from 92% in 2014–15 to 97% today[,]" but the "share of teens who say they are online almost constantly has roughly doubled since 2014–15 (46% now and 24% then)."[818] Based on the ubiquity of kids and teens' internet use and associated harms, there is sufficient evidence to establish that the mass collection of minors' personal data is widespread and prevalent.

To stop the excessive collection, processing, retention, and transfer of the personal data of minors, the Commission should issue a rule that has layered protections to safeguard children and teens from substantial injury. The first layer should be a rule dictating that the personal data of individuals under 18 may only be collected, processed, or transferred if strictly necessary to achieve the minor's

---

[814] Dylan Williams et al., Reset Australia, *Profiling Children for Advertising: Facebook's Monetisation of Young People's Personal Data* 22 (2021), https://au.reset.tech/uploads/resettechaustralia_profiling-children-for-advertising-1.pdf.
[815] Berjon, *supra* note 103.
[816] 15 U.S.C. § 57a(b)(3).
[817] *See* Andrew Young & Stefaan G. Verhulst, *Why We Need Responsible Data For Children*, Conversation (Mar. 23, 2020), https://theconversation.com/why-we-need-responsible-data-for-children-134052 ("[D]ata systems used are often designed with (consenting) adults in mind without a focus on the unique needs and vulnerabilities of children. This can lead to the collection of inaccurate and unreliable data as well as the inappropriate and potentially harmful use of data for and about children.").
[818] Emily Vogels et al., *Teens, Social Media and Technology 2022*, Pew Rsch. Ctr. (Aug. 10, 2022), https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/.

specific purpose for interacting with the business or strictly necessary to achieve certain essential purposes that provide a clear benefit to the minor or to the public.[819] For data that is strictly necessary, collection from minors under 13 years old should still require verifiable parental consent (as is required under COPPA).

COPPA currently dictates that operators of websites or online services directed to children under 13 years of age, including edtech providers, may not condition participation in any activity on a child disclosing more information than is reasonably necessary for the child to participate in that activity."[820] This standard may have been workable when COPPA was passed in 1998, when children were barely using the Internet and commercial surveillance practices had not yet become prevalent. But today it means that a website could simply bury a "skip" button below an extensive data request and be in compliance with COPPA. COPPA's verifiable parental consent provisions face a similar problem. They may have been workable in 1998 when parents had to deal with minimal requests for consent, but it is unrealistic in 2022 to expect parents to (1) understand the scope of today's data ecosystem in such a way that they can meaningfully consent to data collection for their children, and (2) actually review the lengthy privacy policies for the myriad websites and apps used by children. Moreover, COPPA only covers websites and

---

[819] *See e.g.* CCPA § 1798.121(a) (enumerating the purposes for which California consumers can ask a business to limit the use of their sensitive personal data to, such as (1) "use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services;" (2) "Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes;" (3) "Short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business;" (4) "Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business;" and (5) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.")

[820] FTC, *Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act* (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Policy%20Statement%20of%20the%20Federal%20Trade%20Commission%20on%20Education%20Technology.pdf (citing 15 U.S.C. § 6502(b)(1)(C)).

online services directed at children, but data collection from children and teens is harmful whether it is collected by a child-directed or general audience site. Unfair practices are happening despite COPPA because parents and minors do not have a meaningful choice. Life in 2022 requires the use of online services and apps by children and teens, and there is currently no way to reasonably avoid the harms caused by these services.

Imposing a rule that requires that the personal data of individuals under 18 may only be collected, processed, or transferred if strictly necessary to achieve the minor's specific purpose for interacting with the business or strictly necessary to achieve certain essential purposes is fully within the Commission's mission and is not undercut by Congress's decision to pass COPPA. Congress was right to define the practices prohibited by COPPA as unfair and deceptive in 1998, and we do not seek to upend that Congressional judgment. But nothing in COPPA suggests that it was meant to be the exhaustive or exclusive account of data practices that could unfairly harm children. If that were the intent, Congress could have expressly preempted the Commission's authority to define unfair and deceptive data practices that harm children, something it has done in other contexts. But it did not. COPPA is a floor, not a ceiling, and the Commission retains its authority to lay down more restrictive rules to protect the privacy of children against evolving business practices. As the Commission itself recently stated in its policy statement on edtech and COPPA:

> When Congress enacted the Children's Online Privacy Protection Act ("COPPA"), it empowered the Commission with tools beyond administering compliance with notice and consent regimes. The Commission's COPPA authority demands enforcement of meaningful substantive limitations on operators' ability to collect, use, and retain children's data, and requirements to keep that data secure.[821]

Systems that collect and use data on children and teens in ways that are not strictly necessary are unfair regardless of whether a parent has nominally consented to them. Therefore, the Commission should issue a rule that adds a layer of protection before a consent request requiring that the personal data of individuals under 18

[821] *Id.*

may only be collected, processed, or transferred if strictly necessary to achieve the minor's specific purpose for interacting with the business or strictly necessary to achieve certain essential purposes.

5.2. It is an unfair and deceptive practice to make intentional design choices in order to facilitate the commercial surveillance of minors.

Responsive to question 17.

As detailed in the recent Petition for Rulemaking to Prohibit the Use on Children of Design Features that Maximize for Engagement by the Center for Digital Democracy (CDD) and Fairplay, the use of engagement-optimizing design practices on children is unfair in violation of section 5 of the Federal Trade Commission Act.[822] EPIC supports CDD and Fairplay's Petition for Rulemaking, and in these comments we echo the call for a rule prohibiting the use of engagement-optimizing design practices for all the reasons detailed in the petition. Engagement-optimizing design practices are often used to enable commercial surveillance, causing substantial injury to minors. Platforms make intentional design choices to keeps kids and teens online for longer periods of time to drive increased data collection and surveillance,[823] and the harms enumerated in the prior section are all exacerbated by these design practices.

In addition to being unfair, it is also a deceptive practice to implement engagement-optimizing design choices to drive commercial surveillance. These deceptive design choices are intentionally misleading. The entire goal of engagement-optimizing design is to deceive minors into spending more time online so the cycle of commercial surveillance can continue. The company extracts more personal data on the minor, the minor is shown more ads during their extended time on the app or platform, and the company makes more money.[824] Design goals

[822] Ctr. for Digit. Democracy et al., *Petition for Rulemaking to Prohibit the Use on Children of Design Features that Maximize for Engagement* (Nov. 17, 2022), https://fairplayforkids.org/wp-content/uploads/2022/11/EngagementPetition.pdf [hereinafter Engagement-Optimizing Rulemaking Petition].
[823] *See* McCann, *supra* note 794, at 16 ("[S]urveillance advertising is allowing advertisers to develop increasingly sophisticated strategies to capture their attention.").
[824] *See* 5Rights Foundation, *Pathways: How Digital Design Puts Children at Risk* 7 (2021), https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf.

are set with business interests in mind, often with little regard for the wellbeing and safety of children.[825] Businesses use design features to increase and maintain engagement with children, including "push notifications, endless scrolling feeds, quantifying and displaying popularity, making it easy to share, in-app or in-game purchases, making it easy to connect, [and] friend or follower suggestions."[826] Business models rely on and reinforce these design choices. At their core, "[d]igital platforms are designed to maximize revenue, and design choices that increase engagement and facilitate data collection put children at risk."[827]

By orchestrating engagement in this way, the deception is material. These design choices are material because they surreptitiously steer minors into the harmful and exploitative commercial extraction of their personal data, time, and attention. Moreover, the lack of transparency concerning website and platform design choices and goals constitutes an omission of material information. In other words, if certain design choices had been disclosed to minors or their parents, they may have made the choice not to use the website or application in question.

Design choices intended to increase data collection are prevalent.[828] Engagement-optimizing design practices exist across a wide range of contexts, devices, and websites or applications, and they are used on consumers of every age.[829] These deceptive and unfair designs include algorithms intended to go unnoticed by children and teens, causing them to provide more personal information than necessary or to stay online for longer periods of time.[830] The harms from resulting from such extended periods online are both well documented and widespread.[831] The Commission has authority to issue a rule concerning design choices and their effect on minors because unfair and deceptive design choices are prevalent across the commercial surveillance ecosystem.

---

[825] *Id.* at 7.
[826] *Id.*
[827] Golin Testimony, supra note 773, at 1.
[828] 15 U.S.C. § 57a(b)(3).
[829] *See* McCann, *supra* note 794.
[830] *See* 5Rights, *supra* note 824.
[831] *See Id.*

To protect children and teens from the harms of engagement-optimizing design practices, the Commission should adopt a rule prohibiting design features that unduly maximize minors' engagement with online platforms, including categorical prohibitions on the practices outlined in CDD and Fairplay's Petition for Rulemaking.[832]

6. DATA SECURITY

Responsive to questions 10–13, 30–36, and 47.

The Commission should declare that a business's failure to implement reasonable security measures to protect consumer data is an unfair trade practice, and that any entity which represents that it protects the security of consumer data but fails to adopt reasonable data security measures has engaged in a deceptive trade practice. Consumers are facing an epidemic of data breaches and resulting identity theft and harm due to a lack of investment in and commitment to data security. The Commission has tried over the last two decades to improve the situation through case-by-case enforcement and the encouragement of industry self-regulation, but it is clear those approaches are not sufficient. Companies will not adequately invest in data security unless they face significant consequences for a failure to do so.

That is why it is necessary for the Commission to make clear in a rule what it has already made implicit through its enforcement actions: companies that fail to protect the data they are holding violate the law. And the rule should also shift the burden in cases where a major breach has occurred, establishing a presumption that large breaches are evidence of unreasonable data security practices absent clear evidence to the contrary. The rule should be even more strict for breaches of sensitive data, where a breach should be per se unfair; once a consumer's sensitive data has been breached, there is little to nothing they can do to avoid fraud, identity theft, and other substantial injuries that the breach has caused.

The Commission has a long track record of bringing enforcement actions against companies that engage in lax data security practices. So it is a natural extension of those targeted enforcement actions to establish a rule that any entity

[832] Engagement-Optimizing Rulemaking Petition, *supra* note 822.

seeking to collect, process, retain, or transfer personal data must establish, implement, and maintain reasonable administrative, technical, and physical measures to secure such data against unauthorized access,[833] and that it is a deceptive practice to misrepresent data security practices to consumers.[834] Poor data security continues to be an unfortunate and prevalent practice that feeds the constant stream of data breaches we read about every day.[835] There is no question

---

[833] *See, e.g.*, First Am. Complaint, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015), https://www.ftc.gov/legal-library/browse/cases-proceedings/1023142-x120032-wyndham-worldwide-corporation [hereinafter Wyndham]; Complaint, *In re Residual Pumpkin Entity, LLC, d/b/a CafePress*, FTC File No. 1923209 (Jun. 23, 2022), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923209-cafepress-matter [hereinafter CafePress]; Complaint, *In re SkyMed International, Inc.*, FTC File No. 1923140 (Jan. 26, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923140-skymed-international-inc-matter [hereinafter SkyMed]; Complaint, *In re InfoTrax Systems, L.C.*, FTC File No. 1623130 (Dec. 30, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3130-infotrax-systems-lc [hereinafter InfoTrax]; Complaint, *In re LightYear Dealer Technologies, LLC*, FTC File No. 1723051 (Sept. 6, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3051-lightyear-dealer-technologies-llc-matter [hereinafter LightYear]; Complaint, *FTC v. Equifax, Inc.*, No. 1:2019-cv-03297 (N.D. Ga. Jul. 22, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3203-equifax-inc [hereinafter Equifax]; Complaint, *FTC v. D-Link Corp.*, No. 3:17-CV-00039-JD (N.D. Cal. Mar. 20, 2017), https://www.ftc.gov/legal-library/browse/cases-proceedings/132-3157-x170030-d-link [hereinafter D-Link]; Complaint, *FTC v. Ruby Life Inc. d/b/a AshleyMadison.com*, No. 1:16-cv-02438 (D.D.C. Dec. 14, 2016), https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3284-ashley-madison [hereinafter AshleyMadison]; Complaint, *In re Lenovo, Inc.*, FTC File No. 1523134 (Jan. 2, 2018), https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3134-lenovo-inc [hereinafter Lenovo].

[834] *See, e.g.*, Complaint, *In re Support King, LLC*, FTC File No. 1923003 (Dec. 21, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3003-support-king-llc-spyfonecom-matter [hereinafter SpyFone]; Complaint, *In re Zoom Video Communications, Inc.*, FTC File No. 1923167 (Feb. 1, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3167-zoom-video-communications-inc-matter [hereinafter Zoom]; Complaint, *In re Uber Technologies, Inc.*, FTC File No. 1523054 (Oct. 26, 2018), https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3054-c-4662-uber-technologies-inc-matter [hereinafter Uber]; Complaint, *In re Paypal, Inc.*, FTC File No. 1623102 (May. 24, 2018), https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3102-paypal-inc-matter (Venmo hiding inadequate data security systems from regulators and consumers, allowing hackers to access users' accounts and use their funds) [hereinafter Paypal].

[835] *See, e.g.*, Bree Fowler, *Data Breaches Break Record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/. Statista provides a graph of the number of reported data breaches dating back to 2005 (at which time there were 157); Statista Rsch. Dep't, *Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to First Half 2022*, Statista (Aug. 31, 2022), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-

that inadequate data security practices do not benefit consumers or competition—quite the opposite.

6.1. It is an unfair and deceptive practice to collect, process, retain, or transfer personal data without maintaining reasonable administrative, technical, and physical measures to secure such data against unauthorized access.

Consumers rely on the entities that collect their personal data to take the necessary steps to protect that data. The company decides what data to collect, how long to retain it, how to dispose of it, and how to safeguard it from unauthorized access throughout the lifecycle of its use. There are cost-effective and well-established methods for reducing the likelihood of breaches and for mitigating the amount of harm caused by unauthorized access when it does occur. Poor data security practices increase the likelihood and severity of breaches, which in turn increase the risk of identity theft and other harms to consumers. It is an unfair trade practice when entities fail to maintain reasonable data security practices—poor data security practices lead to increased risk of identity theft and other harms; consumers do not have the expertise to evaluate an entity's data security practices nor can

---

number-of-breaches-and-records-exposed/; *see also Adobe Breach Impacted At Least 38 Million Users*, Krebs on Security (Oct. 29, 2013), https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/; Andrew J. Hawkins, *Uber Admits to Covering up Massive 2016 Data Breach in Settlement with US Prosecutors*, Verge (July 25, 2022), https://www.smh.com.au/business/companies/uber-to-pay-204m-to-settle-data-breach-cover-up-20180927-p5069k.html (impacting 57 million people); Alvaro Puig, *Equifax Data Breach Settlement: What You Should Know*, FTC Consumer Alert (July 22, 2019), https://consumer.ftc.gov/consumer-alerts/2019/07/equifax-data-breach-settlement-what-you-should-know (impacting 147 million); Josh Fruhlinger, *Marriott Data Breach FAQ: How Did It Happen and What Was the Impact?*, CSO (Feb. 12, 2020), https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html (hundreds of millions impacted); Seena Gressin, *The Capital One Data Breach: Time to Check Your Credit Report*, FTC Consumer Alert (July 30, 2019), https://consumer.ftc.gov/consumer-alerts/2019/07/capital-one-data-breach-time-check-your-credit-report (100 million Americans impacted, breach including credit scores, social security numbers, and bank account numbers); Emma Bowman, *After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users*, NPR (Apr. 9, 2021), https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users; *Second Colossal LinkedIn "Breach" in 3 Months, Almost All Users Affected*, Malwarebytes Labs (June 30, 2021), https://blog.malwarebytes.com/awareness/2021/06/second-colossal-linkedin-breach-in-3-months-almost-all-users-affected/ (impacting 700 million); *T-Mobile: Breach Exposed SSN/DOB of 40M+ People*, Krebs on Security (Aug. 18, 2021), https://krebsonsecurity.com/2021/08/t-mobile-breach-exposed-ssn-dob-of-40m-people/.

consumers prevent misuse of their data after a breach; and the harms from data breaches continue at a staggering rate with no countervailing benefit to consumers nor to competition. It is also a deceptive trade practice when entities fail to disclose their deficient data security practices, including inadequate and generic disclaimers, and when entities explicitly misrepresent their data security practices to consumers.

