Before the
Federal Trade Commission
Washington, DC 20580

In the Matter of	)	
	)	
	)	
Commercial Surveillance ANPR R11004	)	Docket FTC-2022-0053
	)	
	)	
	)	
	)	
	)	
	)	
	)	
	)	

Comments of the National Telecommunications and Information Administration Regarding Commercial Surveillance ANPR R11004

Comments of the National Telecommunications and Information Administration Regarding Commercial Surveillance ANPR R11004

Executive Summary:

The National Telecommunications and Information Administration (NTIA) strongly supports the Federal Trade Commission (FTC) promulgating rules to improve data security protections and diminish the harmful effects of commercial surveillance. The lack of a strong, unified national approach to privacy is bad for businesses, our standing in international conversations on privacy, and most importantly, the American people. The FTC's role in protecting the public and promoting competition is crucial to a healthy digital economy, and new rules can help ensure its capabilities keep pace with the evolution of new technologies. These rules should eschew consent-dominated privacy governance in favor of data minimization and purpose limitation requirements, and cover the comprehensive range of commercial data practices under the FTC's jurisdiction with heightened protections where appropriate for harms that disproportionately impact vulnerable populations. The FTC's rulemaking proceeding presents a valuable opportunity to implement a strong and cohesive framework of privacy protections that complements efforts at other agencies and in Congress.

NTIA has spent decades identifying how data abuses impact individuals, communities, and the digital economy, and discussing the need for clear rules of the road to diminish the harmful effects of commercial surveillance. In our role as the President's principal advisor on telecommunications and information policy issues, NTIA studies and develops policy on the impact of technology and the Internet on privacy, including the extent to which modern data practices are adequately addressed by the current U.S. privacy protection framework. For example, NTIA helped draft the 2012 "Consumer Privacy Bill of Rights"[1] and the 2014 "Big Data: Seizing Opportunities, Preserving Values" reports,[2] and led the 2018 Consumer Privacy Request for Comment.[3] In December 2021, NTIA convened a series of listening sessions on the intersection of privacy, equity, and civil rights, and will soon issue a Request for Comment on the subject, using the feedback provided through these processes to draft a report.[4]

[1] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy* (Consumer Privacy Bill of Rights), (Feb. 2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.
[2] The White House, *Big Data: Seizing Opportunities, Preserving Values*, (May 2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
[3] National Telecommunications & Information Administration, *Request for Comments on Developing the Administration's Approach to Consumer Privacy*, (Sept. 25, 2018), https://www.ntia.doc.gov/federal-register-notice/2018/request-comments-developing-administration-s-approach-consumer-privacy.
[4] National Telecommunications & Information Administration, *NTIA Virtual Listening Sessions on Personal Data: Privacy, Equity, and Civil Rights*, (Jan. 3, 2022), https://www.ntia.doc.gov/other-publication/2022/ntia-virtual-listening-sessions-personal-data-privacy-equity-and-civil-rights.

The Biden Administration has established its commitment to strengthening privacy protections through numerous public statements and actions,[5] such as Principles for Enhancing Competition and Tech Platform Accountability;[6] the Executive Order on Promoting Competition in the American Economy;[7] and the Executive Order on Protecting Access to Reproductive Healthcare Services.[8] These statements and actions highlight Biden administration objectives like "provid[ing] robust federal protections for Americans' privacy" that "put the burden on platforms to minimize how much information they collect, rather than burdening Americans with reading fine print;"[9] protecting children and young people by "restricting excessive data collection and targeted advertising [to them]" as they are "especially vulnerable to harm";[10] and enacting "strong protections to ensure algorithms do not discriminate against protected groups," including "through persistent surveillance."[11] All of these priorities would be supported by the FTC adopting comprehensive rules that reject consent-dominated approaches in favor of data purpose limitations and minimization requirements and heightened protections for harms that disproportionately impact vulnerable populations.

The significant presence of potential federal legislation in consumer privacy reform discussions does not obviate the importance of the FTC's efforts to adopt strong, comprehensive rules governing commercial surveillance and data security. NTIA strongly supports the Commission's rulemaking process and considers the Commission's work—enforcing existing statutes and rules, investigating concerning commercial practices, updating current regulations, and promulgating new ones—to be essential. Simultaneously, NTIA strongly supports comprehensive, federal privacy legislation that would create new protections for the public and baseline requirements for

---

[5] The White House, *Remarks by President Biden on Protecting Access to Reproductive Health Care Services*, (July 8, 2022), https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/07/08/remarks-by-president-biden-on-protecting-access-to-reproductive-health-care-services ("The choice we face as a nation is between the mainstream and the extreme, between moving forward and moving backwards, between allowing politicians to enter the most personal parts of our lives and **protecting the right to privacy…embedded in our Constitution**.") (emphasis added).

[6] The White House, *Readout of White House Listening Session on Tech Platform Accountability*, (Sept. 8, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/08/readout-of-white-house-listening-session-on-tech-platform-accountability.

[7] Exec. Order No. 14,036, 86 Fed. Reg. 36,987, 36,992 (July 9, 2021), https://www.govinfo.gov/content/pkg/FR-2021-07-14/pdf/2021-15069.pdf ("[T]o address persistent and recurrent practices that inhibit competition, the Chair of the FTC, in the Chair's discretion, is also encouraged to consider working with the rest of the Commission to exercise the FTC's statutory rulemaking authority, as appropriate and consistent with applicable law, in areas such as unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy").

[8] Exec. Order No. 14,076, 87 Fed. Reg. 42,053 (July 8, 2022), https://www.govinfo.gov/content/pkg/FR-2022-07-13/pdf/2022-15138.pdf.

[9] The White House, *Readout of White House Listening Session on Tech Platform Accountability*, *supra* n. 6.

[10] *Id.*

[11] *Id.*; *see also* Exec. Order No. 13,985, 86 Fed. Reg. 7009 (Jan. 20, 2021), https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01753.pdf; The White House, *The Biden-Harris Administration Immediate Priorities*, https://www.whitehouse.gov/priorities (citing racial equity as one of seven "immediate administration priorities").

businesses and cement protections and requirements that already exist.[12] Ongoing efforts by the FTC and by Congress to protect privacy and increase competition are as complementary as they are crucial.

The FTC's role in protecting consumers and promoting competition is essential to a healthy digital economy, and rules can help ensure that the agency's capabilities keep pace with the emergence of new technologies and business models. The evolution of new technical capabilities and the legal challenges that the FTC describes in its notice have also strengthened the value of clear baseline rules for businesses and consumers. The FTC is uniquely positioned to develop these rules because of its subject-matter expertise from decades of law enforcement actions and policy explorations, as well as its broad authority over commerce.

NTIA recommends that the following principles guide those rules:

1. The FTC should abandon the "notice and choice" model as the primary privacy safeguard.[13]

- The complexities and pace of today's digital world long ago outpaced what notice and transparency can accomplish as a predominant focus of privacy policy, and they cannot be the primary bulwark against invasive or unfair data practices. Under a notice-and-choice dominated governance system, businesses have been given wide latitude to determine what kinds of collection and use practices are appropriate or fair, and have often used that latitude to prioritize profits over privacy or safety. The inability of individuals to meaningfully protect themselves has created an extractive data economy in need of better guardrails.
- A consent-dominated approach to consumer privacy has left the public vulnerable to exploitative data practices. Privacy and consumer protection experts have demonstrated for more than two decades that notice and choice mechanisms do not actually provide individuals with meaningful agency, nor act as a check on abuse.[14]
- The complexities of the data ecosystem and accompanying challenges of describing data practices in accurate, yet digestible forms; human tendencies to misinterpret the risks; and the

[12] *See, e.g.*, Alan Davidson*, NTIA Administrator and Assistant Secretary for Communications and Information for the U.S. Department of Commerce,* Fireside Chat, Internet Governance Forum USA, (July 21, 2022), https://livestream.com/accounts/686369/events/10538464/videos/232196813 ("[A] national comprehensive privacy law would benefit American consumers and it would benefit American business. And, you know, we're ready for it. And I think … it would benefit our leadership around the world.")*; see also* Teralyn Whipple, *NTIA Head Says Agency Supports National Data Privacy Law*, Broadband Breakfast (July 21, 2022), https://broadbandbreakfast.com/2022/07/ntia-head-says-agency-supports-national-data-privacy-law.