Lax data security practices cause substantial injury to consumers because they increase the risk of breach or unauthorized access that can lead to identity theft, financial and/or public benefits fraud, and other financial losses and privacy invasions. The Commission has long recognized that breaches of personal data cause substantial injuries and that inadequate data security practices are the root cause of those breaches. As the Commission noted in its complaint against Wyndham, in which a hotel chain unfairly exposed the payment card information of hundreds of thousands of consumers across three data breaches, the "failure to implement reasonable and appropriate security measures exposed consumers' personal information to unauthorized access, collection, and use."[836] Similarly, in its complaint against D-Link, the Commission explained that "[a]s a result of Defendants' failures, thousands of Defendants' routers and cameras have been vulnerable to attacks that subject consumers' sensitive personal information and local networks to a significant risk of unauthorized access."[837] Breaches of sensitive personal information necessarily lead to losses including financial injury, identity

[836] Wyndham, *supra* note 833, at ¶ 40.
[837] D-Link, *supra* note 833, at ¶¶ 15–16, 18; *see also* Lenovo, *supra* note 833, at ¶ 11 ("And in fact, [the software at issue in Complaint] created two significant security vulnerabilities that put consumers' personal information at risk of unauthorized access."); AshleyMadison, *supra* note 833, at ¶ 31; InfoTrax, *supra* note 833, at ¶ 10(f)(iii); Equifax, *supra* note 833, at ¶ 23(A)(iv), 23(C); LightYear, *supra* note 833, at ¶ 11(d); CafePress, *supra* note 833, at ¶ 11(a).

theft, medical identity theft, fraud,[838] and other concomitant harms.[839] This is especially pronounced in large data sets, as the Commission noted in its complaint against Equifax:

> Defendant's failure to reasonably secure the sensitive personal information in their network […] has resulted in substantial injury to nearly 150 million consumers whose personal information was stolen by identity thieves. These injuries include wasted time and money to secure personal accounts and consumer reports from future identity theft, the cost of obtaining additional credit monitoring products or security freezes, and a significantly increased risk of becoming victims of identity theft in the future. Additionally, because information such as SSNs and dates of birth are immutable, identity thieves could wait years before capitalizing on the stolen information. Thus, Defendant's security failures are likely to continue to substantially injure consumers in the future.[840]

The most recent Commission reports from 2020[841] and 2021[842] show that credit card fraud and government documents or benefits fraud individually accounted for

---

[838] *See, e.g.*, InfoTrax, *supra* note 833, at ¶ 23 (noting that data breaches make identity theft and fraud more likely, even if identity theft and fraud do not occur immediately after a breach); *id.* at ¶ 25 (noting that failure to provide reasonable security "has caused or is likely to cause substantial injury to consumers in the form of fraud, identity theft, monetary loss, and time spent remedying the problem"); CafePress, *supra* note 833, at ¶ 34 (noting that breached personal information is often used to commit identity theft and fraud); LightYear, *supra* note 833, at ¶ 16 (noting that the identity theft victim's credit suffers when the thief fails to pay bills, victim's tax refund often long-delayed due to tax fraud committed by thief using victim's identity).

[839] *See e.g.*, Wyndham, *supra* note 833, at ¶ 40; InfoTrax, *supra* note 833, at ¶ 23; AshleyMadison, *supra* note 833, at ¶ 40. *See also* Bureau of Just. Stat., Dep't of Just., *Victims of Identity Theft, 2018* 11 (Apr. 2020), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf; Solove & Citron, *supra* note 61, at 745 ("Knowing that thieves may be using one's personal data for criminal ends may produce significant anxiety."); Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* 51–54 (2022) (describing the professional and personal consequences of DOJ employees' intimate privacy being violated by exposure to reporters).

[840] Equifax, *supra* note 833, at 14.

[841] FTC, *Consumer Sentinel Network: Data Book 2020* 9 (2021), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf (calculating percentage by taking fraction of number of reports by theft type out of total identity theft reports).

[842] FTC, *Consumer Sentinel Network: Data Book 2021* 9 (2021), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf (also calculating percentage by taking fraction of number of reports by theft type out of total identity theft reports).

more than 27% of identity theft reports nationwide. In 2021, the Department of Justice found that 68% of victims of identity theft suffered $1 or more in direct financial losses with their most recent incident of identity theft[843] and estimated that this fraud cost the U.S. economy more than $15 billion.[844] Similarly, in late 2020, websites used to generate auto insurance quotes were exploited to obtain personal data later used to submit fraudulent claims for pandemic and unemployment benefits.[845]

The impacts of identity theft can be far-reaching, hard to discover, and difficult to remedy after the fact. A Government Accountability Office report indicated that past victims have "lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft."[846] Yet these harms do not appear on the victim's bank statement or credit report, and can be nearly impossible to control where a Social Security Number (SSN) is used by virtue of the role the SSN plays as a government and private sector identifier.[847] To make matters worse, a stolen SSN, unlike a stolen credit card, cannot be effectively cancelled or replaced.[848] Criminals in possession of SSNs can open new financial accounts and perpetrate identity theft because many financial institutions rely on SSNs to verify transactions.[849] Research by the Bureau of Justice Statistics indicates

---

[843] Bureau of Just. Stat., *supra* note 839, at 9.
[844] *See id.* at 1 ($15.1 billion in total financial losses due to identity theft where the victim lost $1 or more). This was also true in the DOJ's two prior reports. *See* Bureau of Just. Stat., Dep't of Just., *Victims of Identity Theft, 2016* 1 (Jan. 2019), https://bjs.ojp.gov/content/pub/pdf/vit16.pdf ($17.5 billion); Bureau of Just. Stat., Dep't of Just., *Victims of Identity Theft, 2014* 7 (Sept. 2015), https://bjs.ojp.gov/content/pub/pdf/vit14.pdf ($15.4 billion).
[845] *Industry Letter Re: Cyber Fraud Alert*, N.Y. State Dep't of Fin. Servs., Cybersecurity Div. (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert.
[846] U.S. Gov't Accountability Off., GAO-14-34, *Agency Responses to Breaches of Personally Identifiable Information Need to be More Consistent* 11 (2013), http://www.gao.gov/assets/660/659572.pdf.
[847] Br. of Amicus Curiae EPIC at 14, *Storm v. Paytime, Inc.*, No. 15-3690 (3d Cir. Apr. 18, 2016), https://epic.org/documents/storm-v-paytime-inc/.
[848] *Id.* at 13.
[849] Social Security Admin., *Identity Theft and Your Social Security Number* 1 (2021), https://www.ssa.gov/pubs/EN-05-10064.pdf ("A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.").

that identity theft can result in severe distress, per its most recent Victims of Identity Theft report:

> In the 2018 study, victims were asked to rate how distressing the most recent incident of identity theft was to them on a 4-point scale, ranging from not at all distressing to severely distressing. Among all identity-theft victims, 8% reported that the crime was severely distressing (table 9). The percentage of victims reporting that the crime was severely distressing was higher among those who experienced the opening of a new account only (15%), misuse of personal information only (17%), or multiple types of identity theft (16%), than among those who experienced the misuse of only one type of existing account (7%). Severe distress was most prevalent among victims who experienced multiple types of identity theft that included misuse of an existing account or misuse of personal information to open a new account or for other fraudulent purposes (25%).[850]

Medical identity theft can also be particularly costly for consumers and has become more prevalent over the past several years. AARP observed that cases of medical identity theft reported to the Commission rose "from about 6,800 in 2017 to nearly 43,000 in 2021," an increase of more than 500 percent.[851] Any individual instance of medical identity theft "can endure for years," with victims suffering "long term problems with aggressive medical debt collection" and "severely impaired credit" due to fraudulent bills.[852] The non-economic risks of medical identity theft are also alarming—if the fraudster's medical information is incorporated into the victim's records, that person could receive incorrect diagnoses and treatments.

The harms caused by data breaches are not reasonably avoidable by consumers. There is no way for consumers to avoid the harms caused by lax data security practices because consumers cannot evaluate a business's data security practices ex ante and cannot prevent misuse of breached data ex post. And in many cases the consumer does not have a direct relationship with the entity holding their data or, if they do, does not have a meaningful choice in the entities that process and

[850] Bureau of Just. Stat., *supra* note 839.
[851] *Medical Identity Theft*, AARP, https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html (last visited Nov. 15, 2022).
[852] *Id.*

store their data. A consumer cannot "take their business elsewhere" (nor even take their data elsewhere) when an entity like Equifax demonstrates poor data security practices; every consumer in the country is subject to credit reports.[853] Even in circumstances where it is technically possible for a consumer to switch providers, logistically it may prove difficult where the service (e.g., internet access service) or family of proprietarily-integrated products (e.g., the Apple ecosystem) are necessary to the consumer's day-to-day activities and cannot be easily switched—it is not as simple for the consumer as switching brands of beverage or cereal. And consumers do not have any mechanism to know what, if any, data security practices companies have implemented. Even if the consumer could know what data security practices every company was using, the average consumer is not a cybersecurity expert and could not translate that knowledge into any operationalizable decision to use or not use specific services. The burden should be on a business that collects or retains personal data to maintain reasonable security standards; the business is the only entity in a position to implement the necessary safeguards to secure the data.

The market does not incentivize good data security, and consumers are unable to change this dynamic on their own. As one example, in 2017 consumer reporting agency (CRA) Equifax reported a breach impacting more than 147 million consumers, including the exposure of more than 145 million SSNs.[854] Consumers do not need to opt in to their data being collected by CRAs, nor can they opt out by virtue of the CRA's role.[855] As such, consumers are unable to exert meaningful market pressure on CRAs to improve their data security practices. Even where there is a direct relationship between the consumer and the company, for example health insurance, it may be difficult for consumers to exert their market power.[856]

---

[853] *The Equifax Data Breach*, FTC, https://www.ftc.gov/equifax-data-breach (last visited Nov. 15, 2022).
[854] Equifax, *supra* note 833, at ¶ 13.
[855] *What Is a Credit Reporting Agency?*, CFPB (Sept. 1, 2020), https://www.consumerfinance.gov/ask-cfpb/what-is-a-credit-reporting-company-en-1251/. However, consumers can opt-out of receiving pre-screened offers. *See, e.g.*, *Opting Out of Getting Prescreened Offers*, CFPB, https://consumer.ftc.gov/articles/prescreened-credit-insurance-offers#opt (last visited Nov. 15, 2022).
[856] *See, e.g.*, Jessica Davis, *Anthem Settles with 44 States for $40M Over 2014 Breach of 78.8M*, HealthITSecurity (Oct. 1, 2020), https://healthitsecurity.com/news/anthem-settles-with-44-states-for-40m-over-2014-breach-of-78.8m.

But unlike consumers, the businesses that collect, process, and store personal data can adopt security measures to protect that data. The Department of Homeland Security has estimated that 85 percent of data breaches were preventable;[857] more recently, the Internet Society estimated that 95 percent of breaches could have been prevented.[858] The Commission has often noted that reasonable security measures are a relatively minimal cost.[859] However, companies do not currently have adequate incentives to prevent data breaches despite the serious externalized costs for consumers and the American economy when these breaches occur. Companies must face significant penalties for falling behind in their data security safeguards, or else it will be more profitable to spend less on security and take the risk.[860] The Supreme Court has acknowledged that "[d]amages also force defendants to internalize the full measure of the damages that they cause and take sufficient care to prevent future harms."[861] The Commission should issue rules that set baselines for reasonable security measures and shift the incentive structure such that it is more costly for companies to have bad data security practices than good.

Poor data security practices do not offer countervailing benefits to competition nor to consumers that outweigh the injury or harm of data breaches to consumers and to the economy. There is no question that data breaches are harmful to consumers, and these breaches have no benefit whatsoever. As noted above, the Justice Department's Bureau of Justice Statistics has consistently

---

[857] 37 Dep't of Homeland Sec. Comput. Emergency Readiness Team, TA15-119, Alert: Top 30 Targeted High Risk Vulnerabilities (2016), https://www.us-cert.gov/ncas/alerts/TA15-119A. The California AG's Office similarly concluded that many of the hundreds of breaches it studied could have been prevented, or detected and corrected more rapidly, by implementation of its recommended data security controls. *See* Kamala D. Harris, Attorney General, *California Data Breach Report* 32 (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.
[858] Internet Society's Online Trust Alliance, *2018 Cyber Incident & Breach Trends Report* 3 (July 9, 2019), https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf.
[859] *See, e.g.*, CafePress, *supra* note 833, at ¶ 11(a), 11(i)(i); SkyMed, *supra* note 833, at ¶ 23; InfoTrax, *supra* note 833, at ¶ 11; LightYear, *supra* note 833, at ¶ 22; Equifax, *supra* note 833, at ¶¶ 23(A)(iv), 24; AshleyMadison, *supra* note 833, at ¶ 42; Levono, *supra* note 833, at ¶ 25.
[860] *See, e.g.*, Bruce Schneier, *The Uber Hack Exposes More Than Failed Data Security*, The New York Times (Sept. 26, 2022), https://www.nytimes.com/2022/09/26/opinion/uber-hack-data.html; Michael Kende, *How Secure Is Our Data, Really?*, MIT Press Reader (May 16, 2021), https://thereader.mitpress.mit.edu/how-secure-is-our-data-really/.
[861] *Friends of the Earth v. Laidlaw Envtl. Serv. (TOC), Inc.*, 528 U.S. 167, 185 (2000) (finding that civil penalties have a deterrent effect and can therefore prevent future harm).

estimated that identity theft costs the U.S. economy more than $15 billion dollars annually in consumer losses alone.[862] There is also no commercial benefit to poor data security practices because companies should not compete on who can provide lower levels of data security. Multiple experts have highlighted the market failures (namely: externalized costs) that prevent competitive pressure from mitigating data breaches.[863] The Commission has repeatedly noted in its unfairness actions that companies could have prevented unauthorized access with low-cost security measures.[864] And should even those measures prove insufficient, cyber insurance can mitigate the burden on companies. Companies must be incentivized to make use of cost-effective harm-mitigation techniques. Indeed, a rule requiring companies to adopt reasonable data security measures would likely help to spur competition in the data security field by ensuring that companies will continue to demand better security services.

Poor data security is prevalent in the market. There is extensive evidence of inadequate data security in the marketplace, as recent Congressional testimony highlights[865] and as the past 10+ years of data breaches[866] and FTC data security cases[867] have shown. In its most recent annual report, the Identity Theft Resource Center estimated a record-breaking 1,862 data breaches occurred in 2021.[868] As

---

[862] *See* Bureau of Just. Stat., *supra* note 844.
[863] *See, e.g.*, Schneier, *supra* note 860; Kende, *supra* note 860; James C. Cooper & Bruce H. Kobayashi, *Unreasonable: A Strict Liability Solution to the FTC's Data Security Problem*, 28 Mich. Tech. L. Rev. 257, 263–64 (2022), https://repository.law.umich.edu/mtlr/vol28/iss2/3.
[864] *See, e.g.*, CafePress, *supra* note 833, at ¶ 11(a), 11(i)(i); SkyMed, *supra* note 833, at ¶ 23; InfoTrax, *supra* note 833, at ¶ 11; LightYear, *supra* note 833, at ¶ 22; Equifax, *supra* note 833, at ¶¶ 23(A)(iv), 24; AshleyMadison, *supra* note 833, at ¶ 42; Lenovo, *supra* note 833, at ¶ 25.
[865] A data security whistleblower from Twitter called attention to problems that are likely pervasive across the industry. *Data Security at Risk: Testimony from a Twitter Whistleblower: Hearing Before the S. Comm. on the Judiciary*, 117th Cong. (2022), https://www.judiciary.senate.gov/meetings/data-security-at-risk-testimony-from-a-twitter-whistleblower ("So what are the problems, I discovered two basic issues. First, they don't know what data they have, where it lives, or where it came from. And so unsurprisingly, they can't protect it…. And this leads to the second problem, which is, the employees then have to have too much access to too much data and too many systems.").
[866] *See supra* note 835.
[867] *See supra* notes 833–834.
[868] *Record Number of Data Breaches in 2021*, IAPP Daily Dashboard (Jan. 25, 2022), https://iapp.org/news/a/record-number-of-data-breaches-in-2021/ (citing to ITRC report which estimated "1,862 breaches last year, up 68% from the year prior, and exceeded 2017's previous record of 1,506").

noted above, 95 percent of breaches could have been prevented.[869] A survey by IBM attributes a recent decline in response capabilities to the fact that approximately only one quarter of organizations with response plans (itself only 77% of organizations) apply them across the enterprise and that one quarter of organizations with plans admitted that their plans were informal or ad hoc.[870] One cybersecurity certification company identified numerous deficiencies resulting from inadequate staffing, including the failure to patch vulnerabilities in a timely fashion, to engage in ongoing risk assessment and management, and to train employees.[871] Companies must be incentivized to invest in staff and procedures to safeguard the consumer data with which they have been entrusted, or multiple breaches each impacting tens or hundreds of millions of Americans will continue to occur every year. The unfair practice of poor data security is prevalent and the harm of unauthorized access resulting in increased risk of identity theft is persistent.

It is also a deceptive practice for an entity to fail to maintain reasonable security measures when they represent that they secure the data they collect; the Commission should be able to issue penalties for first-time violations. Companies that fail to protect the data they collect not only engage in unfair business practices, they also deceive consumers through their material omissions and misleading misrepresentations about how they protect user data. The Commission should establish a data security deception rule to ensure that companies are penalized for these deceptive acts.

Consumer protection experts have called for the application of the Magnuson-Moss Warranty Federal Trade Improvement Act (Warranty Act) to deficient cybersecurity practices, in particular deficiencies exhibited by Internet of Things companies.[872] Their argument is presented here primarily for analogical

---

[869] Internet Society's Online Trust Alliance, *supra* note 858, at 3.
[870] IBM Security, *Cyber Resilient Organization Study* 8 (2020), https://www.ibm.com/account/reg/us-en/signup?formid=urx-45839.
[871] (ISC)², *Cybersecurity Workforce Study 2022* 10 (2022), https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx.
[872] *See, e.g.*, Stacy-Ann Elvy, *Hybrid Transactions and the Internet of Things: Goods, Services, or Software?*, 74 Wash. & Lee L. Rev. 77, 119–24, 154–64 (2017); Dallin Robinson, *Click Here to Sue Everybody: Cutting the Gordian Knot of the Internet of Things with Class Action Litigation*, 26 Rich. J.L. & Tech. 4, 7

purposes, as we urge the Commission to regulate this behavior using a data security trade rule under its section 5 unfair or deceptive acts or practices authority, not under the Warranty Act, and as consumer software purchases are often licenses rather than actual sales (meaning implied warranties of fitness or merchantability may not apply).[873] In short: products and services offered as ready for public consumption are implicitly without undisclosed vulnerabilities, especially when the consumer cannot make use of the product or service without providing personal data or when the data security vulnerability threatens cascading downstream harms.[874]

In addition to material omissions, entities may affirmatively misrepresent their practices. Most companies explicitly recognize in their terms, policies, or other disclosures that they are responsible for ensuring that the personal data they collect is secured against unauthorized access or breach. Consumers also understandably expect that the companies collecting their data will take the necessary steps to protect it. When a company fails to do so, that is a deceptive trade practice: (1) it is likely to mislead a reasonable consumer, as the consumer is not in a position to evaluate the inner workings of the company's data security operations[875] and the consumer has an expectation about the company's practices;[876] and (2) it is material (likely to affect a consumer's choice or conduct)—more than 87% of consumers

(2020) (citing to *Flynn v. FCA US LLC*, 327 F.R.D. 206 (S.D. Ill. 2018) as it is "the first case to proceed past summary judgment in which no actual data breach had occurred" although the case was later dismissed upon reconsideration for lack of standing, *Flynn v. FCA US LLC*, 15-CV-855-SMY, 2020 WL 1492687, at *4 (S.D. Ill. Mar. 27, 2020), *aff'd as modified*, 39 F.4th 946 (7th Cir. 2022)).

[873] *See* Elvy, *supra* note 872, at 155.

[874] *See id.* at 155–56 ("However, if the ordinary purpose for which IOT devices are used includes the facilitation of interconnectivity and the exchange of data between devices, networks, individuals, and companies, and software and services are needed to achieve this goal, this warranty is breached where a company collecting data from an IOT device fails to secure the device and the associated data.").

[875] *Pfizer, Inc.*, 81 F.T.C. 23 (1972) ("The consumer is entitled, as a matter of marketplace fairness, to rely upon the manufacturer to have a reasonable basis for making performance claims. A consumer should not be compelled to enter into an economic gamble to determine whether a product will or will not perform as represented. The economic gamble involved in a consumer's reliance upon affirmative product claims is created by the vendors' activities, and cannot be easily avoided by consumers.").

[876] *See, e.g.*, Paypal, *supra* note 834, at ¶ 27 ("These results are directly contrary to the expectations of a reasonable consumer."). Even general statements and disclaimers cannot cure this deception. *See, e.g.*, Wyndham *supra* note 833, at ¶ 21; CafePress *supra* note 833, at ¶ 8.

indicate that they would not do business with a company if they had concerns about its security practices.[877] But consumers cannot and should not be expected to act as freelance cybersecurity experts; companies should be held to the promises that they make. The Commission should also seek civil penalties for first-time violations regarding affirmatively deceptive claims about consumer data security.

The Commission's own cases establish the prevalence of these deceptive acts in the marketplace. Examples of affirmatively deceptive conduct include: collecting phone numbers purportedly for security purposes but then using those phone numbers for advertising purposes,[878] claiming information is encrypted when it is not,[879] claiming users can control who has access to information about the user's transactions when the user cannot,[880] claiming to conduct ongoing monitoring but not doing so on a timely basis,[881] and characterizing efforts as "commercially reasonable" or "industry standard" when they are deficient.[882] These are not one-off problems. In the context of credit card payments and data security, for example, Verizon consistently reports that 44% or more of organizations fail to maintain PCI-DSS compliance in between annual compliance validations (most recently more than 56% failed to maintain compliance).[883]

The Commission has found deficient security practices to be misleading even where the company qualifies its security program with general statements, such as

---

[877] Venky Anant et al., *The Consumer-Data Opportunity and the Privacy Imperative*, McKinsey & Co. (Apr. 27, 2020), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative (April 2020) (reporting that more than 87% of consumers indicate that they would not do business with a company if they had concerns about its security practices) [hereinafter McKinsey Survey].

[878] *See, e.g.*, Complaint, *FTC v. Twitter, Inc.*, Case No. 3:22-cv-03070 (N.D. Cal. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023062TwitterFiledComplaint.pdf ; Natasha Lomas, *Yes Facebook Is Using Your 2FA Phone Number to Target You with Ads*, TechCrunch (Sept. 27, 2018), https://techcrunch.com/2018/09/27/yes-facebook-is-using-your-2fa-phone-number-to-target-you-with-ads/.

[879] *See, e.g.*, Uber, *supra* note 834, at ¶ 18(d).

[880] *See, e.g.*, Paypal, *supra* note 834, at ¶¶ 25–29.

[881] *See, e.g.*, Uber, *supra* note 834, at ¶ 13.

[882] *See, e.g.*, Wyndham, *supra* note 833, at ¶ 21; AshleyMadison, *supra* note 833, at ¶ 30(d).

[883] Verizon, *2022 Payment Security Report* 82 (Sept. 2022), https://www.verizon.com/business/resources/T38f/reports/2022-payment-security-report.pdf

characterizing them as "commercially reasonable efforts"[884] or disclaiming that "100% complete security does not presently exist anywhere online or offline."[885] Because cybersecurity is a material factor in a consumer's purchasing decision,[886] failing to disclose poor data security practices constitutes a material omission and should be treated as a deceptive act or practice.

Given the number of enforcement actions the Commission has brought addressing companies misrepresenting their data security practices, either affirmatively and explicitly or by material omission, there is sufficient precedent for the Commission to establish poor data security as a deceptive trade practice. The Commission is well aware of the problem, as its many enforcement actions attest—what is needed now is a trade rule that establishes this is a clearly deceptive act or practice and enables the Commission to obtain first-time penalty authority to deter companies from deceiving consumers through poor data security practices.

As part of this trade rule, the Commission should codify the best practice standards which it has articulated to the business community with consistency over the last decade.[887] These include: access controls,[888] secure password practices (e.g., unique passwords periodically changed) and user authentication (e.g., multi-factor

[884] Wyndham, *supra* note 833, at ¶ 21.
[885] *See, e.g.*, CafePress, *supra* note 833, at ¶ 8.
[886] McKinsey Survey, *supra* note 877.
[887] *See, e.g.*, FTC, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf; FTC, *Stick with Security: A Business Blog Series* (2015), https://www.ftc.gov/business-guidance/privacy-security/stick-with-security-business-blog-series (synthesizing takeaways from 60+ data security cases); FTC, *Careful Connections: Keeping the Internet of Things Secure* (2020), https://www.ftc.gov/business-guidance/resources/careful-connections-keeping-internet-things-secure (specific to IoT); FTC, *Cybersecurity Basics*, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/basics (last visited Nov. 15, 2022); Complaint at ¶ 13, *In re Drizly, LLC*, FTC File No. 2023185 (Oct. 24, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Complaint.pdf (2022) [hereinafter Drizly].
[888] William McGeveran, *The Duty of Data Security*, 103 Minn. L. Rev. 1135, 1189–90 (2018), https://www.minnesotalawreview.org/wp-content/uploads/2019/02/1McGeveran_FINAL.pdf (describing access controls as among the most basic components of security, common amongst multiple frameworks).

authentication),[889] segmentation of systems,[890] traffic monitoring, ongoing security reviews, data mapping, data minimization,[891] staying current on known vulnerabilities,[892] employee training, overseeing service providers and product integrations, and taking additional security precautions where appropriate (e.g., remote access,[893] storing and/or transmitting sensitive information,[894] etc.).

These measures are not sector-specific. The Commission's lessons in *Start with Security*, published more than seven years ago in June 2015, are intended for "businesses of all sizes, in all sectors."[895] These included data minimization, access controls, secure passwords and authentication, network segmentation and traffic monitoring, heightened security for sensitive personal information and for remote access, applying security practices to new products, ensuring service providers implement reasonable security measures, keeping security current and addressing known vulnerabilities, and physical security.[896] Minimum standards with flexibility as to implementation will provide the guardrails necessary to protect consumers from weak data security, but prevent regulations from becoming outdated and

---

[889] *Id.* at 1192, 1194 (noting use of out-of-the-box default passwords as an atrocious data security practice).
[890] *Id.* at 1194 (noting lack of firewalls as an atrocious data security practice).
[891] *See, e.g.*, Drizly, *supra* note 887, at ¶ 13(f) (noting Drizly's failure to use reasonable information security practices included the failure to "[h]ave a policy, procedure, or practice for inventorying and deleting consumers' personal information stored on its network that was no longer necessary."); Complaint, *In re Chegg, Inc.,* FTC File No. 2023151 at ¶ 9(f) (Oct. 31, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Complaint.pdf (similar allegation) [hereinafter Chegg].
[892] *See, e.g.*, Wyndham, *supra* note 833, at ¶¶ 24(d), 29.
[893] FTC, *Start with Security: A Guide for Business* 8 (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (lesson 6); Samuel Levine, Remarks at Cleveland-Marshall College of Law Cybersecurity and Privacy Protection Conference (May 19, 2022), https://www.ftc.gov/news-events/news/speeches/remarks-samuel-levine-cleveland-marshall-college-law-cybersecurity-privacy-protection-conference (citing to Arielle Waldman, *FBI: Ransomware hit 649 critical infrastructure entities in 2021*, SearchSecurity (Mar. 24, 2022), https://www.techtarget.com/searchsecurity/news/252515076/FBI-Ransomware-hit-649-critical-infrastructure-entities-in-2021, which states: "[p]hishing emails, remote desktop protocol (RDP) exploitation and the exploitation of software vulnerabilities" were the top three attack vectors).
[894] Equifax, *supra* note 833, at ¶¶ 22(E), 23(D).
[895] FTC, *Staff Perspective: Engage, Connect, Protect* 2 (Apr. 2018), https://www.ftc.gov/system/files/documents/reports/engage-connect-protect-ftcs-projects-plans-foster-small-business-cybersecurity-federal-trade/ecp_staffperspective_2.pdf.
[896] *See Start with Security*, *supra* note 893.

allow industry to innovate on data security in response to evolving cyber threats. In this manner, the Commission's regulations would promote rather than stifle innovation. Under a "reasonable security measures" framework, the Commission could task businesses with greater responsibility when they collect more voluminous or more sensitive data, as in each of these instances, the severity and magnitude of the harm of a possible cyber incident would become correspondingly greater.[897]

The Commission may consider established public policies among all other evidence.[898] Existing data security rules enforced by the Commission under the Children's Online Privacy Protection Act (COPPA),[899] Gramm-Leach-Bliley Act (GLBA),[900] and Federal Credit Report Act (FCRA);[901] enforced by state agencies in California,[902] Massachusetts, [903] New York,[904] Oregon,[905] and Ohio;[906] and

[897] The Commission hinted at this kind of approach in its complaint against Equifax, for example. *See* Equifax, *supra* note 833, at ¶ 24 ("Defendant could have prevented or mitigated the failures described in Paragraph 23 through cost-effective measures suitable for an organization of Defendant's size and complexity.").
[898] 15 U.S.C. § 45(n).
[899] 16 C.F.R. pt. 312; 16 C.F.R. §§ 312.3(e), 312.8.
[900] 16 C.F.R. pt. 314.
[901] 16 C.F.R. pt. 682.
[902] *See* Cal. Civ. Code §§ 1798.100(e),1798.81.5, 1798.91.04 (specific to connected devices). In 2016, then-AG of the California Department of Justice Kamala Harris also offered recommendations based on the CIS framework, which outlined explicitly parallel recommendations from NIST, ISO, HIPAA, FFIEC, and PCI DSS frameworks. *See* Harris, *supra* note 857, at 31 ("The controls are intended to apply to organizations of all sizes and are designed to be implementable and scalable."); *id.* at Appendix B.
[903] 201 Mass. Code Regs. 17.00 (2010).
[904] N.Y. Comp. Codes R. & Regs. tit. 23, § 500 (2022) (NYDFS regs); S. 5575B, § 899-bb, 2019 Reg. Sess. (N.Y. 2019), https://legislation.nysenate.gov/pdf/bills/2019/S5575B (SHIELD Act data security provisions).
[905] S. 684, 80th Leg., 2019 Regular Session (Or. 2019).
[906] Ohio Rev. Code § 1354 (2018) (allowing for an affirmative defense to tort claims for failure to implement reasonable security controls where that company's cybersecurity program reasonably conforms to one of several industry recognized frameworks, including NIST, HIPAA, GLBA, and PCI-DSS).

encouraged through frameworks like those proposed by FINRA,[907] NIST,[908] and CISA[909] offer persuasive evidence in support of what the Commission has outlined repeatedly in its own section 5 enforcement efforts.