[13] Addressed in NTIA's answers to FTC questions 6, 14, 43, 73, and 79.

[14] Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 J.L. & POL'Y INFO. SOC'Y 543 (2008); Julie Cohen, *Turning Privacy Inside Out*, Theoretical Inquiries in Law 20.1 1-22, 4 (2019) ("The first and most important reason for failure is that notice-and-consent protections, which function as the principal regulatory tool in the U.S. system and as an increasingly important backstop in the European system, simply do not work"); Woodrow Hartzog & Neil Richards, *The Pathologies of Digital Consent*, 96 Washington University Law Review 1461 n.3 (2019) (citing a long list of scholarly critiques); Remarks of Commissioner Rebecca Kelly Slaughter, *Wait But Why? Rethinking Assumptions About Surveillance Advertising IAPP Privacy Security Risk Closing Keynote 2021,* 4-6 (Oct. 22, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597998/iapp_psr_2021_102221_final2.pdf.

sheer volume of consumer technologies each of us encounters every day fundamentally undermine the operative logic of notice and choice. What's more, the information provided by a privacy policy might not have actionable consequences, as a given transaction may be unavoidable or an alternative may not exist.

- At the same time, transparency and notice are still important components of consumer privacy policy. Transparency can serve important policy functions beyond privacy self-help, such as the insight it can provide into corporate practices for consumer watchdogs and regulators.
- Rules that abandon consent as a primary privacy safeguard supports the Biden Administration's goal to "provide robust federal protections for Americans' privacy" that "put the burden on platforms to minimize how much information they collect, rather than burdening Americans with reading fine print."[15]

2. The FTC's rules should shift the burden of assessing and mitigating privacy risks from individuals to businesses, particularly through significant data purpose limitations.[16]

- The FTC should create limits on corporate conduct that shift the burden of privacy risk management from individuals to businesses, which would help shift undesirable incentives and promote a more trustworthy data economy. Rules governing data collection and use by private companies should include data minimization requirements, purpose limitations, retention limitations, risk management, security requirements, and deletion requirements to mitigate data harms. These measures are a necessary corrective to an exploitative status quo enabled by a consent-centric paradigm.
- Requirements that establish safer data collection and use practices help prevent privacy invasions and misuses of data before they occur. When a company minimizes the data it collects (or ensures data is appropriately deleted), it reduces the possibility of revealing information against the wishes of the data subject, and reduces targets for cyber-attacks from bad actors seeking access to valuable information. Purpose limitations, deletion requirements, and retention limitations also diminish the likelihood that data collected in one context will be inappropriately repurposed, such as information collected for security purposes being used for targeted advertising.
- Companies benefit from purpose limitations, retention limitations, minimization requirements, and deletion requirements for consumer data. Minimizing the collection of data that is not strictly necessary to provide requested services or make a service run effectively and safely diminishes the risk of public relations concerns, legal liabilities, and ensuing losses in corporate value that result from data breaches and other unauthorized or privacy-invasive uses of data.

[15] The White House, *Readout of White House Listening Session on Tech Platform Accountability*, *supra* n. 6.
[16] Addressed in NTIA's answers to questions 6, 14, 43, 73, & 79.

- The FTC should also address data security issues in this rulemaking, as clear, strong security requirements reinforce the effects of data purpose limitations and minimization requirements, and the privacy of data is meaningless if that data is not secure.
- Further, companies should be required to assess and mitigate the risks of their data collection practices such that harms are identified and mitigated before the data that is collected and processed.
- Rules that would shift the burden of mitigating privacy risks from individuals to businesses, particularly though data purpose limitations and data minimization requirements, would support the Biden Administration's statement that "[t]here should be clear limits on the ability to collect, use, transfer, and maintain our personal data."[17]

3. The FTC's rules should regulate data on a comprehensive basis, with heightened protections for particular contexts or practices where appropriate, including for data abuses more frequently or severely experienced by vulnerable populations.[18]

- Trade regulation rules constraining commercial surveillance practices should provide comprehensive limitations and protections, with heightened protections for particularly vulnerable groups or concerning practices where appropriate. A comprehensive approach—with heightened protections where warranted by context-driven considerations of societally undesirable risks—diminishes the possibility of creating an insufficient and inconsistent privacy regime that adapts poorly to inevitable technological change.
- A comprehensive approach minimizes the risk of underinclusive protections. Data that may seem unidentifiable or incapable of revealing sensitive facts about someone could create greater privacy risks in aggregate, as many studies on the increasing ease of re-identifying "anonymized" data have shown.[19] Extending data protections exclusively to specific categories could ignore the privacy risks that occur when data is sold, shared, or used in a new context than the one in which it was initially collected.
- While additional protections for certain categories of data or populations of individuals may be warranted in cases where the risk of underinclusive or insufficient protections are particularly acute, a purely sectoral approach is less capable of adapting to rapid technological shifts, and likely to exclude relevant categories of data or conduct.
- Marginalized communities may experience certain data harms, such as privacy invasions, inaccurate automated assessments, or biased automated assessments, more frequently or severely, and may face particularly significant obstacles to recovery from those harms. Harmful data collection and use practices by companies can also reinforce existing structural biases or augment existing risks to important rights, such as access to reproductive care.

---

[17] The White House, *Readout of White House Listening Session on Tech Platform Accountability*, *supra* n. 6.
[18] Addressed in NTIA's answers to the FTC's questions 10, 12, 14, 28, 30, 57, 60, and 68.
[19] Latanya Sweeney, *Only You, Your Doctor, and Many Others May Know*, Tech Science (Sept. 29, 2015), https://techscience.org/a/2015092903; Luc Rocher et al., *Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models*, 10 Nature Comm's 3069 (2019), https://www.nature.com/articles/s41467-019-10933-3.

- Other individuals may be more vulnerable to such abuses due to shared vulnerabilities to structural abuses of power, such as children and teenagers, older individuals, students, or workers.
- Awareness of the disparate effects of data abuses for different groups and a scrupulous commitment to equity do not undermine the urgent need to enact privacy protections for everyone. But the FTC's rules should be mindful of the particular vulnerabilities created by these power dynamics. This means promulgating rules that increase degrees of oversight and mitigating protocols based on risk given the contexts of use and potential for harm.
- Comprehensive rules with certain heightened protections for vulnerable populations such as marginalized communities and young people would serve a number of administration priorities. The Biden Administration has repeatedly highlighted its commitment to rooting out racism, misogyny, and other structural biases that limit the opportunities of individuals based on who they are, what they believe, or whom they love,[20] including the impact of persistent surveillance on marginalized communities,[21] and the privacy invasions experienced by survivors of online harassment, who are disproportionately women, LGBTQI+ individuals, and people of color.[22] President Biden has also highlighted the particular vulnerability of young people to manipulative practices and privacy invasions, and the imperative of protecting them from predation.[23]

---

[20] Exec. Order No. 13,985, *supra* n. 11 ("It is therefore the policy of my Administration that the Federal Government should pursue a comprehensive approach to advancing equity for all, including people of color and others who have been historically underserved, marginalized, and adversely affected by persistent poverty and inequality."); The White House, *Readout of White House Listening Session on Tech Platform Accountability*, *supra* n. 6 ("**Stop discriminatory algorithmic decision-making**. We need strong protections to ensure algorithms do not discriminate against protected groups, such as by failing to share key opportunities equally, by discriminatorily exposing vulnerable communities to risky products, or through persistent surveillance.") (emphasis in original).

[21] *Id*. ("We need strong protections to ensure algorithms do not discriminate against protected groups, such as… through persistent surveillance.").