All businesses should adopt a **duty of care** approach to the consumer data that they collect; if they can't protect it, they shouldn't collect it. A Senate report emphasized, in the wake of the Equifax data breach, that "[c]onsumers . . . understand the need to protect information like online passwords, pin numbers, and Social Security numbers. But a consumer taking appropriate care of this information may not be enough to keep PII out of the hands of criminal hackers."[910] Consumers should not bear the burden of preventing harm from data breaches. Beyond entities like Equifax, the Commission itself has noted that social media companies, retailers, apps, and devices "are still covered by the FTC Act's prohibition against deceptive or unfair conduct, including with respect to their use and protection of consumer information."[911] As such, reasonable data security should include a duty of care for consumer data within the company's custody.

---

[907] *See, e.g.*, FINRA, *Report on Cybersecurity Practices* (Feb 2015), https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf [hereinafter FINRA 2015]; FINRA, *Core Cybersecurity Threats and Effective Controls for Small Firms* (May 2022), https://www.finra.org/sites/default/files/2022-05/Core_Cybersecurity_Threats_and_Effective_Controls-Small_Firms.pdf [hereinafter FINRA 2022].

[908] NIST, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1* (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [hereinafter NIST 1.1]; NIST, *Getting Started with the NIST Cybersecurity Framework: A Quickstart Guide* (Updated Apr. 19, 2022), https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide [hereinafter NIST Quickstart] (providing a helpful high-level overview).

[909] CISA, *Cross-Sector Cybersecurity Performance Goals* (2022), https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf [hereinafter CISA Goals].

[910] *See* Staff of Permanent Subcomm. on Investigations, S. Comm. on Homeland Sec. & Governmental Affs., 116th Cong., *How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach* 1 (Comm. Print 2019), https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf.

[911] Final Rule, FTC, *Standards for Safeguarding Customer Information* (Dec. 9, 2021), https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information (first citing *In re Facebook, Inc.*, Docket No. C-4365 (Apr. 28, 2020); then citing *FTC* v. *Wyndham Worldwide Corporation,* 799 F.3d 236 (3d Cir. 2015); then citing *FTC v. D-Link Systems, Inc.*, Case No. 3:17-cv-00039-JD (N.D. Cal. July 2, 2019); and then citing *Twitter, Inc.*, Docket No. C-4316 (Mar. 11, 2011)).

Data mapping can ensure that a company understands the scope of what it must protect, what safeguards or security measures it should adopt, and the way it should respond when its security measures have failed to prevent a breach. As Profs. Solove and Hartzog have explained:

> Privacy requirements such as data mapping provide awareness about potential security vulnerabilities. Data mapping shows what data is being collected and maintained, the purposes for having this data, the whereabouts of this data, and other key information.[912]

It is difficult to imagine a company could consider itself "prepared" to respond to a cyber incident if it does not map what data it collects and where it is stored.[913] It also seems unlikely that a company could detect unauthorized access of data if it does not map out which users and which partners are permitted to access which databases. Data mapping can support other important basic cybersecurity practices, such as access controls, segmentation of systems, and traffic monitoring (see immediately below). Twitter whistleblower Peter "Mudge" Zatko recently highlighted this issue in testimony before Congress, stating, "I discovered two basic issues. First, they don't know what data they have, where it lives, or where it came from. And so unsurprisingly, they can't protect it."[914] The problem is not unique to Twitter—two Meta engineers questioned during a recent court hearing admitted that there is no single individual within Meta who would be able to answer where all the data on a single user is stored, and moreover that "[i]t would take a significant team effort to even be able to answer that question."[915] In several Complaints over the last three years, the Commission has identified the failure to

---

[912] Daniel J. Solove & Woodrow Hartzog, *Breached! Why Data Security Law Fails and How to Improve It* 156–57 (2022).

[913] This is also consistent with NIST and FINRA frameworks. *See* McGeveran, *supra* note 888, at 1183–84 ("The NIST Framework and FINRA's small business self-assessment tool similarly begin with identification of personal data and associated vulnerabilities."); *see also* NIST 1.1, *supra* note 908, at 24.

[914] *See Data Security at Risk*, *supra* note 865.

[915] Isobel Asher Hamilton, *Senior Facebook Engineers Say No One at the Company Knows Where Your Data Is Kept*, Bus. Insider (Sept. 8, 2022), https://www.businessinsider.com/meta-doesnt-know-where-all-your-data-is-engineers-say-2022-9.

map data as a deficient security practice.[916] The Commission should issue a rule that requires data mapping.

Among the most basic data security practices is implementing **access controls**.[917] Access controls limit how users can discover and interact with data on the company's network, often using a "least privilege" system.[918] The Commission took this very approach in the final Safeguards Rule, finding it inappropriate for all employees and service providers to have access to all customer information, and that in addition to implementing access controls, a financial institution must "restrict access only to customer information needed to perform a specific function."[919] Access controls are a means by which a company can reduce the risk of consumer harm without reducing the amount or type of consumer data it collects.

---

[916] *See, e.g.*, InfoTrax, *supra* note 833, at ¶ 14; Equifax, *supra* note 833, at ¶ 22(B); Zoom, *supra* note 834, at ¶ 12(g).

[917] FTC et al., *Cybersecurity for Small Business: Cybersecurity Basics* 3, https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf (last visited Nov. 21, 2022) ("Control who logs on to your network and uses your computers and other devices.") (last visited Nov. 15, 2022) [hereinafter Cybersecurity Basics]; *Data Security at Risk supra* note 865 ("And this [the absence of data mapping] leads to the second problem, which is, the employees then have to have too much access to too much data and too many systems."); *FTC Safeguards Rule: What Your Business Needs to Know*, FTC, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last visited Nov. 15, 2022) (citing to 314.4(c)(1) of Safeguards Rule); Wyndham, *supra* note 833, at ¶ 24(j); Chegg, *supra* note 891, at ¶ 9(a); Drizly, *supra* note 887, at ¶ 13(c); Uber, *supra* note 834, at ¶ 18(a); SkyMed, *supra* note 833, at ¶ 12(c); InfoTrax, *supra* note 833, at ¶ 10(d); LightYear, *supra* note 833, at ¶ 11(e); Equifax, *supra* note 833, at ¶¶ 22(D), 23(C); SpyFone, *supra* note 834, at ¶ 17(b); AshleyMadison, *supra* note 833, at ¶ 31(b); 201 Mass. Code Regs. 17.04(1)(d,3), 17.04(2) (2010), https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the/download; N.Y. Comp. Codes R. & Regs. tit. 23, § 500.07 (2022); FINRA 2015, *supra* note 907, at 17–20; FINRA 2022, *supra* note 907, at 7; NIST Quickstart, *supra* note 908 ("Manage access to assets and information"); CISA Goals, *supra* note 909, at 9 (control 1.5); NIST 1.1, *supra* note 908, at 29, 30.

[918] Michael Gegick & Sean Barnum, *Least Privilege*, CISA https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/least-privilege (last visited Nov. 15, 2022); National Initiative for Cybersecurity Careers and Studies (NICCS), *Protecting Windows Systems with Access Controls, Encryption, and Group Policy* (Aug. 16, 2022), https://niccs.cisa.gov/education-training/catalog/infosec-learning-llc/protecting-windows-systems-access-controls; NIST 1.1, *supra* note 908, at 30.

[919] Final Rule, FTC, *Standards for Safeguarding Customer Information*, 86 Fed. Reg. 70286 (Dec. 9, 2021), https://www.govinfo.gov/content/pkg/FR-2021-12-09/pdf/2021-25736.pdf (noting that "[s]uch overbroad access could create additional harm in the event of an intruder gaining access to a system by impersonating an employee or service provider").

The Commission has raised this issue in past complaints, stating in the 2010 Complaint against Twitter:

> From approximately July 2006 until July 2009, Twitter granted almost all of its employees the ability to exercise administrative control of the Twitter system, including the ability to: reset a user's account password, view a user's nonpublic tweets and other nonpublic user information, and send tweets on behalf of a user. Such employees have accessed these administrative controls using administrative credentials, composed of a user name and administrative password.[920]

The Consent Order the Commission entered into with Twitter required a "comprehensive information security program," but no specific requirements regarding limiting the number of employees with administrative control.[921] And it seems Twitter chose not to address the issue—in Peter "Mudge" Zatko's whistleblower complaint filed earlier this year with the Securities and Exchange Commission, he said he found "serious access control problems, with far too many staff (about half of Twitter's 10,000 employees, and growing) given access to sensitive live production systems and user data in order to do their jobs."[922] And this access control problem has real consequences: according to Mudge's complaint, "In 2020 alone, Twitter had more than 40 security incidents, 70% of which were access control-related. These included 20 incidents defined as breaches; all but two of which were access control related."[923]

[920] *See, e.g.*, Complaint at ¶ 7, *In re Twitter*, FTC File No. 092 3093 (Mar. 11, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twittercmpt.pdf.
[921] Decision and Order, *In re Twitter*, FTC File No. 092-3093 (Mar. 11, 2011).
[922] Peter "Mudge" Zatko, Whistleblower Aid, *Re: Protected Disclosures of Federal Trade Commission Act Violations, Material Misrepresentations and Omissions, and Fraud by Twitter, Inc.* 27–28 (July 6, 2022), https://s3.documentcloud.org/documents/22186683/twitter-whistleblower-disclosure.pdf (internal citations omitted).
[923] *Id.* at 28.

Secure password practices,[924] **user authentication**,[925] and **segmentation of systems**[926] are also critical.[927] Deficient password practices can include failing to change passwords from manufacturer defaults or using easy-to-guess passwords,[928] failing to adequately protect password databases from attacks by hackers,[929] failing to revoke passwords for ex-employees of service providers,[930] allowing employees to reuse passwords to access multiple services,[931] and failing to monitor unsuccessful login attempts.[932] Deficient authentication practices can include failing to provide security notifications to users when login credentials were changed,[933] failing to require multi-factor authentication,[934] failing to require authentication to access backup databases,[935] and failing to prevent bad actors from using breached authentication data to verify a user.[936] Segmentation of systems (e.g., internal firewalls)[937] can help to limit how much consumer harm results from a single breach by making it difficult for a threat actor infiltrating one part of the company's

---

[924] 201 Mass. Code Regs. 17.04(1)(b)–(c) (2010).
[925] *See FTC Safeguards Rule: What Your Business Needs to Know*, *supra* note 917 (citing to 314.4(c)(5) of Safeguards Rule); Cybersecurity Basics, *supra* note 917, at 1, 6, 20, 24 ("Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password—like a temporary code on a smartphone or a key that's inserted into a computer."); 201 Mass. Code Regs. 17.04(1) (2010); N.Y. Comp. Codes R. & Regs. Tit. 23, § 500.12 (2022); CISA Goals, *supra* note 909, at 8 (control 1.3); NIST 1.1 *supra* note 908, at 30.
[926] Wyndham, *supra* note 833, at ¶ 24(a). The PCI-DSS framework which safeguards payment card data also requires this. *See* McGeveran, *supra* note 888, at 1166 (citing to Requirement 1 of PCI-DSS); *see also* CISA Goals, *supra* note 909, at 22(control 8.1); NIST 1.1 *supra* note 908, at 30.
[927] Indeed, cyber insurance companies seem to agree on this point. *See* McGeveran, *supra* note 888, at 1172–73 (citing to *Sample cyber insurance applications*, IAPP, https://iapp.org/resources/article/sample-cyberinsurance-applications/ (last visited Nov. 15, 2022)) (noting that all three companies inquire about firewalls, password strength, and multifactor authentication in their risk assessment questionnaires).
[928] *See, e.g.*, Wyndham, *supra* note 833, ¶¶ 24(e)–(f); CafePress, *supra* note 833, at ¶ 11(f); CISA Goals, *supra* note 909, at 8–9 (controls 1.2, 1.4).
[929] *See, e.g.*, Chegg, *supra* note 891, at ¶¶ 9(b)–(c); CafePress, *supra* note 833, at ¶ 11(c); Equifax, *supra* note 833, at ¶ 22(D); D-Link, *supra* note 833, at ¶ 15(b),(c).
[930] AshleyMadison, *supra* note 833, at ¶ 31(b)(iii); CISA Goals, *supra* note 909, at 10 (control 1.7).
[931] AshleyMadison, *supra* note 833, at ¶ 31(b)(vi); CISA Goals, *supra* note 909, at 9 (control 1.6).
[932] AshleyMadison, *supra* note 833, at ¶ 31(b)(i).
[933] Paypal, *supra* note 834, at ¶ 40(c)(1).
[934] Uber, *supra* note 834, at ¶ 18(a)(iii), 24; Zoom, *supra* note 834, at ¶ 12(d).
[935] LightYear, *supra* note 833, at ¶ 11(e).
[936] CafePress, *supra* note 833, at ¶ 25.
[937] *See, e.g.*, Wyndham, *supra* note 833, at ¶ 24(a), 28; Zoom, *supra* note 834, at ¶ 12(e); Equifax, *supra* note 833, at ¶¶ 22(C)–(D), 23(B); InfoTrax, *supra* note 833, at ¶ 10(e).

network to access other parts of the network. The Commission should set minimum requirements for secure password practices, user authentication, and segmentation of systems.