[22] The White House, *Remarks by Vice President Harris Announcing the Launch of the White House Task Force to Address Online harassment and Abuse*, (June 16, 2022), https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/06/16/remarks-by-vice-president-harris-announcing-the-launch-of-the-white-house-task-force-to-address-online-harassment-and-abuse ("One in three women under the age of 35 report being sexually harassed online. Over half of the LGBTQ+ people in our country are survivors of severe harassment. Nearly one in four Asian Americans report being called an offensive name, usually motivated by racism — being called an offensive name online. And Black people who have been harassed online in our country are three times more likely to be targeted, again, because of their race… So let us be clear: No one should be afraid that an abuser will use their private personal data — or that a person's private personal data will be used against them. And all people deserve to use the Internet free from fear.").

[23] The White House, *Remarks of President Joe Biden – State of the Union Address as Prepared for Delivery*, (Mar. 1, 2022), https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/03/01/remarks-of-president-joe-biden-state-of-the-union-address-as-delivered ("[W]e must hold social media platforms accountable for the national experiment they're conducting on our children for profit. It's time to strengthen privacy protections, ban targeted advertising to children, demand tech companies stop collecting personal data on our children."); The White House, *Readout of White House Listening Session on Tech Platform Accountability*, *supra* n. 6 ("Protect our kids by putting in place even stronger privacy and online protections for them, including prioritizing safety by design standards and practices for online platforms, products, and services. Children, adolescents, and teens are especially vulnerable to harm. Platforms and other interactive digital service providers should be required to prioritize the safety and

wellbeing of young people above profit and revenue in their product design, including by restricting excessive data collection and targeted advertising to young people.").

Specific Questions Raised in the ANPR:

(a) To What Extent Do Commercial Surveillance Practices or Lax Security Measures Harm Consumers?

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

The enormous complexity of the commercial surveillance ecosystem makes discerning likely privacy risks exceedingly difficult, particularly given the lack of transparency surrounding these practices.[24] These difficulties support shifting the burden of mitigating privacy risks from individuals to the companies that gather, use, and profit from their information.

Many privacy risks attached to commercial surveillance practices are also difficult to identify on an individualized basis, as the aggregate effects of mass collection and unconstrained use practices are often the cause of the harms an individual might ultimately experience. Individualized harms can also be easier to comprehend and address than harms felt by communities, yet group-level inferences can contribute to the wrongful assessment of an individual candidate for an apartment, educational opportunity, or job in part because they are a member of that group.

Behavioral psychologists and privacy experts have constructed a significant body of literature on the ways in which the human brain is poorly positioned to adequately assess privacy risks, as most people struggle to correctly evaluate risks that are remote, abstract, or attenuated,[25] as many privacy risks are. Detecting the harms of using a service with invasive online tracking can require a number of logical steps to identify cause and effect, and the connection between data processing activities and potential harms is rarely obvious or intuitive. For example, some data that may not be deemed traditionally sensitive, such as data on household energy use or consumer shopping habits, can be processed alone or in concert with other data to build granular behavioral profiles and contribute to harmful outcomes, such as discrimination or loss of personal autonomy through psychological manipulation. Causality can be obscured in situations where the harms only occur much later, due to technological developments that enable new insights to be gleaned from the data, or because the initial origin of recovered, compromised data is impossible to trace. In contrast, the immediate benefits of using the product or service will generally be more concrete, more ascertainable, and easier to understand.[26]

Certain privacy harms are also more difficult to trace or understand than others, while being no less injurious or in need of prevention. Most people can readily identify that bodily injury (such as an assault enabled by an assailant's access to their victim's location information)[27] or financial

[24] *Infra* n. 31.
[25] *See generally*, Daniel Solove, *The Myth of the Privacy Paradox*, 89 Geo. Wash. L. Rev. 1 (2021); *see* Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting*, in Economics of Information Security 165, 172–73 (L. Jean Camp & Stephen Lewis eds., 2004); Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'*, 31 Current Issues in Psychology 2020 (2019).
[26] Acquisti & Grosslags, *supra* n. 25 (explaining the impact of hyperbolic discounting on privacy decision-making).
[27] Danielle Citron & Daniel Solove, *Privacy Harms*, 102 Boston University Law Review 793, 832-3 (2019) (describing how "the improper sharing of personal data can create unique opportunities for physical violence").

loss (such the theft of funds due to compromised account credentials, or the purchase of a credit monitoring software following a data breach)[28] are harms that merit prevention, mitigation, and redress. Other harms are simply more resistant to quantification than others, or do not have a weighty history of societal condemnation, such as violations of sexual privacy for which victims were blamed for the harm they suffered.[29] Psychological harms, harms connected to societal stigma, diffuse harms, community-based harms, and others are as worthy of the FTC's attention, alongside harms like physical injury and financial loss that have a richer history of societal censure and can be easier to quantify.

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

The FTC should promulgate rules that establish a floor of protections for most kinds of data, with exceptions and heightened safeguards where appropriate. Rules that solely focus on sensitive categories of data will become quickly outdated as technological threats evolve and change. They also fail to guard against the full spectrum of harms that such protections are intended to address, as seemingly benign data can become much more revealing in aggregate.[30] The spread of machine learning technologies throughout the economy exacerbate this concern, as models may produce sensitive inferences based on information that is not inherently sensitive. Types of information deemed non-sensitive—or which is deemed less appropriate for privacy protections due to important policy objectives served by making it broadly accessible—may also produce privacy risks that should not be ignored. For instance, while making domain name registration information widely accessible serves important law enforcement, IP rights enforcement, and cybersecurity research objectives, it also contains highly sensitive personal information that can put registrants at enhanced risk of spamming, as well as identity theft, spoofing, doxing (the public dissemination of private and identifying information), online harassment, and even physical harm.

Categorizing data is a reasonable part of constructing a privacy regime that does not unduly fetter anodyne or beneficial data practices, or accidentally prohibit desirable conduct. But exclusively extending protections to sensitive data, personally identifiable data, or other categories of data currently deemed most likely to reveal, embarrass, or directly produce other undesirable consequences would ignore important privacy harms that arise from other kinds of data over time, and would be brittle rather than resilient to the inevitable threat of obsolescence as technology continually evolves.

(11) Which, if any, commercial incentives and business models lead to lax data security measures or harmful commercial surveillance practices? Are some commercial incentives and

---

[28] *Id.* 834-5 ("Privacy violations can result in financial losses that the law has long understood as cognizable harm.").
[29] Danielle Citron, *Sexual Privacy,* 128 Yale Law Journal 1870, 1875-6 (2019).
[30] Solove, *supra* n. 25, at 23.

business models more likely to protect consumers than others? On which checks, if any, do companies rely to ensure that they do not cause harm to consumers?

NTIA strongly supports a vibrant digital ecosystem in which companies can create new modes of connection, learning, exploration, and enterprise. At the same time, NTIA recognizes the incentive mismatch skewing commercial decisions over data collection, retention, and sharing practices.

In today's data-driven economy, consumer data is used for a range of purposes beyond the purpose for which it was originally collected, which allows it to remain commercially viable for uses distinct from that original purpose, including uses that may be harmful.[31] For companies engaged in targeted advertising, for example, more precise targeting is believed to make consumers more likely to click on an advertisement or seek a particular product or service; this practice incentivizes these companies to collect and retain more data on millions of people, and also to use and monetize the significant amount of data they obtain in ways that may not be appropriate.[32]

Incentivizing personalized targeting has driven design choices with additional undesirable effects. Business models built on behavioral advertising tend to incorporate features that promote users staying on the service for longer, such that they see and click on a greater number of ads—which, in turn, creates user engagement statistics that are more attractive to future advertisers (and future acquirers).[33] Since outrage and controversy tend to promote continual engagement,

---

[31] *See, e.g.*, Sam Schechner and Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook.*, The Wall Street Journal (Feb. 22, 2019), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636. The FTC has previously characterized the data broker industry as one that collects massive amounts of data largely without consumers' knowledge and that can store this information indefinitely; indefinite retention of data can create security risks. *See* Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability*, at 46-49 (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf; *see also* Lesley Fair, *FTC Says Data Broker Sold Consumers' Precise Geolocation, Including Presence at Sensitive Healthcare Facilities*, Federal Trade Commission (Aug. 29, 2022), https://www.ftc.gov/business-guidance/blog/2022/08/ftc-says-data-broker-sold-consumers-precise-geolocation-including-presence-sensitive-healthcare (alleging in a recent complaint that a data broker engaged in an unfair trade practice in violation of the FTC Act when it "acquired consumers' precise geolocation data and then marketed in a form that allow[s] [its] clients [. . .] to track consumers' movements to and from sensitive locations.").

[32] *See, e.g.*, Geoffrey A. Fowler, *Your Kids' Apps are Spying on Them*, The Washington Post (June 9, 2022), https://www.washingtonpost.com/technology/2022/06/09/apps-kids-privacy ("After identifying the child-directed apps, Pixalate studied how each handled personal information, most notably charting what data each sent to the ad industry. Of all the apps Pixalate identified, 7 percent sent either location or internet address data. But popular apps were much more likely to engage in tracking because they have an incentive to make money from targeted ads, it said.").

[33] *See* Dipayan Ghosh and Ben Scott, *#DigitalDeceit: The Technologies Behind Precision Propaganda on the Internet* (2018) at 6, https://d1y8sb8igg2f8e.cloudfront.net/documents/digital-deceit-final-v3.pdf ("For internet companies that operate at a global scale, including search engines and social media platforms, there is tremendous potential value in maintaining behavioral data on users. There is a virtuous cycle in the collection of behavioral data for two primary reasons. First, the more behavioral data they are able to collect on users, the better they are able to serve them targeted ads that cater to their unique interests. Second, the better they are able show the most relevant content to the user, the longer they can keep that user on the platform, thereby maximizing potential advertising space for the user.").

some businesses are incentivized to build services conducive to fostering and presenting divisive and provocative material and disregard the dangers of product features with those effects when the end result is greater user engagement.[34] Spending long periods of time on certain social media platforms has also been repeatedly linked to negative health or wellbeing outcomes for some individuals.[35]

Businesses also seek to track and monetize individuals' behaviors beyond their use of any one service or product—tracking individuals across devices, to different Wi-Fi spots, and across space and time has been a fundamental component of the commercial surveillance ecosystem for years. The value of consumer data as a commodity has also prompted companies to incorporate design choices into their digital products and services that prompt users to share more information about themselves than they otherwise might. This visibility into consumers' inferred or actual habits, preferences, and aspirations can also provide dominant firms with advantages over smaller companies that lack access to such information, creating competitive concerns.[36]

---

[34] *See* Jeff Gary and Ashkan Soltani, *First Things First: Online Advertising Practices and Their Effects on Platform Speech*, Knight First Amendment Institute at Columbia University (Aug. 21, 2019), https://knightcolumbia.org/content/first-things-first-online-advertising-practices-and-their-effects-on-platform-speech ("Since by definition, the more provocative the content, the more likely it is to garner and retain attention, platforms are economically incentivized to permit and even to encourage the spread of extreme or controversial harmful speech, as it is likely to directly benefit them financially…The risk of data breach or theft to platforms and users is significant, as websites serving targeted advertisements must create, maintain, and store enormous datasets on millions of users") (internal citation omitted). *See also* Elizabeth Dwoskin et al., *The Case Against Mark Zuckerberg: Insiders Say Facebook's CEO Chose Growth Over Safety*, The Washington Post (Oct. 25, 2021), https://www.washingtonpost.com/technology/2021/10/25/mark-zuckerberg-facebook-whistleblower (describing internal emails documenting Facebook's tests of a change to its newsfeed algorithm designed to improve user engagement, and alleging how despite evidence that those changes increased the spread of misinformation on Facebook, the company would not adopt proposals to scale back the changes if the result would lower user engagement); Keach Hagey and Jeff Horwitz, *Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead*., The Wall Street Journal (Sept. 15, 2021), https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215 (same).

[35] *See, e.g.,* Sunny Fitzgerald, *The Internet Wants to Keep You 'Doom-scrolling.' Here's How to Break Free.*, The Washington Post (July 30, 2020), https://www.washingtonpost.com/lifestyle/wellness/coronavirus-doom-scrolling-stop/2020/07/29/2c87e9b2-d034-11ea-8d32-1ebf4e9d8e0d_story.html; Rachel Sheffield and Catherine Francois, *Is Instagram Causing Poorer Mental Health Among Teen Girls?*, United States Congress Joint Economic Committee (Dec. 1, 2021), https://www.jec.senate.gov/public/index.cfm/republicans/2021/12/is-instagram-causing-poorer-mental-health-among-teen-girls; Dylan Walsh, *Study: Social Media Use Linked to Decline in Mental Health*, Massachusetts Institute of Technology Sloan School of Management: Ideas Made to Matter (Sept. 14, 2022), https://mitsloan.mit.edu/ideas-made-to-matter/study-social-media-use-linked-to-decline-mental-health ("[R]esearchers found a significant link between the presence of Facebook and a deterioration in mental health among college students."); Georgia Wells et al., *Is Facebook Bad for You? It is for About3260 Million Users, Company Surveys Suggest*, The Wall Street Journal (Nov. 5, 2021), https://www.wsj.com/articles/facebook-bad-for-you-360-million-users-say-yes-company-documents-facebook-files-11636124681 ("Facebook researchers have found that 1 in 8 of its users report engaging in compulsive use of social media that impacts their sleep, work, parenting or relationships, according to documents reviewed by The Wall Street Journal.").

[36] *See, e.g.*, Majority Staff, H. Subcommittee on Antitrust, Commercial and Administrative Law, Comm. on the Judiciary, Majority Staff Report and Recommendations on Investigation of Competition in Digital Markets (July 2022), at 12, https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf ("Additionally, in the absence of adequate privacy guardrails in the United States, the persistent collection and

The lack of sufficient constraints on data brokers and other companies to collect and retain data that they can effectively protect may further that incentive mismatch. Frameworks that introduce friction to disincentivize harmful practices—either directly through regulation or through regulation that favors frictional solutions—can promote values beyond efficiency, including fairness, trust, security, and respect for individual autonomy.[37] NTIA recommends that the FTC consider and evaluate the positive value of introducing friction in data system designs and data collection, use, and management practices.[38]

(12) Lax data security measures and harmful commercial surveillance injure different kinds of consumers (e.g., young people, workers, franchisees, small businesses, women, victims of stalking or domestic violence, racial minorities, the elderly) in different sectors (e.g., health, finance, employment) or in different segments or "stacks" of the Internet economy. For example, harms arising from data security breaches in finance or healthcare may be different from those concerning discriminatory advertising on social media which may be different from those involving education technology. How, if at all, should potential new trade regulation rules address harms to different consumers across different sectors? Which commercial surveillance practices, if any, are unlawful such that new trade regulation rules should set out clear limitations or prohibitions on them? To what extent, if any, is a comprehensive regulatory approach better than a sectoral one for any given harm?

New trade regulation rules should prioritize comprehensiveness and include heightened safeguards for particular practices as the FTC deems necessary. This approach would minimize the risk of omitting relevant data practices, which would be more likely to occur with rigidly stratified legal definitions. Comprehensive rules maximize longevity and resilience against technological change, while an exclusively sectoral basis would overlook relevant harms.

misuse of consumer data is an indicator of market power online. Online platforms rarely charge consumers a monetary price—products appear to be 'free' but are monetized through people's attention or with their data. In the absence of genuine competitive threats, dominant firms offer fewer privacy protections than they otherwise would, and the quality of these services has deteriorated over time. As a result, consumers are forced to either use a service with poor privacy safeguards or forgo the service altogether.") (internal citations omitted); *id*. at 33 ("[A] dominant platform can use its market power to extract more data from users, undermining their privacy.") (internal citation omitted).