Traffic monitoring, **staying current on known vulnerabilities**, **security reviews**, and **employee training** are active measures that a company should be required to undertake to continually safeguard consumer data from breach. Traffic monitoring facilitates early detection of attempts at unauthorized access.[938] The Commission has identified the failure to monitor traffic as a deficient security practice in numerous complaints.[939] Precautions against known vulnerabilities, such as prompt installation of security patches and software updates, can reduce the likelihood of breach, preventing unauthorized access in the first place.[940] When teams at other organizations discover an attack vector that could be used to gain unauthorized access to consumer data and share that information with the rest of the industry, that attack vector becomes a known vulnerability. When a company decides not to safeguard against that vulnerability, that company is knowingly leaving a door open for bad actors to access the consumer data entrusted to their care. Security reviews, such as penetration testing or pen-testing, can help to identify deficiencies.[941] The Commission has identified the failure to safeguard

---

[938] *See* Cybersecurity Basics, *supra* note 917, at 4 ("Monitor your computers for unauthorized personnel access, devices (like USB drives), and software."; "Check your network for unauthorized users or connections."; "Investigate any unusual activities on your network or by your staff."); 16 C.F.R. pt. 314.4(c)(8) ; N.Y. Comp. Codes R. & Regs. Tit. 23, § 500.06 (2022); NIST Quickstart, *supra* note 908 ("Maintain and monitor logs"); CISA Goals, *supra* note 909, at 8 (control 1.1); NIST 1.1, *supra* note 908, at 36, 38–39.

[939] Wyndham, *supra* note 833, at ¶¶ 24(h)–(i); Chegg, *supra* note 891, at ¶ 9(g); SkyMed, *supra* note 833, at ¶ 12(f); InfoTrax, *supra* note 833, at ¶¶ 10(f), 17; LightYear, *supra* note 833, at ¶ 11(d); Equifax, *supra* note 833, at ¶¶ 22(F), 23(A)(iii)–(iv), 23(C)(iii); AshleyMadison, *supra* note 833, at ¶ 35; Zoom, *supra* note 834, at ¶ 12(e).

[940] Again, cyber insurance companies seem to agree on this point. *See* McGeveran, *supra* note 888, at 1172–73 (citing to IAPP, sample cyber insurance applications, and noting that all three companies inquire about patching in their risk assessment questionnaires); *see also Known Exploited Vulnerabilities Catalog*, Cybersecurity & Infrastructure Sec. Agency, https://www.cisa.gov/known-exploited-vulnerabilities-catalog (last visited Nov. 15, 2022); NIST Quickstart, *supra* note 908 ("Manage device vulnerabilities"); CISA Goals, *supra* note 909, at 17 (control 5.1); NIST 1.1, *supra* note 908, at 26, 36, 39, 43.

[941] *See, e.g.*, *FTC Safeguards Rule: What Your Business Needs to Know*, *supra* note 917 ("assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of

against known vulnerabilities and the failure to conduct security reviews as deficient security practices in numerous complaints.[942] Employee training can protect against social engineering attacks such as phishing attempts.[943] Commission complaints have cited to the lack of employee training as a deficiency on numerous occasions, with regard to both engineers and other employees.[944] The Commission should set minimum requirements for traffic monitoring, response to known vulnerabilities, security reviews, and employee training.

---

databases or controls from outside or inside your information systems"); Drizly, *supra* note 887, at ¶¶ 13(d)–(e); N.Y. Comp. Codes R. & Regs. tit. 23, § 500.05 (2022); FINRA 2015 at 21–22; *see also* 16 C.F.R. pts. 314.4(b)(2), 314.4(d), 314.4(g); 201 Mass. Code Regs. 17.03(2)(h)–(i) (2010); McGeveran, *supra* note 888, at 1187–88 ("Numerous frameworks call for continual risk assessment. This effectively becomes a duty of ongoing monitoring…. The FTC has taken action against over a dozen companies for failure to test against widely known vulnerabilities. This firmly established requirement of consistent self-examination helps security systems remain up-to-date with technology and changing threat models.") (internal citations omitted); NIST Quickstart, *supra* note 908 ("Test and update detection process"); CISA Goals, *supra* note 909, at 18 (control 5.6); NIST 1.1, *supra* note 908, at 33, 40.

[942] The two practices are related, as security reviews should entail confirming that the system has been shored up against known vulnerabilities, including replacing equipment that no longer receives security patches. *See, e.g.*, Wyndham, *supra* note 833, at ¶¶ 24(d), 29; CafePress, *supra* note 833, at ¶¶ 11(a), (d)–(e); Equifax, *supra* note 833, at ¶¶ 22(A), 23(A); D-Link, *supra* note 833, at ¶ 15(a); Zoom, *supra* note 834, at ¶ 12(b). Security review practices can include pen-testing, vulnerability testing, reviewing logs, etc. *See, e.g.*, CafePress, *supra* note 833, at ¶ 11(h); SkyMed, *supra* note 833, at ¶ 12(d); InfoTrax, *supra* note 833, at ¶ 10(b); LightYear, *supra* note 833, at ¶¶ 10, 11(c)–(d); D-Link, *supra* note 833, at ¶ 15(a); AshleyMadison, *supra* note 833, at ¶ 31(e); SpyFone, *supra* note 834, at ¶ 17(c); Zoom, *supra* note 834, at ¶ 12(b); PayPal, *supra* note 834, at ¶ 40(b).

[943] *See Security Tip (ST04-014): Avoiding Social Engineering and Phishing Attacks*, CISA (Aug. 25, 2020), https://www.cisa.gov/uscert/ncas/tips/ST04-014; Cybersecurity Basics, *supra* note 917, at 10 ("Keep in mind that phishing scammers change their tactics often, so make sure you include tips for spotting the latest phishing schemes in your regular training"); *id.* at 11 ("Teach [staff] how to avoid phishing scams and show them some of the common ways attackers can infect computers and devices with malware. Include tips for spotting and protecting against cyber threats in your regular employee trainings and communications."); *see also* 16 C.F.R. pt. 314.4(e); 201 Mass. Code Regs. 17.03(2)(b)(1), 17.04(8) (2010), https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the/download; N.Y. Comp. Codes R. & Regs. tit. 23, § 500.10, 500.14 (2022); FINRA 2015, *supra* note 907, at 31–32; FINRA 2022, *supra* note 907, at 10; NIST Quickstart, *supra* note 908 ("Train users"); CISA Goals, *supra* note 909, at 15 (controls 4.3, 4.4); NIST 1.1, *supra* note 908, at 31.

[944] *See, e.g.*, Chegg *supra* note 891, at ¶ 9(e); SkyMed, *supra* note 833, at ¶ 12(b); Lightyear, *supra* note 833, at ¶ 11(b); Equifax, *supra* note 833, at ¶ 23(E); AshleyMadison, *supra* note 833, at ¶ 31(c); Zoom, *supra* note 834, at ¶ 12(a); Uber, *supra* note 834, at ¶ 18(b).

Companies must be required exercise additional measures to ensure they are that they are **overseeing service providers and product integrations**[945] and that they **implement stronger protections in higher-risk situations**.[946] These measures go beyond basic cybersecurity hygiene, as they must be proportionate to the level of risk. Under both COPPA[947] and GLBA,[948] the Commission has imposed an expectation that companies will use reasonable means to confirm that service providers or third parties with access to data not merely implement but actively maintain adequate safeguards to ensure the confidentiality and security of consumer information. "The Commission views the regular assessment of the security risk of service providers as an important part of maintaining the strength of a financial institution's safeguards."[949] However, under its section 5 authority, the

---

[945] 16 C.F.R. pt. 314.4(f); 201 Mass. Code Regs. 17.03(2)(f) (2010); McGeveran, *supra* note 888, at 1171 (noting private sector framework of Vendor Security Alliance proposes a standard questionnaire for evaluating the security practices of potential service providers, including questions about access controls and pen-testing); N.Y. Comp. Codes R. & Regs. tit. 23, § 500.11 (2022); CCPA § 1798.81.5(c); FINRA 2015, *supra* note 907, at 26–30; FINRA 2022, *supra* note 907, at 6–7; CISA Goals, *supra* note 909, at 19 (controls 6.1, 6.2, 6.3); NIST 1.1, *supra* note 908, at 28, 39.

[946] *See, e.g.*, Karen Scarfone, *Security Concerns with Remote Access*, https://csrc.nist.gov/CSRC/media/Events/HIPAA-Security-Rule-Implementation-and-Assurance/documents/NIST_Remote_Access.pdf (last visited Nov. 15, 2022); NIST 1.1, *supra* note 908, at 29; N.Y. Comp. Codes R. & Regs. tit. 23, § 500.12(b) (2022); Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law against Illegal Use and Sharing of Highly Sensitive Data* FTC Bus. Blog (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal; NIST Quickstart, *supra* note 908, ("Protect sensitive data"); CISA Goals, *supra* note 909 at 14 (control 3.4).

[947] *Complying with COPPA: Frequently Asked Questions*, FTC L(1), https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (last visited Nov. 18, 2022) (referring to § 312.8).

[948] *Standards for Safeguarding Customer Information*, 16 C.F.R. § 314 (2021) (citing to 16 CFR 314.4(d)). In terms of enforcement actions, *see, e.g.*, Complaint, *In re Ascension Data & Analytics, LLC*, FTC File No. 1923126 at ¶¶ 13, 14–17, 20 (2021); Complaint, *In re TaxSlayer, LLC*, FTC File No. 1623063 at ¶ 14(d) (2017).

[949] *Standards for Safeguarding Customer Information*, 16 C.F.R. § 314 (2021), https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information (citing Kevin McCoy, *Target to Pay $18.5M for 2013 Data Breach that Affected 41 Million Consumers*, USA Today (May 23, 2017), https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/) ("For example, in 2013, attackers were reportedly able to use stolen credentials obtained from a third-party service provider to access a customer service database maintained by national retailer Target Corporation, resulting in the theft of information relating to 41 million customer payment card

Commission has identified numerous incidents of a company's failures to properly oversee third parties.[950] In multiple enforcement actions, the Commission has also emphasized the sensitivity of consumer data that has been accessed without authorization.[951] The Commission should require a heightened level of protection with respect to third parties, integrations, remote access, sensitive consumer data, and other situations that implicate greater risk of harm.

The Commission should also **incorporate privacy principles into its data security trade rule**, acknowledging that enhanced privacy can result in enhanced security, just as weak privacy is likely to result in weak security. As Profs. Dan Solove and Woody Hartzog have outlined:

> There are several ways that bad privacy can lead to bad security: (1) Weak privacy controls can lead to improper access through the front door; (2) Collecting and storing unnecessary data can make data breaches much worse; (3) Poor privacy regulation can allow for more tools and practices that compromise security; and (4) A lack of accountability over data can increase the likelihood that the data will be lost, misplaced, or misused.[952]

Ultimately, the best way to protect consumer data is to not collect, or not store, the data beyond what is reasonably necessary. Data that is never collected in the first place, or that is quickly deleted,[953] cannot be breached. Perhaps the most critical rule the Commission could promulgate to improve data security is a data minimization rule as outlined in section 1 of these comments.

---

accounts."). Supply chain security literature suggests that third parties are often a preferred attack vector. *See, e.g.,* ABA Cybersecurity Legal Task Force, *Vendor Contracting Project: Cybersecurity Checklist Second Edition* 1 (2021), https://www.potteranderson.com/media/publication/941_Vendor%20Contracting%20Project%20-%20Cybersecurity%20Checklist.pdf; *Target Hackers Broke in Via HVAC Company*, Krebs on Security (Feb. 5, 2014), https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

[950] *See, e.g.*, Wyndham, *supra* note 833, at ¶ 24(j); Lightyear, *supra* note 833, at ¶ 11(b); AshleyMadison, *supra* note 833, at ¶ 31(d); Lenovo, *supra* note 833, at ¶ 24; SpyFone, *supra* note 834, at ¶ 17(e); Zoom, *supra* note 834, at ¶ 12(c).

[951] SkyMed, *supra* note 833, at ¶ 13; InfoTrax, *supra* note 833, at ¶ 10(g); Equifax, *supra* note 833, at ¶¶ 22(E), 23(D); SpyFone, *supra* note 834, at ¶ 17(a); Uber, *supra* note 834, at ¶¶ 18(d), 20.

[952] *See* Solove & Hartzog, *supra* note 912, at 143.

[953] *See, e.g.*, 16 C.F.R. pts. 314.4(c)(6), 682; N.Y. Comp. Codes R. & Regs. tit. 23, § 500.13 (2022); NIST 1.1, *supra* note 908, at 34.

Companies should be required to document the above steps in a **written information security plan**.[954] The Commission has identified the lack of a written plan as a deficient security practice in numerous complaints.[955]

The above measures are not meant to be an exhaustive list,[956] and should apply to companies at a level commensurate with the scope and scale of the type and volume of data they collect.[957] Just as heightened measures should be required for riskier processing or processing of more sensitive types of data, less stringent measures may be required for companies collecting smaller amounts of data or types of data that inflict less severe harms if breached (e.g., state of residence as opposed to Social Security Number). This risk-based approach is already in place in the banking industry,[958] and has been enacted as data security policy at the state level.[959] It is likely that a cottage industry will emerge to assist companies with a data security regime that grows as the company's data collection and processing grows (or as those data practices become riskier).

---

[954] *Model Written Information Security Program*, IAPP, https://iapp.org/resources/article/model-written-information-security-program/ (last visited Nov. 15, 2022); 201 Mass. Code Regs. 17.03 (2010), https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the/download.

[955] *See, e.g.*, Chegg, *supra* note 891, at ¶ 9(d); Drizly, *supra* note 887, at ¶ 13(a); Skymed, *supra* note 833, at ¶ 12(a); Lightyear, *supra* note 833, at ¶ 11(a); AshleyMadison, *supra* note 833, at ¶ 31(a); Uber, *supra* note 834, at ¶¶ 18(c), 40(a).

[956] Device mapping, for example, was not addressed above, despite multiple Commission Complaints citing the failure to do so as a deficient security practice. *See, e.g.*, Wyndham, *supra* note 833, at ¶¶ 24(g), 27; LightYear, *supra* note 833, at ¶ 11(g). Similarly, encryption as opposed to storing information in plain text. *See, e.g.*, Wyndham, *supra* note 833, at ¶¶ 22(b), 31; CafePress, *supra* note 833, at ¶ 11(b); Equifax, *supra* note 833, at ¶¶ 22(D)–(E), 23(C)(i), 23(D); Uber, *supra* note 834, at ¶ 18(d); SpyFone, *supra* note 834, at ¶ 17(a).

[957] McGeveran, *supra* note 888, at 1179 (noting that across multiple data security frameworks "the duty of data security scales up or down in proportion to the resources and risk profile of each data custodian").

[958] *See, e.g.*, David W. Perkins, *Tailoring Bank Regulations: Differences in Bank Size, Activities, and Capital Levels* (Dec. 21, 2017), https://digital.library.unt.edu/ark:/67531/metadc1094396/.

[959] 201 Mass. Code Regs. 17.03(1) (2010), https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the/download (requiring a security program include "administrative, technical, and physical safeguards that are appropriate to: (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information").

That said, if the Commission imposes incident reporting requirements as part of a data security trade rule, likelihood of harm (informed by sensitivity of data) should not be a threshold requirement, as likelihood of harm may entail a legal judgment which could disincentivize timely and comprehensive reporting.[960]

In establishing a data security trade rule, the Commission should clearly articulate that rule violations can be found in either the results (e.g., a breach occurred) or in the process (e.g., data handling practices were non-secure, regardless of whether or not a breach occurred). Over its many enforcement actions, the Commission has also articulated practices which it finds to be indicative of particularly insecure ways of handling data. These have included the failure to have vulnerability disclosure policies,[961] failing to patch known software vulnerabilities, failing to segment database servers, storing SSNs in unencrypted plain text, transmitting personal information in plain text, and failing to perform vulnerability and penetration testing as part of timely security reviews.[962] Although many of these are the logical and necessary consequence of failing to fulfill the reasonable security measures described above, it may be valuable to emphasize the difference, for example, between bringing an enforcement action against a company for failing to utilize a specific encryption protocol as opposed to bringing an action for storing SSNs in a manner that allowed those SSNs to be easily obtained and misused (e.g., unencrypted, plain text).

Although all organizations should do some measure of ongoing security review, for organizations possessing a large volume of data or particularly sensitive data, an independent auditor should be responsible for assessing compliance, and their assessment should be technical, be public, use audit-like standards, and allow for external stakeholder input. High-risk organizations

---

[960] *See, e.g.*, Tech. Pol'y Clinic at Princeton's Ctr. For Info. Tech. Pol'y, *Comment Letter on Safeguards Rule, 16 CFR part 314, Project No. P145407* (Aug. 2, 2019), https://www.regulations.gov/comment/FTC-2019-0019-0054.

[961] FTC, *Public Comment on NTIA Safety Working Group's "Coordinated Vulnerability Disclosure 'Early Stage' Template"* (Feb. 16, 2017), https://www.ftc.gov/legal-library/browse/advocacy-filings/ftc-staff-comment-national-telecommunications-information-administration-regarding-safety-working.

[962] *See, e.g.*, FTC, *FTC's Use of Its Authorities to Protect Consumer Privacy and Security* (2020), https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf.

should not be allowed to "grade their own homework." As the Twitter whistleblower remarked in Congressional testimony:

> [H]ow was Twitter still operating like this? Since there was a 2011 consent decree that was aimed at addressing a fair amount of this? . . . One, there were a lot of evaluations and examinations, which were interview questions. So essentially, the organization was allowed to grade their own homework. Did you make things better? Yes, we did. Okay, check. There wasn't a lot of ground truth. There wasn't a lot of quantified measurements. And a fair amount of the interviews came from companies, auditors that Twitter themselves were able to hire. So I think that's a little bit of a maybe conflict of interest.[963]

He suggested the solution include: "accountability, and setting quantitative goals and standards that can be measured and audited independently" in order to "change management structures, and drive change in companies when it's needed such as this."[964] This emphasis on accountability and independent auditing is key.

The Commission has committed to requiring biennial assessments by independent experts in its consent decrees.[965] However, the mere fact that a third party may be conducting the assessment is no guarantee that it will incorporate sufficient evidence to achieve the Commission's consumer protection goals. The third party may overstate their competence,[966] or may merely take the company at their word, which is largely permitted by an assessment (as opposed to an audit).[967] As Professor Ari Ezra Waldman has observed in the context of privacy assessments:

> The FTC requires assessments, and assessments are not the intense, independent, under-the-hood investigations we think of when we think of audits. They leave wiggle room for regulated companies. Audits are independent third-party analyses, where the auditor herself reviews evidence and makes conclusions independent of the audit subject.

---

[963] *Data Security at Risk*, *supra* note 865.
[964] *Id.*
[965] *FTC's Use of Its Authorities to Protect Consumer Privacy and Security*, *supra* note 962.
[966] *See, e.g.*, Ari Ezra Waldman, *Outsourcing Privacy*, 96 Notre Dame L. Rev. Reflection 194, 199–201, 207–08 (2021), https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1097&context=ndlr_online.
[967] *See, e.g.*, Waldman, *supra* note 771, at 1239–1241; Chris Jay Hoofnagle, *Assessing the Federal Trade Commission's Privacy Assessments*, 14(2) IEEE Sec. & Priv. 58–64 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2707163; Gray, *supra* note 714.

> Assessments are based on assertions from management rather than wholly independent analyses from auditors, and are usually framed by goals set by management…. In other words, the only evidence showing that Google met FTC requirements was Google's statements to that effect. The fact that these assessments can be fulfilled through rough conclusory statements without independent investigation shows how assessments can become mere symbols of compliance.[968]

In the context of security rather than of privacy, one expert has characterized the difference between audits and assessments, using the example of access controls:

> One component of access control security is a strong password policy. An assessment would check to see if the organization has a strong password policy while a security audit would actually attempt to set up access with a weak password to see if the control actually has been implemented and works as defined in the policy.[969]

The Commission has authority to approve and re-approve assessors (including forcing the company to hire a different assessor) and requires assessors to "identify evidence to support their conclusions, including independent sampling, employee interviews, and document review."[970] Even these improvements are still likely to fall short of the Commission's goals unless they incorporate technical testing, external stakeholder input, and public scrutiny.[971] Encouragingly, the Commission's most recent consent decree as of the time of this writing requires that "no finding of any Assessment shall rely primarily on assertions or attestations by Respondent's management."[972]

---

[968] Waldman, *supra* note 331, at 806–07. Chris Hoofnagle has additionally noted "Furthermore, because assessments are self-certifications of compliance, they're unlikely to document departures from the duties agreed to in a consent order. In fact, assessors can find departures from duties and still conclude that the program is in compliance." Hoofnagle, *supra* note 967, at 7.
[969] Kevin G. Coleman, *Security Assessment or Security Audit?*, infoTECH Spotlight (Sept. 21, 2009), https://it.tmcnet.com/topics/it/articles/64874-security-assessment-security-audit.htm.
[970] Andrew Smith, *New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers*, FTC Bus. Blog (Jan. 6, 2020), https://www.ftc.gov/business-guidance/blog/2020/01/new-and-improved-ftc-data-security-orders-better-guidance-companies-better-protection-consumers.
[971] *See* Hoofnagle, *supra* note 967, at 58–64.
[972] Decision and Order at Part VI(D)(5), *In re Chegg,* FTC File No. 2023151 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Decision-and-Order.pdf.

Technical tests are important, as assessors can claim to have conducted independent "inquiry tests" which again constitute merely documenting assertions of staff.[973] Companies themselves may not understand how their systems work,[974] meaning their assertions are inherently less meaningful than actual technical testing. After a data breach, the regulated company should be subject to scrutiny for what it "actually does" not merely what it "is *supposed* [to do] to safeguard data."

Requiring input from external stakeholders (or alternatively permitting employees to provide input anonymously[975]) and subjecting the final product to public scrutiny allows for "technologists, academics, and plaintiff lawyers"[976] to help identify deficiencies, leveraging a greater pool of resources than the regulator would otherwise have access to. In the context of cybersecurity, there must be a balance between extremes: this requirement should not result in giving bad actors a roadmap to a company's system, but on the other hand it should not fall short of the transparency needed to elicit meaningful input.

If the Commission is to focus on protecting individual consumers rather than build additional scaffolding for the symbolic structure of compliance architecture,[977] it must require that data security assessments be conducted by independent third parties and rely on technical testing, entail audit-like standards, and allow for input from external stakeholders during the process and from the public after the results are published.

When a company allows customer data to be breached, that is evidence that they engaged in inadequate data security practices; this presumption is a

---

[973] Gray *supra* note 714, at 11; Hoofnagle, *supra* note 967, at 3. For instance, a company can claim that its scripts do not "respawn" cookies, and the assessor is permitted to accept that representation as true without further investigation.
[974] *See* Hamilton, *supra* note 915; *Data Security at Risk*, *supra* note 865.
[975] *See Data Security at Risk*, *supra* note 865; *see also* Hoofnagle, *supra* note 967, at 8. ("If asked, privacy advocates, competitors, and even newspaper reporters might have raised some of Google's troubling privacy practices and public gaffes. Competitors and whistleblowers are a major source of tips about privacy wrongdoing.")
[976] Hoofnagle, *supra* note 967, at 9.
[977] Waldman, *supra* note 331, at 810 ("That is, if we understand privacy law in managerial terms—as focused on managing corporate risk, balancing regulation and profit, and enhancing innovation—instead of protecting individuals, we tend to see merely symbolic structures developed in line with those terms as constituting compliance with the law.").

necessary deterrent to prevent further externalization of data security costs onto consumers through poor data security practices.[978] Although businesses may claim that they were the victims of sophisticated attackers,[979] if the business collects consumer data, it has taken on the responsibility of protecting that data, and it is liable when data in its custody is breached. Insurance can help to mitigate the cost of such data security protocol failures, which in turn will limit the impact on cost to consumers.[980]

Consumers should not bear the brunt of the costs of unauthorized disclosure, no matter how diligent the breached company may have been. A company is in control of what data it chooses to collect, how long it chooses to retain it, and when and how it decides to dispose of the data. A company is in control of what processes it uses to safeguard that data, including mitigating the harm in the event of a breach (e.g., segmenting systems). If a company collects consumer data, it accepts liability for what happens to that data until that data has been safely disposed of. This may drive up the cost of compliance with a data security trade rule, but insurance for cyber incidents can serve as a buffer to reduce how much of those costs are passed on to consumers. Cyber insurance may itself also encourage better cyber security

---

[978] *See, e.g.*, Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. Cal. L. Rev. 241, 277–96 (2007) (arguing courts should adopt a strict liability standard with regard to data breaches).

[979] *See, e.g.*, Microsoft Security Response Center, *Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server* (Sept. 29, 2022), https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/.

[980] Josephine Wolf, *Time for Regulators to Take Cyber Insurance Seriously*, Lawfare (Mar. 17, 2020), https://www.lawfareblog.com/time-regulators-take-cyber-insurance-seriously ("Organizations increasingly rely on cyber insurance to help manage online risks. It is time for regulators to stop treating this market as a small, peripheral piece of the insurance industry and instead focus their attention on how they can help transform it into a more stable and effective tool for cybersecurity risk management."); *Cyber Insurance*, FTC https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance (last visited Nov. 21, 2022) ("Cyber insurance is one option that can help protect your business against losses resulting from a cyber attack…. Also, consider whether your cyber insurance provider will: Defend you in a lawsuit or regulatory investigation (look for "duty to defend" wording)."). But insurance companies may need more information. *See, e.g.*, Cyberspace Solarium Comm'n, *Final Report* 79 (2020), https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view (recommendation 4.4).

practices by companies.[981] For example, an IAPP survey of three cybersecurity insurance providers revealed common expectations of best practices, including firewalls, patching, passwords, and authentication, and noted that they may deny coverage if policyholders "do not exercise the degree of caution they promised in the underwriting process."[982]

The U.S. Department of the Treasury recently noted the important risk-transfer function of cyber insurance; that insurance can play an important role in strengthening cyber hygiene and cybersecurity resiliency; and that the industry is growing, with more than $4 billion in direct premiums written in 2020.[983] The Cybersecurity & Infrastructure Agency (CISA) notes that over the first half of 2018 the overall cyber insurance take-up rate was approximately 32%, with 75% of largest companies in key sectors purchasing some cyber insurance and fewer than 5% of small and medium businesses participating.[984] Although the industry is still comparatively young, it is growing quickly. And with good reason—in addition to

---

[981] U.S. Gov't Accountability Off., GAO-22-104256, *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks* 18–19 (2022), https://www.gao.gov/assets/gao-22-104256.pdf ("In addition to covering costs associated with common risks, cyber insurance can encourage policyholders to manage their cyber risk and increase cyber resilience, according to several government entities and researchers…. Some government entities and researchers also have noted that the insurance market can encourage implementation of cybersecurity best practices by linking premiums with the policyholder's cybersecurity practices," but noting that it may make companies more likely to pay ransomware demands which in turn may encourage more cyber attacks); McGeveran, *supra* note 888, at 1171–72 ("Insurers can and do push their policyholders to adopt practices that reduce the insurer's risk of loss—and simultaneously promote better protection of personal data.")

[982] McGeveran, *supra* note 888, at 1173.

[983] *Potential Federal Insurance Response to Catastrophic Incidents*, 87 Fed. Reg. 59161, 59161–62 (Sept. 29, 2022), https://www.federalregister.gov/documents/2022/09/29/2022-21133/potential-federal-insurance-response-to-catastrophic-cyber-incidents ("Through underwriting and pricing, insurers can encourage or even require policyholders to implement strong cybersecurity standards and controls."); Leslie Scism, *Insurers Creating a Consumer Ratings Service for Cybersecurity Industry*, Wall St. J. (Mar. 26, 2019), https://www.wsj.com/articles/insurers-creating-a-consumer-ratings-service-for-cybersecurity-industry-11553592600 ("Many insurers see the burgeoning cyber-risk market as a rare growth opportunity when many other insurance lines are growing sluggishly."); Internet Society's Online Trust Alliance *supra* note 858, at 7 (noting that cyberinsurance market is showing signs of maturing).

[984] CISA, *Assessment of the Cyber Insurance Market* 5 (Dec. 21, 2018), https://www.cisa.gov/sites/default/files/publications/20_0210_cisa_oce_cyber_insurance_market_assessment.pdf ("Aon Inpoint estimates that while 75 percent of financial institutions, retail, health care, and hospitality companies with revenue over $1 billion purchase some cyber insurance, fewer than 5 percent of small and medium businesses are consumers in the market.").

data breaches in which privacy is violated and ransomware in which data or systems are made inaccessible, there are also the threats of leveraging devices to cause harm to other systems.[985] Companies are in the best position to protect consumers from these harms, and the insurance industry is catching up to the market scale that is needed, but companies must be adequately incentivized if the Commission's data security trade rule is going to change data security practices market-wide. While state data breach laws have been much maligned for the alleged patchwork they were said to create, it cannot be denied that they have incentivized companies to report cyber incidents to impacted consumers and regulators more effectively than the absence of such laws.[986]

It is important to note that incident response is only one aspect of data security.[987] Although incident response is an important component of a reasonable data security regime, the Commission's data security trade rule should go beyond breach notification[988] and anticipated Commission responses when a breach has occurred.[989] As Profs. Solove and Hartzog have argued:

> viewing data security policy primarily as a collection of requirements for breach notifications and technical controls excludes many of the most important issues from security, and it silos privacy and security in ways that are unproductive.[990]

This is especially true in light of the priority the Securities and Exchange Commission has placed on incident/vulnerability reporting and on describing the

---

[985] *See, e.g.*,Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, 50 U. Mich. J.L. Reform 913 (Apr. 20, 2017) (describing how a botnet comprised of inadequately secured IoT devices was used to cause a Denial of Service attack in 2016, and articulating a theory of products liability for manufacturers of hacked devices, especially as these attacks have become highly foreseeable).
[986] McGeveran, *supra* note 888, at 1152 (noting breach notification requirements have driven "a large proportion of corporate efforts to improve institutional data security").
[987] *Cyber Essentials Toolkits*, CISA, https://www.cisa.gov/publication/cyber-essentials-toolkits (last visited Nov. 18, 2022) (crisis response is just 1 of 6 aspects of essentials).
[988] *See, e.g.*, *Breach Notification Laws*, Nat'l Conf. of State Legislators (Jan. 17, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[989] *See, e.g.*, Smith, *supra* note 970.
[990] *See* Solove & Hartzog, *supra* note 912, at 132–33.

company's cybersecurity risk assessment policy, if one exists.[991] It falls to the Commission to address the important overlap between privacy and security.