[37] Paul Ohm and Jonathan Frankle, *Desirable Inefficiency*, 70 Fla. L. Rev. 777, 782 (2018), https://scholarship.law.ufl.edu/flr/vol70/iss4/2. Friction as a means to achieve desired outcomes is not a new concept. For example, the waiting period introduced in a mobile device when a user incorrectly enters a passcode to unlock the device is an example of designed friction that "balances the inconvenience imposed on a forgetful user or poor typist with the device's security." *See id*. at 791. *See also* Brett M. Frischmann and Susan Benesch, Friction-In-Design Regulation as 21st Century Time, Place and Manner Restriction (Aug. 2022), at 25, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4178647 (listing examples of regulations that introduce friction or support outcomes that favor a frictional approach); Ellen Goodman, *Digital Fidelity and Friction*, 21 Nevada Law Journal 6 (2021), https://scholars.law.unlv.edu/nlj/vol21/iss2/6.

[38] *See, e.g.,* Ohm & Frankle at 782 ("Following the lead of software designers, regulators should consider mandating desirable inefficiency in order to address various concerns about information systems [. . .] Information privacy sometimes (but not always) depends on the speed with which data can be transmitted and processed, so we think mandatory time delays might sometimes offer a new source of privacy protections.").

The context surrounding various commercial surveillance practices, such as data sensitivity, the location or setting of data collection or usage, the purpose of data collection or use, relevant privacy norms, power dynamics between data collector and data subject, and other factors can significantly impact whether a given practice is anodyne, beneficial, or concerning. These contextual factors may be influenced by the sector in which a certain data practice occurs, such as healthcare, consumer finance, and others, where individuals must be able to trust that their data is in safe hands for the given sector to function, and typical practices consistently produce concerning data risks, such as collecting or sharing a student's test scores or an employee's human resources file.

But not all data uses that occur in these sectors will involve such information, and data that may not be inherently sensitive may be much more revealing in aggregate. What's more, information that produces the risks that the sectoral rule was intended to target may be produced by types of entities not covered by the sectoral rule or types of activities not covered by the sectoral rule.

Our existing sectoral laws illustrate how the specificity of sector-limited legal definitions fail to evolve alongside new technologies. The Health Insurance Portability and Accountability Act's (HIPAA) Privacy Rule creates important protections for personally identifiable health data collected by health plans, healthcare clearinghouses, and other entities,[39] but doesn't extend to health data collected by other entities that can create comparable privacy risks, such as a company that operates a period tracking app and collects information about a user's menstrual cycle. The FTC has acted to fill that gap,[40] but resources are finite, and the efforts it spends investigating and bringing an enforcement action in response to one concerning practice are efforts it cannot devote elsewhere.

The Commission's rules should be predicated on comprehensive protections for the collection and use of data by the companies under its jurisdiction, and build in any additional protections for practices it deems most likely to produce the most severe harms or risk of harms, or which threaten particularly vulnerable or marginalized populations. The FTC should make it clear that any rules it adopts present a floor, not a ceiling, for any more targeted regulations on corporate use of data about individuals and groups. A purely sectoral approach should learn from the existing deficiencies of federal privacy laws rather than replicate them.

(b) To What Extent Do Commercial Surveillance Practices or Lax Data Security Measures Harm Children, including Teenagers?

(14) What types of commercial surveillance practices involving children and teens' data are most concerning? For instance, given the reputational harms that teenagers may be characteristically less capable of anticipating than adults, to what extent should new trade

[39] U.S. Dept. of Health & Human Services, Summary of the HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#:~:text=The%20Privacy%20Rule%20protects%20all,health%20information%20(PHI).%22

[40] *See, e.g.,* FTC, *FTC Approves Final Order in Practice Fusion Privacy Case, Federal Trade Commission*, Press Release (Aug. 16, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/08/ftc-approves-final-order-practice-fusion-privacy-case.

regulation rules provide teenagers with an erasure mechanism in a similar way that COPPA provides for children under 13? Which measures beyond those required under COPPA would best protect children, including teenagers, from harmful commercial surveillance practices?

A deletion mechanism for teenagers would be a welcome objective that promotes young people's privacy, their safety, and their ability to explore new ideas and communities online. From connected devices or apps that a parent might use to monitor a child's growth, movements, or safety, to children's own uses of digital services at home, at school, and among friends, networked technologies have become an inextricable part of growing up.

As adolescents use smart phones, communicate through social networks, entertain themselves on streaming services, and engage in other aspects of digital life, data is collected about them; used to infer information about their lives; and shared, sold, or retained.[41] The principle that the relative immaturity of adolescents should compel different safeguards and consequences than would be appropriate for adults has informed a wide variety of age-contingent laws, regulations, and norms, such as the legal drinking age (21), age requirements to gamble (18 in most states), and different criminal penalties for juvenile law-breaking.[42] In the same way that teens are protected in other areas of public policy from certain risks that their relative immaturity makes them ill-equipped to adequately assess, teens should be able to use online services in a manner that protects them from privacy invasions and manipulative tactics against which they cannot be expected to appropriately guard themselves.

Simultaneously, the need for privacy protections for young people co-exists with a need to enact stronger privacy protections for everyone. Young people are certainly in need of stronger privacy protections and should be treated with special care given their relative ability to assess risk and make informed choices vis à vis adults. But as a consumer protection matter, most adults are also poorly positioned to make the kinds of risk assessments that a notice-and-choice regime requires of everyone. There may be certain protections that it would be appropriate to enact for children or teenagers as specific populations, but those should build on comprehensive protections that enhance privacy and mitigate digital risks for all age groups. Rules that do not rely on notice and consent as their central privacy protection mechanism, and focus instead on purpose limitations, data minimization requirements, and other corporate-facing measures will improve the

[41] Douglas MacMillan and Nick Anderson, *Student Tracking, Secret Scores: How College Admissions Offices Rank Prospects Before They Apply*, The Washington Post (October 14, 2019), https://www.washingtonpost.com/business/2019/10/14/colleges-quietly-rank-prospective-students-based-their-personal-data ("Records reviewed by The Post show that at least 44 public and private universities in the United States work with outside consulting companies to collect and analyze data on prospective students, by tracking their Web activity or formulating predictive scores to measure each student's likelihood of enrolling…While colleges have used data for many years to decide which regions and high schools to target their recruiting, the latest tools let administrators build rich profiles on individual students and quickly determine whether they have enough family income to help the school meet revenue goals.").

[42] Cheryl B. Preston and Brandon T. Crowther, *Legal Osmosis: The Role of Brain Science In Protecting Adolescents*, 43 Hofstra L. Rev. 447, 451-452 (2014) (noting that "the law has historically provided legal protections for minors in the areas of torts, juvenile justice, medical consent, family law, and contracts" and listing age limitations for consuming alcohol, gambling, obtaining firearms, and other activities).

ecosystem for everyone. A safer, more privacy-protective digital ecosystem is a digital ecosystem that is safer and more privacy-protective for children and teens.

(c) How should the Commission Balance Costs and Benefits?

(24) The Commission invites comment on the relative costs and benefits of any current practice, as well as those for any responsive regulation. How should the Commission engage in this balancing in the context of commercial surveillance and data security? Which variables or outcomes should it consider in such an accounting? Which variables or outcomes are salient but hard to quantify as a material cost or benefit? How should the Commission ensure adequate weight is given to costs and benefits that are hard to quantify?

The digital economy produces many benefits for the public, such as useful and efficient products and services. In the last two decades, novel, creative, and profitable uses of data have flourished, and companies operating in the United States have profoundly benefitted from an environment that has permitted widespread collection of personal data with few restrictions. This largely unfettered collection of information contributed to the development of the modern digital economy.

At the same time, the increase in data collection and use has incentivized mass surveillance and targeted marketing, resulting in a loss of privacy for individuals and communities. One civil liberties organization estimates that the advertising industry's real time online bidding system causes the location and online activity of each individual in the United States to be exposed 747 times per day.[43] Individuals routinely express exasperation, pessimism, and resignation over the privacy invasions to which they feel unavoidably subjected.[44]

The Commission should promulgate trade regulations that can help correct this misalignment of values and incentives. Strong privacy protections support individual and collective dignity, free expression, self-determination, and fairness when tracking a person's habits and activities can reduce their personhood to a marketing profile and open them up to targeting on the basis of protected characteristics. Protecting these values and rights should be at the forefront of policymakers' considerations when they examine how they can better protect the public's privacy. As the Commission determines how it should evaluate the costs and benefits of existing practices and the costs and benefits of limiting or prohibiting specific practices, the following considerations may be of value.

The Commission should bring an awareness of the difficulty of quantifying many privacy harms to its analysis of various data practices. Identifying the most effective strategies for preventing privacy harms can be challenging given the difficulty of quantifying them. Among other

[43] Irish Council for Civil Liberties, *The Biggest Data Breach; ICCL Report on the Scale of Real-Time Bidding Data Broadcasts in the U.S. and Europe*, (May 16, 2022), https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe.

[44] *See, e.g.,* Brooke Auxier et al, *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (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/.

complexities that make specifying determinations difficult are the following: 1), some harms only arise awhile after the information was gathered and shared (e.g., insights can be gleaned from data now that couldn't a few years ago); 2), the costs of lost privacy include injuries that are difficult to quantify unequivocally or at all; and 3), it is sometimes hard to attribute loss to specific data sources (such as identity thieves who might not know the original source of the data they obtain themselves, and unlikely to explain that misused information came from a particular breach or hack). Such harms are also ill-adapted to the criteria that potential plaintiffs have been required to meet to pursue privacy claims in court, and their attenuated and diffuse nature have invited critiques that harms that are difficult to unequivocally trace—as there might be multiple causes of the injury—do not merit redress.[45] Awareness of and attention to these challenges is vital to an accurate evaluation of the relevant costs and benefits of various data practices truly entail.

In evaluating those costs and benefits, the Commission will encounter arguments about the benefits of profitable, privacy-invasive business models that it should interrogate very carefully. The Commission should view arguments that data harms to individuals and the public are inherently outweighed by the profits and growth of the companies collecting their data with heavy skepticism.[46] Arguments criticizing third-party tracking reduction measurements because they limit the profits enabled by behavioral advertising[47] should also be rigorously examined for the objectives and values those arguments prioritize; it is unclear whether promoting such extractive business models, profitable though they may be, is a worthy public policy objective. Arguments that claim the benefit of receiving digital products and services without a financial payment should inherently outweigh ensuing privacy losses or other data harms should also be viewed with great skepticism, particularly given how much longer data harms may take to present themselves and how difficult they can be to trace and attribute.

---

[45] *See, e.g.,* Ryan Calo, *A Long-Standing Debate: Reflections on Risk and Anxiety: A Theory of Data Breach Harms by Daniel Solove and Danielle Keats Citron,* 96 Tex. L. Rev. Online 59 (2018), https://digitalcommons.law.uw.edu/faculty-articles/410;

[46] *See, e.g.,* FTC Commissioner Joshua Wright, *Dissenting Statement, In the Matter of Apple Inc.* (Jan. 2014) (arguing that the "apparent benefits to some consumers and to competition from Apple's allegedly unfair practices," should have been considered more robustly in the FTC's consideration before its judgment against the company), https://www.ftc.gov/sites/default/files/documents/public_statements/dissenting-statement-commissioner-joshua-d.wright/140115applestatementwright.pdf; Justus Haucap, *Data Protection and Antitrust: New Types of Abuse Cases? An Economist's View in Light of the German Facebook Decision*, CPI Antitrust Chronicle, (July 11, 2019), (concluding, among other things, that it would be more difficult to prove the use of data is an exploitive abuse of market power that harms consumers given that the data is used to improve business services) https://www.researchgate.net/publication/334398813_Data_Protection_and_Antitrust_New_Types_of_Abuse_Cases_An_Economist's_View_in_Light_of_the_German_Facebook_Decision.

[47] *See, e.g.,* The Interactive Advertising Bureau (IAB), *State of Data 2022 Part II: Preparing for The New Addressability Landscape,* at 13-14; Bruce Biegel and Charles Ping, *The Outlook for Contextual Solutions In Data Driven Advertising & Marketing Context, Search And Intent Signals Driving A New Era,* Winterberry Group (Oct. 2021) at 20, https://s3.amazonaws.com/media.mediapost.com/uploads/Winterberry_OutlookForContextualSolutions.pdf (discussing concerned advertising industry reacting to news headlines and "the Google-derived statistic, which cites average publisher revenue decreasing by 52% when third-party cookies were removed.").

The Commission's analysis should also be significantly informed by the distortion of the digital marketplace, thanks to asymmetric access to important information among companies and the public. Individuals are at a disadvantage when information about their spending habits, needs, and tastes are known to companies, while the true use and value of their own data is opaque to them.[48] Similarly, there are additional costs with assumptions and targeting that is either directed to specific communities or excludes them.[49] These skewed dynamics harm businesses as well as the public.[50]

Finally, the Commission's analysis should address how failing to prevent and deter privacy-invasive or otherwise exploitative practices that harm members of the public undermines trust in the digital economy. Strong privacy protections that limit abusive practices and promote trust will create substantial benefits for individuals, the public, and the digital economy.

(26) To what extent would any given new trade regulation rule on data security or commercial surveillance impede or enhance innovation? To what extent would such rules enhance or impede the development of certain kinds of products, services, and applications over others?

The relationship of consumer protection regulations to commercial innovation is often wrongly reduced to a false choice between entrepreneurial ingenuity on the one hand, and public safety on the other. Yet these are complementary, rather than antithetical, goals.

As privacy scholars have observed, privacy enables creativity, exploration, and intellectual risk-taking—the cultivation of important new ideas is much more difficult under the scrutiny of powerful incumbents with significant incentives to either stymie or absorb new challengers or business models.[51] What's more, the facilitation of commercial innovation as a public policy goal entails promoting conditions conducive to more creative and novel products, services, and business models—which should certainly include digital products and services that create fewer risks of privacy invasions or other information abuses. New commercial surveillance rules can

---

[48] *See, e.g.,* Stigler Committee on Digital Platforms, Final Report: The University of Chicago Booth School of Business, Stigler Center for the Study of the Economy and the State, at 67 (2019) https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf ("When facing a zero-money price, and when quality is difficult to observe, consumers are not receiving salient signals about the social value of their consumption because the price they believe they face does not reflect the economics of the transaction, and they are ignorant of those numbers"); Australian Competition & Consumer Commission, Digital Platforms Inquiry: Final Report (July 2019), at 23.

[49] *See, e.g.,* Muhammad Ali et al., *Discrimination Through Optimization: How Facebook's Ad Delivery Can Lead to Skewed Outcomes,* Proceedings of the ACM on Human-Computer Interaction 2019, Vol. 3, Issue CSCW, 199, https://dl.acm.org/doi/10.1145/3359301.

[50] *See, e.g.,* Katharine Kemp, Concealed Data Practices and Competition Law: Why Privacy Matters, 16 European Competition Journal 628, Issue 2-3, at 628-672 (2020), https://www.tandfonline.com/doi/full/10.1080/17441056.2020.1839228 (arguing that the degradation of data privacy causes objective harm to consumers and undermines the competitive process).

[51] Julie Cohen, *What Privacy Is For*, 126 Harv. L. Rev. 1904 (2013) ("But a society that values innovation ignores privacy at its peril, for privacy also shelters the processes of play and experimentation from which innovation emerges. In short, privacy incursions harm individuals, but not only individuals. Privacy incursions in the name of progress, innovation, and ordered liberty jeopardize the continuing vitality of the political and intellectual culture that we say we value.").

incentivize the development of new business models that better protect privacy and create smaller or fewer risks of online harms, when absent a legal requirement to collect less data or only collect it for certain purposes, that incentive would not exist—particularly under misaligned market conditions where lack of transparency, lack of competition, and resignation to privacy invasions dampen the potentially corrective effects of consumer privacy preferences. As with automobile safety regulations, we believe that American industry is able to adapt, thrive, and build despite changing constraints that change current incentives and consumer interests.

(27) Would any given new trade regulation rule on data security or commercial surveillance impede or enhance competition? Would any given rule entrench the potential dominance of one company or set of companies in ways that impede competition? If so, how and to what extent?