Other sectors have solved this problem—credit card companies have strong anti-fraud protections because they bear the financial risk of fraud losses suffered by consumers. The Fair Credit Billing Act (FCBA) precludes a credit card issuer from imposing liability on a customer (business or consumer) for unauthorized use of a credit card, except in narrowly defined circumstances.[992] As EPIC & the National Consumer Law Center have noted:

> As a result, the banking industry has developed a robust set of protections governing the use of credit cards to minimize their own losses from theft, fraud and even user negligence. The banks control the system, imposing on merchants their requirements to protect against losses . . . . The banks—who will bear the burden of failure—have every incentive to develop vigorous procedures to limit these losses. The security procedures used by banks to monitor and avoid losses is constantly changing, to combat new threats.[993]

Similarly, liability has led to significant improvements in auto safety over the last five decades in large part due to internalization of the previously externalized costs to drivers.[994] Because there is no federal law providing similar protections and incentives to safeguard and promote consumer data security,[995] regulatory action is

---

[991] Press Release, Sec. Exch. Comm'n, *SEC Proposes Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies* (Mar. 9, 2022), https://www.sec.gov/news/press-release/2022-39.

[992] 15 U.S.C. § 1643.

[993] *See, e.g.*, EPIC & Nat'l Consumer L. Ctr., Comments on Fifth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, *In re Advanced Methods to Target & Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, at 11 (Aug. 17, 2022), https://www.fcc.gov/ecfs/document/10817350228611/1.

[994] Kende, *supra* note 860 ("Controlling for millions of vehicle miles traveled, there were almost five times as many fatalities in 1965 as in 2015."); *id.* ("[Liability] provides an incentive, even after the tests [e.g. safety ratings], to ensure that quality is maintained and defects are promptly reported and repaired. This is the shift that must take place for cybersecurity.").

[995] Notwithstanding regulations regarding breach reporting and incident response, which are distinct from security measures designed to prevent breaches in the first place. *See, e.g.*, SEC, *supra* note 991; CISA, *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, https://www.cisa.gov/circia (last visited Nov. 18, 2022).

required now. As renowned security technologist and fellow at Harvard Kennedy School Bruce Schneier recently noted in the New York Times:

> In all of these cases, the victimized organizations could have very likely protected our data better, but the reality is that the market does not reward healthy security. Often customers aren't even able to abandon companies with poor security practices, as many of them build "digital moats" to lock their users in. Customers don't abandon companies with poor security practices. Hits to the stock prices quickly recover. It's a classic market failure of a powerful few taking advantage of the many, and that failure is one that only representation through regulation can fix.[996]

Two professors at Antonin Scalia Law School have similarly argued, in a recent Michigan Technology Law Review article, that a strict liability regime is likely to be superior to a reasonableness framework due to the failure of firms to internalize the cost and benefits of their data security decisions.[997] They note that the concept of strict liability for data breaches is not novel—Professor Danielle Citron advocated for this more than a decade ago[998]—however the novelty of their approach is "not to expand liability under tort law doctrine, but rather for a federal agency, such as the FTC, to act as the national regulator of data security with broad preemptive effect."[999] They further argue that the firm has incentives to take socially optimal security precautions—which will in turn lead to socially optimal data collection decisions—if a firm internalizes the harm,[1000] and moreover that strict liability would facilitate cyber insurance calibrated to an optimal standard of care.[1001]

The Commission should apply a strict liability standard where sensitive data has been breached. If a company is going to engage in the collection, retention, and responsible disposal of sensitive information of any number of consumers, it must

---

[996] Schneier, *supra* note 860.
[997] *See* Cooper & Kobayashi, *supra* note 863, at 263–64.
[998] *Id.* at 265 (citing Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. Cal. L. Rev. 241 (2007)).
[999] *Id.* (acknowledging Ben-Shahar's examination of public law alternatives to private suits under tort law).
[1000] *Id.* at 287.
[1001] *Id.* at 295.

be held to account for the downstream consumer harms that result from the initial harm of unauthorized access to that sensitive data. For similar reasons, organizations of a larger size or collecting a large amount of data—we suggest meeting either (1) $250 million in annual gross revenue or (2) sensitive covered data of more than 5 million individuals or devices linkable to individuals, per the American Data Privacy and Protection Act[1002]—should also trigger a strict liability standard for consumer harm.

In all other instances, there should be a rebuttable presumption of a violation where a breach has occurred. Demonstrating compliance with reasonable data security practices, such as those articulated above, would certainly be relevant to rebutting this presumption.

7. Dark Patterns & Digital Deception

7.1. It is an unfair practice for a business to use manipulative design or dark patterns to nudge consumers to "accept" terms or options that broaden the scope of personal data that the business collects, uses, or discloses.

Responsive to question 13.

As commerce has moved online, so have deceptive tactics, and they have become even more sophisticated and difficult for consumers to navigate given the control that companies have over the interfaces through which consumers access goods and services. The Commission has described dark patterns as "design practices that trick or manipulate users into making choices that they would not otherwise have made and that may cause harm."[1003] These practices are especially harmful in the data protection context. Companies have pushed for decades to frame data collection and processing as an issue of consumer "choice" while deploying manipulative choice architecture to ensure that consumers always "choose" to permit more data collection, broader purposes, and loose or non-existent data sale or transfer restrictions. These practices have become even more

[1002] ADPPA § 2(17).
[1003] FTC Dark Patterns Report *supra* note 130, at 2.

powerful as companies operating online can more easily experiment to find the most effective ways to trick consumers.[1004]

Dark patterns are prevalent, harmful practices that undermine a consumer's autonomy and manipulate them to their detriment. These unfair and deceptive design patterns substantially injure consumers, are not reasonably avoidable, and provide no countervailing benefits to consumers or competition. As the Commission explained in its recent staff report, businesses have relied for decades on manipulative design tactics to "get consumers to part with their money or data."[1005] The Commission has already taken steps to address this through its workshop,[1006] enforcement actions,[1007] its report,[1008] and the issuance of a new enforcement policy statement.[1009] Now the Commission should build on that work further by establishing a trade regulation rule against manipulative designs within the scope of its commercial surveillance rulemaking.

[1004] *Id.* at 2.
[1005] FTC Dark Patterns Report, *supra* note 130, at 1.
[1006] *See* Press Release, FTC, *Bringing Dark Patterns to Light: An FTC Workshop* (Apr. 29, 2021), https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop; Transcript of *Bringing Dark Patterns to Light: An FTC Workshop*, FTC (Apr. 29, 2021), https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf [hereinafter FTC Dark Patterns Workshop Transcript].
[1007] *See, e.g.*, *FTC v. Age of Learning, Inc.*, No. 2:20-cv-07996 (C.D. Cal. Sept. 1, 2020); Press Release, FTC, *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; Complaint, *FTC v. Prog Leasing, LLC,* No. 1:20-cv-01668 (N.D. Ga. Apr. 20, 2020); Press Release, FTC, *Rent-to-Own Payment Plan Company Progressive Leasing Will Pay $175 Million to Settle FTC Charges It Deceived Consumers About Pricing* (Apr. 20, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/04/rent-own-payment-plan-company-progressive-leasing-will-pay-175-million-settle-ftc-charges-it; *FTC v. LendingClub Corp.*, No. 3:18-cv-02454 (N.D. Cal. July 14, 2021); Press Release, FTC, *LendingClub Agrees to Pay $18 Million to Settle FTC Charges* (July 14, 2021), https://www.ftc.gov/news-events/press-releases/2021/07/lendingclub-agrees-pay-18-million-settle-ftc-charges; *FTC v. AH Media Grp.*, No. 3:19-cv-04022-JD (N.D. Cal. May 8, 2020); Press Release, FTC, *FTC Halts Online Subscription Scheme that Deceived People with "Free Trial" Offers* (May 8, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/05/ftc-halts-online-subscription-scheme-deceived-people-free-trial-offers.
[1008] FTC Dark Patterns Report, *supra* note 130.
[1009] Press Release, FTC, *FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions* (Oct. 28, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions.

Dark patterns cause substantial injury to consumers. The Commission has recognized that "use of manipulative design techniques in the digital world can pose heightened risks to consumers."[1010] Indeed, one "pervasive" type of dark pattern "involves design elements that obscure or subvert consumers' privacy choices."[1011] There are many different ways that businesses can design their user interfaces to trick consumers into "agreeing" to broader collection and use of their personal data. The most common harmful methods that are deployed involve interfaces that (1) are not easy to understand, (2) are not symmetrical in choice, (3) use confusing methods, (4) use manipulative language or choice architecture, or (5) are difficult to execute.

These practices are harmful because they rob the consumer of the ability to make choices or express their intention. Dark patterns expose consumers to three primary types of harms: financial harms; privacy harms; and cognitive burdens.[1012] Dark patterns also cause substantial financial injuries to consumers.[1013] As the OECD has explained:

> Dark patterns such as sneak into basket, hidden costs, drip pricing or scarcity cues are clearly aimed at getting consumers to buy something that they may not have needed or to spend more than they may have otherwise intended. Some dark patterns may more indirectly lead consumers to incur financial losses, such as preselection (e.g.[,] a more expensive variant is preselected),

---

[1010] FTC Dark Patterns Report, *supra* note 130, at 2 (first citing FTC Dark Patterns Workshop Transcript, *supra* note 1006, at 34) ("When you move from a brick-and-mortar environment to a digital environment, there's more aspects of the environment you can manipulate . . . you can also collect and leverage information about consumers."); then citing Eur. Comm'n, Directorate-Gen. for Just. & Consumers, *Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation: Final Report* 120 (May 2022), https://data.europa.eu/doi/10.2838/859030 [hereinafter EU Dark Patterns Report] ("Dark patterns and manipulative personalisation practices can lead to financial harm, loss of autonomy and privacy, cognitive burdens, mental harm, as well as pose concerns for collective welfare due to detrimental effects on competition, price transparency and trust in the market.")).

[1011] FTC Dark Patterns Report, *supra* note 130, at 15–16.

[1012] *See* Arunesh Mathur, Jonathan Mayer & Mihir Kshirsagar, *What Makes a Dark Pattern. . . Dark?: Design Attributes, Normative Considerations, and Measurement Methods*, Chi. Conf. on Hum. Factors in Computing Sys., 13–15 (May 2021), https://arxiv.org/pdf/2101.04843.pdf.

[1013] OECD, *Dark Commercial Patterns*, OECD Doc. 336, 24 (2022), https://www.oecd-ilibrary.org/science-and-technology/dark-commercial-patterns_44f5e846-en [hereinafter OECD Dark Patterns Report].

> urgency-related dark patterns (e.g.[,] the consumer is pressured into buying a product they may not have needed), or confirm shaming (e.g.[,] the consumer is shamed into maintaining a subscription they may not need). For dark patterns such as hidden or hard to cancel subscriptions, the unintended financial expenditure may occur on an ongoing basis and could amount to significantly larger losses than those incurred from one-off purchases.[1014]

Dark patterns also drive consumer privacy injuries, in particular the violation of individual autonomy and the exposure of data that consumers believe should remain within their control.[1015] As the OECD has noted, "[b]y hindering consumers' ability to make free and informed choices, dark patterns impair consumer autonomy."[1016] Some examples include default settings that expand the scope of personal data collection, designs that make privacy-protective choices hard to engage with, or designs that shame the consumer into accepting more privacy-intrusive settings.[1017] "As a result, consumers may end up divulging more personal data than intended, potentially exposing them to further risks."[1018]

Lastly, dark patterns may cause psychological and cognitive harms. Consumers may experience emotional distress, frustration, or feelings of shame and being tricked as a result of dark patterns.[1019] Consumers may also experience cognitive burden due to using more energy or attention.[1020] "Frustration and cognitive burden might result from exploiting consumers' inertia or limited

---

[1014] *Id.*
[1015] *See generally* Helen Nissenbaum et. al, *Online Manipulation: Hidden Influences in a Digital World,* 4 Geo. L. Tech. Rev. 1 (2019), https://ssrn.com/abstract=3306006.
[1016] OECD Dark Patterns Report, *supra* note 1013, at 21; *See* Calo, *supra* note 165, at 1031–34 (describing the ways in which digital market manipulation undermines consumer autonomy by targeting them at their most vulnerable moment); Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'*, 31 Current Issues Psych. 105, 107 (2020) ("At a minimum, the power of design means that our choices do not always reflect our real personal preferences. At worst, online platforms manipulate us into keeping the data flowing, fueling an information-hungry business model.").
[1017] OECD Dark Patterns Report, *supra* note 1013, at 25.
[1018] *Id.*
[1019] *Id.* (citing *Harms of Dark Patterns*, Dark Patterns Tip Line, https://darkpatternstipline.org/harms (last visited Nov. 15, 2022)).
[1020] *Id.* (citing Mathur, Mayer & Kshirsagar, *supra* note 1012, at 15–17).

willpower, attention span or time, for example by repeatedly prompting the consumer to agree to certain settings (nagging), making it harder to cancel than to sign up or to select the appropriate choice (trick questions)."[1021]

The harms caused by dark patterns are note reasonably avoidable by consumers because these systems are designed specifically to manipulate consumers and thwart their ability to make informed choices. These manipulative design patterns are effective precisely because consumers are not able to easily avoid them, as choices the company does not want are buried under confusing language or multiple complex layers of settings. For example, if a consumer wishes to cancel their Amazon prime subscription, she cannot avoid the complex process that the company has put in place to discourage cancelation.[1022] The Commission recently explained that consumers are unaware of such manipulation "[b]ecause dark patterns are covert or otherwise deceptive [and] many consumers don't realize they are being manipulated or misled."[1023] User interfaces that employ dark patterns to "maximize information collection and sharing, such as using default settings to make consumer data collection *difficult to avoid*, even when such collection is unnecessary."[1024] Some dark patterns do not allow consumers to reject data

---

[1021] *Id.*

[1022] *See* Complaint and Request for Investigation, Injunction, and Other Relief, *In re Amazon* (Feb. 23, 2021), https://epic.org/wp-content/uploads/privacy/dccppa/amazon/EPIC-Complaint-In-Re-Amazon.pdf; Forbrukerrådet, *You Can Log Out, but You Can Never Leave: How Amazon Manipulates Consumers to Keep Them Subscribed to Amazon Prime* (Jan. 14, 2021), https://fil.forbrukerradet.no/wp-content/uploads/2021/01/2021-01-14-you-can-log-out-but-you-can-never-leave-final.pdf.