Traditionally, arguments for enhancing competition have focused on enhancing the environment for businesses to compete, with the assumption that competition in a variety of areas of innovation would be free to grow. However, companies have yet to compete on a wide scale on the strength of their commitments to customer privacy. Some companies do prioritize and highlight that aspect, but generally they lack the ability to shine against their competitors due lack of transparency surrounding data practices, the profitability of data-centric business models, and other factors. Over decades of development of digital commerce, the appeal of data-centric business models to developers and investors has remained steadfast. Baseline privacy rules may have pro-competitive effects that would benefit the digital economy, small businesses, and the public.

There are many theories on why it is difficult to compete on the basis of privacy-protective practices in this ecosystem. Recently, DuckDuckGo, Proton, and eleven other businesses that market themselves as privacy-protective urged Congress to act to adopt new digital competition legislation to even the field for competition. In particular, they alleged that "tech giants …intentionally … lock users into perpetual surveillance" and make it hard for users "to switch to privacy-protective alternatives."[52] As noted elsewhere, NTIA believes it is important to change the current incentives shaping the commercial data ecosystem so that businesses can innovate without being tied to a system based on commercial surveillance.

If the Commission adopted rules that provided baseline privacy protections, businesses that currently rely on privacy-invasive, data-centric revenue models would need to identify more privacy-protective approaches, creating a more level playing field for privacy-protective businesses that have struggled to challenge competitors that have profoundly benefitted from unsavory data practices. Furthermore, basic privacy requirements might then allow companies to compete on the strengths of the services they actually offer, rather than their ability to trade in personal data. Such rules might create new opportunities for less entrenched market participants to succeed, as larger companies may face greater obstacles in shifting from extractive business models to more privacy-protective ones.

[52] Letter from Andi, Brave, et al to Congressional Leadership (Sept. 13, 2022), https://www.spreadprivacy.com/privacy-companies-call-for-vote/.

Equitable access to data is a critical challenge to address in enabling competition and consequent benefits. The use of specific categories of privacy-enhancing technologies can facilitate better access among market participants while providing protections for individuals' privacy as well as organizations' intellectual property. While much work remains to be done to enable the widespread adoption of these technologies, the Biden Administration has undertaken a number of activities to advance their maturation.[53] In considering the question of data access, the Commission should take into account the opportunities that privacy-enhancing technologies can provide to achieve solutions that meet multiple objectives—including privacy and competition.

(28) Should the analysis of cost and benefits differ in the context of information about children? If so, how?

The benefits of enacting strong, comprehensive privacy protections for individual people, communities, the public at large, and businesses provide strong support for enacting such rules. Young people would benefit from comprehensive privacy rules that reshape existing incentives to pervasively track individuals, and they may also benefit from comprehensive rules with additional limits on the collection and use of their data specifically. Stronger privacy protections would reflect our societal imperative to ensure the ability of young people to safely explore, learn, and thrive.

In some areas, children may be more vulnerable to exploitative practices than adults are, such that the case for mitigating the harms they may experience is particularly strong. Profiles and inferences constructed from their data—from one estimate, an average of 72 million data points about each child by the age of 13 made available to advertising firms[54]— could limit important life opportunities,[55] while the safety risks of privacy invasions may be particularly significant.[56] Children will also often be unable to avoid injuries that result from unfair trade practices. Studies have found that while young children tend to grasp the implications of interpersonal privacy risks, but struggle to extrapolate to systemic risks created by commercial or institutional

[53] *See, e.g.*, The White House, *U.S. and U.K. Launch Innovation Prize Challenges in Privacy-Enhancing Technologies to Tackle Financial Crime and Public Health Emergencies*, Press Release, (July 20, 2022), https://www.whitehouse.gov/ostp/news-updates/2022/07/20/u-s-and-u-k-launch-innovation-prize-challenges-in-privacy-enhancing-technologies-to-tackle-financial-crime-and-public-health-emergencies; Networking and Information Technology Research and Development (NITRD), Advancing Privacy-Preserving Data Sharing and Analytics, https://www.nitrd.gov/coordination-areas/privacy-rd/appdsa.

[54] Fowler, *supra* n. 32.

[55] MacMillan and Anderson, *supra* n. 41; N. Cameron Russell et al., *Transparency and the Marketplace for Student Data*, 22 Va. J.L. & Tech. 107, 115 (2019) (noting how in the course of researching the trade and sale of student data, the authors encountered a data broker who was "perfectly willing to sell a list of 'fourteen and fifteen year old girls for family planning services'").

[56] Charlie Warzel and Stuart A. Thompson*, Where Even the Children Are Being Tracked*, The New York Times (Dec. 21, 2019), https://www.nytimes.com/interactive/2019/12/21/opinion/pasadena-smartphone-spying.html (noting that in response to being shown 6 months of location tracking data for 80 John Muir High students, high school principal's "thoughts went to the kids he knew who were having trouble with an abusive parent. 'I just think about those families,' he said, letting out a short, exasperated sigh. 'If there's child abuse or there's something going on and this parent has access to find out where this kid is even though they're not supposed to. That's what bothers me the most. Because I do know those situations.'").

collection and use practices.[57] Children are less able to discern persuasive intent than adults, potentially making them more likely to fall prey to manipulative tactics to provide their money or private information to an unscrupulous company.[58] The notice-and-choice theory of privacy governance is particularly untenable for minors, and it is unreasonable to expect parents to successfully police every product and service their child is exposed to, including services they are required to use for school. Children may also lack decision-making power over their use of a digital product or service, such as being functionally required to use a product or app in school or for an extracurricular activity.

At the same time, most of those vulnerabilities are not unique to young people, and simultaneously support the need for stronger privacy protections for people of all ages, with heightened protections for young people in certain circumstances. For example, the collection and use of real-time location data can create sufficient privacy and safety risks for both children and adults—a child may be more physically vulnerable if someone who wishes to harm them obtains a dataset that illustrates their movements, but that safety risk certainly still exists for adults.[59] A child whose literacy skills meet a sixth-grade reading level may be less equipped to accurately interpret a privacy policy for a product or service than a college-educated adult,[60] but that difference does not indicate that the adult is *well*-equipped to accurately interpret the policy and make privacy-protective decisions on that basis. The vulnerability of young people to data abuses, and the societal imperative of enabling their ability to safely learn, grow, and flourish, adds further support to the already strong case for enacting trade regulation rules with strong privacy protections for everyone, with stricter limits for uses of children's data where appropriate.

(d) How, if at all, Should the Commission Regulate Harmful Commercial Surveillance or Data Security Practices That Are Prevalent?

(i) Rulemaking Generally

(30) Should the Commission pursue a Section 18 rulemaking on commercial surveillance and data security? To what extent are existing legal authorities and extralegal measures, including self-regulation, sufficient? To what extent, if at all, are self-regulatory principles effective?

---

[57] Sonia Livingstone et al., *Children's Data and Privacy Online: Growing Up in a Digital Age*, London School of Economics and Political Science (2019), at 14-5; Mariya Stoilova et al., *Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy*, 8 Media and Communication 197, Issue 4, at 200 (2020).

[58] Jenny Radesky, MD, et al., *Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children*, Jama Network Open 2-11, 2 (June 17, 2022), https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2793493.

[59] *See, e.g.,* National Security Agency, *How Mobile Device Users Can Limit Their Location Data Exposure,* Central Security Service, Press Release, Aug. 4, 2020, https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2298930/how-mobile-device-users-can-limit-their-location-data-exposure*;* Cindy Southworth, *Testimony of the National Network to End Domestic Violence with the Minnesota Coalition for Battered Women*, Senate Judiciary Committee, Subcommittee on Privacy, Technology and the Law, Hearing on Location Privacy Protection Act of 2014 (June 4, 2014), https://www.judiciary.senate.gov/imo/media/doc/06-04-14SouthworthTestimony.pdf.

[60] Livingstone et al, *supra* n. 57 at 15.