[1023] FTC Dark Patterns Report, *supra* note 130, at 3 (citing Dark Patterns Workshop Transcript, *supra* note 1006, at 73; EU Dark Patterns Report, *supra* note 1010, at 85 ("Dark patterns are hidden, subtle and manipulative in nature, so it is difficult to spot and report them."); U.K. Competition & Mkts. Auth., *Online Choice Architecture: How Digital Design Can Harm Competition and Consumers*, Discussion Paper No. CMA155 42 (Apr. 2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf ("When encountering a harmful OCA practice, such as a dark pattern, most individuals are unlikely to realise they were under the influence of a bias or heuristic that drove their decision making."); Consumer Reps., *Comments to the Federal Trade Commission on Bringing Dark Patterns to Light: An FTC Workshop*, No. FTC-2021-0019-0119 3 (May 29, 2021), https://www.regulations.gov/comment/FTC-2021-0019-0119 ("By their very nature, dark patterns are difficult for consumers to identify.").

[1024] FTC Dark Patterns Report, *supra* note 130, at 16 (emphasis added) (citing Dark Patterns Workshop Transcript, *supra* note 1006, at 32–33, 39); EU Dark Patterns Report, *supra* note 1010, at 60

collection, meaning a consumer could not avoid the collection of their personal information even if they wanted to.[1025] For example:

MANIPULATIVE DESIGN AT WORK

A user visits the website of a pet supply store. A banner appears at the bottom and reads "This site uses cookies for functionality and other purposes. Please click below to learn more about how we use your information." Below this text appears two boxes. One reads "Accept" and the other reads "Learn More Information." The user has no option to reject unnecessary cookies because clicking on the "Learn More Information" button brings her to the website's privacy policy page.

A user visits a popular news site. A cookie banner pops up and covers most of the screen, and the background becomes grayscale, shifting the user's focus to the pop up. The user is presented with two options: a button that says "Accept" in bright blue font and a button that says "Reject" in grayscale, which appears to be an inactive button to the user. The user clicks "Accept" because she believes it is the only available option.

The harms associated with dark patterns are not outweighed by any benefits to competition or consumers because they are manipulative and deceptive practices. The Commission has differentiated between manipulative designs and permissible persuasive designs, which may provide some benefits. Designs are dark patterns "if used to deceive consumers or manipulate them into taking unwitting or detrimental actions[.]"[1026] When a design feature rises to the

("Overall, an important concern for mystery shoppers was not knowing for sure how the websites/apps used their personal data, and with which other companies they would share it. They noted that some websites/apps were asking them for a lot more personal data than what was considered useful for the functioning of the service (e.g., gender, birthdate, astrological sign, etc.)."); DuckDuckGo, *Comments to the Federal Trade Commission on Bringing Dark Patterns to Light: An FTC Workshop*, No. FTC-2021-0019-0103 3 (May 26, 2021), https://www.regulations.gov/comment/FTC-2021-0019-0103; Campaign for a Commercial-Free Childhood & Ctr. for Digit. Democracy, *Comments to the Federal Trade Commission on Bringing Dark Patterns to Light: An FTC Workshop*, No. FTC-2021-0019-0108 18 (May 28, 2021), https://www.regulations.gov/comment/FTC-2021-0019-0108).

[1025] FTC Dark Patterns Report, *supra* note 130130, at 16 ("The [ISP privacy practices] Staff Report explained how such an interface may indicate to consumers that they have no choice but to select 'Accept,' or might lead consumers to select 'Accept' out of expediency without realizing their ability to 'Reject' due to the difference in prominence of the two choices. Second, the Report highlighted interfaces that do not allow consumers to reject data collection or that continuously prompt consumers if they select a disfavored setting.").

[1026] FTC Dark Patterns Report, *supra* note 130, at 2.

level of manipulating the consumer to their detriment, its harms are not outweighed by any benefit to competition or consumers. In contrast, persuasive design features that do not subvert consumer choice, expose data the consumer meant to keep private, increase the cognitive burden on the consumer, or manipulate the consumer in similar fashion are permissible because they do not harm consumers. Industry has failed to demonstrate how manipulating consumers provides the consumer with any benefits. Deceptive design is also anticompetitive because the large companies that can afford to pay fines from regulatory enforcement are unjustly enriched from employing such unfair and deceptive practices. Moreover, smaller companies and companies who do not engage in such harmful practices would benefit from an industry-wide rule prohibiting manipulative dark patterns. Only businesses that engage in these harmful practices will need to change their practices. A uniform rule will promote compliance and provide businesses with clear guidance. Dark patterns do not provide any benefits to consumers or competition that outweigh the substantial harms they impose consumers, and consumers cannot reasonably avoid them. Therefore, dark patterns are an unfair practice.

The employment of dark patterns is widespread and prevalent, as the Commission has seen in its studies and workshops.[1027] Reporters feel confident declaring that "[d]ark patterns are everywhere[.]"[1028] One study found the use of dark patterns has grown increasingly common on digital platforms such as social media, shopping sites, mobile apps, and video games.[1029] The study "discovered 1,818 instances of dark patterns from 1,254 (~11.1%) websites in [its] data set of 11K shopping websites."[1030] The person who coined the term "dark pattern" has explained why they are so prevalent:

> Lots of companies will make it hard for people to leave,' says Brignull. 'They are going to get around to it eventually, but if they might stay for

[1027] *Id.* at 1.
[1028] Erin Ravenscraft, *How to Spot – and Avoid – Dark Patterns on the Web*, Wired (July 29, 2020), https://www.wired.com/story/how-to-spot-avoid-dark-patterns/.
[1029] Arunesh Mather et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 Proc. ACM Hum.-Comput. Interact., *1 (Sept. 2019).
[1030] *Id.* at *2 ("Shopping websites that were more popular, according to Alexa rankings, were more likely to feature dark patterns. These numbers represent a lower bound on the total number of dark patterns on these websites, since our automated approach only examined text-based user interfaces on a sample of product pages per website.").

> an extra 10 percent of the time, or 20 percent, the accounts might live just a little bit longer. And if you're doing that en masse for hundreds of thousands of people, that translates to enormous amounts of money, for people who are going to leave anyway.[1031]

Research supports the conclusion that dark patterns are prevalent.[1032] Eighty percent of popular apps for children contain at least one manipulative design feature.[1033] Out of a sample of 240 popular apps, 95% contained at least one dark pattern.[1034] Of the 200 most popular online retailers in the U.S., all contained at least four instances of "impulse buying features."[1035]

Because dark patterns are a widespread, prevalent, and unfair practice, the Commission should promulgate a rule that gives its previous warnings[1036] teeth. The Commission has recognized that dark patterns harm consumers, has taken enforcement actions in individual cases before, and should use this rulemaking as an opportunity to establish a rule that will prevent manipulative dark patterns

---

[1031] Ravenscraft, *supra* note 1028.
[1032] *See* OECD Dark Patterns Report, *supra* note 1013.
[1033] Jenny Radesky et al., *Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children*, 5(6) JAMA Network Open (June 17, 2022), https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2793493.
[1034] Linda Di Geronimo et al., *UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception*, CHI '20: Proc. 2020 CHI Conf. Hum. Factors Computing Sys. (Apr. 2020), https://doi.org/10.1145/3313831.3376600.
[1035] Carol Moser et al., *Impulse Buying: Design Practices and Consumer Needs*, CHI '19: Proc. CHI Conf. Hum. Factors Computing Sys. 4 (May 2019), https://doi.org/10.1145/3290605.3300472.
[1036] FTC Dark Patterns Report, *supra* note 130, at 18 ("In addition to generally minimizing data collection efforts, businesses should also avoid subverting consumers' privacy choices. First, companies should avoid default settings that lead to the collection, use, or disclosure of consumers' information in a way that they did not expect (and collect information only when the business has a justified need for collecting the data). Second, companies should make consumer choices easy to access and understand. Consumers should not have to navigate through multiple screens to find privacy settings or have to look for settings buried in a privacy policy or in a company's terms of service: they should be presented at a time and in a context in which the consumer is making a decision about their data. Any toggle options presented to the consumer should not be ambiguous or confusing, and one option should not be more prominent than another. Third, choices about sensitive information, in particular, should be presented so that it is clear to the consumer what they are consenting to—as opposed to a blanket consent—and should be presented along with information that they need to make an informed decision (for example, that if the consumer consents to the collection of their information, that information will be shared with third parties). More generally, businesses should take a moment to assess their user interfaces from a consumer's perspective and consider whether another option might increase the likelihood that a consumer's choice will be respected and implemented.").

industry wide. The Commission's dark patterns rule should embody existing best practices on choice architecture, which dictate that systems seeking to obtain user input on the scope of data collection and processing should: (1) be easy to understand; (2) exhibit symmetry in choice; (3) avoid language or interactive elements that are confusing to the consumer (the methods should not use double negatives, and toggles or buttons must clearly indicate the consumer's choice); (4) avoid manipulative language or choice architecture (the methods should not use language or wording that guilts or shames the consumer into making a particular choice or bundles consent to subvert the consumer's choice); and (5) be easy to execute.[1037] The Commission should similarly establish guidelines to determine what is lawful persuasive conduct and declare any nudging practice that does not meet those guidelines to be an unfair manipulative design.

CONCLUSION

For more than twenty years, the United States has failed to rise to the challenge posed by evolving commercial surveillance practices and deficient data security. We cannot wait another decade to pull ourselves out of this deepening data privacy crisis. The time is now for the Federal Trade Commission to protect consumers and enact a trade regulation rule that will promote data minimization; establish fairness and transparency for automated decision-making systems; address systemic discrimination online; ensure that businesses meet their notice and transparency obligations; safeguard the privacy of minors; enforce data security standards; and prohibit manipulative designs that thwart consumer choice. EPIC looks forward to the Commission's proposed rule addressing these urgent matters, and we stand ready to assist the Commission however we can in the rulemaking process.

[1037] *See* Cal. Privacy Prot. Agency, Text of Proposed Regulations, Art. 1 § 7004 (2022), https://cppa.ca.gov/meetings/materials/20220608_item3.pdf.

APPENDIX 1: PROPOSED UNFAIRNESS STATEMENTS

1. **Data Minimization**

   1.1. It is an unfair trade practice to collect, use, transfer, or retain personal data beyond what is reasonably necessary and proportionate to the primary purpose for which it was collected, consistent with consumer expectations and the context in which the data was collected.

2. **Automated Decision-Making Systems**

   2.1. It is an unfair and deceptive practice to use an automated decision-making system implicating the interests of consumers without first demonstrating that it is effective, accurate, and free from impermissible bias.

   2.2. It is an unfair and deceptive practice to use an automated decision-making system implicating the interests of consumers without providing adequate notice of such use, which includes meaningful, readable, and understandable disclosure of the logic, factors, inputs, and training data on which such system relies.

   2.3. It is an unfair practice to use one-to-many facial recognition, emotion recognition, or other biometric technologies for commercial surveillance.

3. **Discrimination**

   3.1. It is an unfair practice to discriminate in or otherwise make unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, sexual orientation, disability, or other protected characteristics.

4. **Notice & Transparency**

   4.1. It is an unfair and deceptive practice to collect, use, retain, or transfer personal data without first assessing, justifying, and providing adequate notice of such collection, use, retention, or transfer.

5. Privacy of Minors

5.1. It is an unfair practice to collect, process, retain, or transfer the personal data of minors under the age of 18 unless strictly necessary to achieve the minor's specific purpose for interacting with the business or to achieve certain essential purposes.

5.2. It is an unfair and deceptive practice to make intentional design choices in order to facilitate the commercial surveillance of minors.

6. Data Security

6.1. It is an unfair and deceptive practice to collect, process, retain, or transfer personal data without maintaining reasonable administrative, technical, and physical measures to secure such data against unauthorized access.

7. Dark Patterns and Deceptive Design

7.1. It is an unfair practice for a business to use manipulative design or dark patterns to nudge consumers to "accept" terms or options that broaden the scope of personal data that the business collects, uses, or discloses.

APPENDIX 2: ANPR QUESTIONS ADDRESSED

Ques.	Section
1	Introductory Material
3	Introductory Material, 5. Privacy of Minors
4	Introductory Material, 5. Privacy of Minors
5	Introductory Material, 5. Privacy of Minors
6	Introductory Material
7	Introductory Material
8	Introductory Material, 5. Privacy of Minors
9	Introductory Material
10	Introductory Material, 5. Privacy of Minors, 6. Data Security
11	Introductory Material, 6. Data Security
12	Introductory Material, 5. Privacy of Minors, 6. Data Security
13	5. Privacy of Minors, 6. Data Security, 7. Digital Deception
14	5. Privacy of Minors
15	5. Privacy of Minors
17	5. Privacy of Minors
19	5. Privacy of Minors
20	5. Privacy of Minors
21	5. Privacy of Minors
22	5. Privacy of Minors
24	Introductory Material
25	Introductory Material
26	1. Data Minimization
27	1. Data Minimization
28	5. Privacy of Minors
29	Introductory Material, 1. Data Minimization
30	6. Data Security
31	6. Data Security
32	6. Data Security
35	6. Data Security
36	6. Data Security
37	2. Automated Decision-Making Systems
38	2. Automated Decision-Making Systems
40	1. Data Minimization, 2. Automated Decision-Making Systems
41	1. Data Minimization
43	1. Data Minimization
44	1. Data Minimization
45	1. Data Minimization

46	1. Data Minimization
47	1. Data Minimization, 2. Automated Decision-Making Systems, 6. Data Security
48	2. Automated Decision-Making Systems
53	2. Automated Decision-Making Systems
54	2. Automated Decision-Making Systems
55	2. Automated Decision-Making Systems
56	2. Automated Decision-Making Systems
57	2. Automated Decision-Making Systems
58	2. Automated Decision-Making Systems
59	2. Automated Decision-Making Systems
60	2. Automated Decision-Making Systems
61	2. Automated Decision-Making Systems
62	2. Automated Decision-Making Systems
63	2. Automated Decision-Making Systems
64	2. Automated Decision-Making Systems
65	2. Automated Decision-Making Systems, 3. Discrimination
66	3. Discrimination
67	3. Discrimination
68	2. Automated Decision-Making Systems, 3. Discrimination
69	3. Discrimination
70	2. Automated Decision-Making Systems, 3. Discrimination
71	3. Discrimination
72	3. Discrimination
73	4. Notice & Transparency
74	4. Notice & Transparency
75	5. Privacy of Minors
76	Introductory Material, 5. Privacy of Minors, passim
77	Introductory Material, passim
79	5. Privacy of Minors
83	4. Notice & Transparency
84	2. Automated Decision-Making Systems, 4. Notice & Transparency
85	4. Notice & Transparency
86	1. Data Minimization, 2. Automated Decision-Making Systems
87	2. Automated Decision-Making Systems
89	2. Automated Decision-Making Systems, 4. Notice & Transparency
90	2. Automated Decision-Making Systems, 4. Notice & Transparency
91	2. Automated Decision-Making Systems, 4. Notice & Transparency
92	4. Notice & Transparency
95	Introductory Material