As discussed elsewhere in this comment, notice and choice mechanisms have failed to provide adequate notice, offer meaningful choice, or prevent undesirable privacy risks and harms. NTIA strongly supports the FTC's effort to develop rules to address the harmful effects of commercial surveillance.

The FTC's role in protecting consumers and promoting competition is well-established and critical to the functioning of a healthy digital economy. Although the states and Department of Justice are partners in enforcing consumer protection and competition laws, the FTC is uniquely positioned with its expertise and authority to provide guardrails for businesses. Rulemaking affords the agency the best way to do this efficiently and across industries, while also ensuring its consumer protection and competition efforts keep pace with the evolution of new technologies.[61]

While some industry-led governance codes, best practices, and procedures have produced better results in other areas of technology policy, they have not been sufficient to protect consumers' privacy or prevent harmful collection and use practices. The National Institute of Standards and Technology (NIST) Privacy Risk Assessment Methodology offers a model to support organizations in effectively evaluating privacy risks to individuals and groups when designing or deploying products, services, and systems that process data,[62] but it is not meant to replace more concrete guidance and mandatory rules. Other efforts, such as a multistakeholder efforts, have not resulted in large-scale adoption of privacy principles.[63] In addition, as the FTC's own oversight has shown, the efficacy of enforcement mechanisms for industry-run codes should not be assumed.[64]

Nor are industry-derived privacy codes well-situated to provide redress to harmed individuals. The profits enabled by invasive collection practices and the relatively minimal consequences of relying on such practices prevent the necessary conditions for companies to create rules that would prioritize privacy or safety over corporate flexibility in circumstances where it would be in the best interest of the public that they do so.

---

[61] Sector-specific rules, which have addressed specific areas, include the Fair Credit Reporting Act from 1970 and HIPAA from 1996.

[62] The NIST Privacy Risk Assessment Methodology is a tool that applies the risk model from NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, and helps organizations analyze, assess, and prioritize, privacy risks to determine how to respond and select appropriate solutions. NIST, *Risk Assessment Tools,* Privacy Engineering Program, https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/focus-areas/risk-assessment/tools.

[63] For example, an NTIA-led effort on mobile app transparency resulted in a 2013 code of conduct, https://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency; and a multi-stakeholder effort led by the Department of Energy produced an energy-related privacy code, https://www.smartgrid.gov/data_guard.

[64] *See, e.g.,* FTC, *TRUSTe Settles FTC Charges it Deceived Consumers Through Its Privacy Seal Program Company Failed to Conduct Annual Recertifications, Facilitated Misrepresentation as Non-Profit,* Press Release (Nov 17, 2014) *("*"The FTC's complaint alleges that from 2006 until January 2013, TRUSTe failed to conduct annual recertifications of companies holding TRUSTe privacy seals in over 1,000 incidences, despite providing information on its website that companies holding TRUSTe Certified Privacy Seals receive recertification every year.").

Given the current economic incentives, rules that are intended to promote privacy should be written and overseen by entities dedicated to serving the public interest.

(ii) Data Security

(36) To what extent, if at all, should the Commission require firms to certify that their data practices meet clear security standards? If so, who should set those standards, the FTC or a third-party entity?

While security and privacy are closely linked, there are sufficient differences to merit some degree of distinction between approaches, including the relative maturity of security standards and distinct incentive structures driving business practices. There is no universally applicable approach to security standards. NTIA suggests that any effort to explore this issue start with a review of existing best practices and guidelines. For example, NTIA has worked to promote security of the communications system through work to help ensure security in the supply chain, as well as efforts such as disclosures about software components and Internet of Things device security measures.[65] NIST has also worked with industry to develop guidance in particular areas.

Having firms certify to meeting appropriate industry standards would ensure that a company selects an official to take on some responsibility for security efforts and ensure a baseline level of security. However, determining what those standards would be is a complex endeavor and may be best pursued through a multistakeholder approach.

The FTC should be careful to avoid taking an overly prescriptive in identifying cybersecurity standards, as doing so could ossify security practices, or lead to a mismatch between standards and the cybersecurity needs of the company. Any such requirements should be performance- and outcome-based.

The Federal Communications Commission (FCC)'s approach to the system for law enforcement access to content might be provide a useful example of an approach. In that case, the FCC has some requirements directly responsive to the Communications Assistance for Law Enforcement Access law (CALEA), but generally "does not get formally involved with the compliance standards development process."[66] Instead, industry has that role.[67] To ensure quality standards are adopted, the law provides the FCC with the ability to develop standards or technical requirements itself, if the standards are deficient, and any party can raise that as a concern.[68] That

---

[65] *See, e.g.,* NTIA, Communications Supply Chain Risk Information Partnership (C-SCRIP), https://www.ntia.gov/cscrip; NTIA, *Stakeholder-Drafted Documents on IoT Security* (July 13, 2018), https://www.ntia.gov/IoTSecurity; NTIA, Software Bill of Materials, https://www.ntia.gov/SBOM.

[66] *See,* Federal Communications Commission, Communications Assistance for Law Enforcement Act, Public Safety Bureau, Policy and Licensing Division, https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance.

[67] *Id.* ("Entities subject to CALEA are responsible for reviewing the Commission's regulations and analyzing how this regulation applies per their specific network architecture"); Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. § 1006(b), at Sec. 107(b), https://ndcac.fbi.gov/calea/thelaw/section107.

[68] 47 U.S.C. § 1006(b) ("If industry associations or standard-setting organizations fail to issue technical requirements or standards or if a Government agency or any other person believes that such requirements or standards are deficient").

way, industry is incentivized to develop thorough standards before an agency would intervene in the specifics.

Whether certification is required or not, the FTC might consider requiring that a company, perhaps those with higher revenue thresholds, designate an official as responsible for compliance with the standards.[69]

(iii) Collection, Use, Retention and Transfer of Consumer Data

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

While differences in technologies and contexts of use create distinct risks, the practical immutability of biometric identifiers and the severity of the harms they can enable make biometric technologies well-suited to specific limitations in new trade regulations.

Biometric technologies encompass a range of applications and technologies that carry inherently different levels of risk of harmful use. NIST defines biometrics as "[a] measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant."[70] For example, fingerprint templates can be derived from surfaces touched by an individual without the presence of that individual or their knowledge; facial recognition technologies can be used from a distance or derived from video footage or photographs, but palm vein recognition currently requires the presence of the data subject. Biometric technologies can be used for differing applications and purposes depending on their configuration and capabilities. Biometric technologies that measure the characteristics of faces can be used for a) facial detection, which recognizes the presence of a face but does not attempt any further analysis; b) facial recognition, which can either authenticate the identity of a data subject or identify them using a pre-existing data set; and c) facial categorization, which purports to sort individuals based on categories such as race, age, or gender. In considering rules, the FTC should recognize the degree to which the risk of harm can vary depending on the context of use and technologies deployed.

Due to their use of physical characteristics, many of which rarely change over time, the use of biometric technologies can create practically immutable identifiers that can be used to link information across contexts, often in ways that are hard for individuals to discern, track, or prevent. Due to the difficulty in changing the physical characteristics from which a template is created, the risks associated with data breach or misuse are significantly higher than that of

[69] For example, with CALEA, relevant carriers must file and maintain up-to-date System Security and Integrity (SSI) plans with the FCC, as described in FCC rules, including the names of people at the companies responsible for the compliance. *See* FCC, CALEA System Security and Integrity (SSI) Policies and Procedures Checklist, https://www.fcc.gov/sites/default/files/calea-checklist-2013.pdf.
[70] Nieles et al., *An Introduction to Information Security,* NIST SP 800-12 Rev. 1, NIST (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

identifiers that can be easily altered, such as usernames or passwords. The FTC's trade regulations, while maintaining an understanding of the relative risks of different uses and technologies, should nonetheless define biometric templates and outputs as inherently carrying higher risk to individuals.

Further, biometric identifiers can be created from data collected for other purposes, such as images put onto social media sites—even private accounts—can be scanned to assemble facial recognition templates and databases.[71] Trade regulations focused on purpose specification should not only include limitations on the consensual use of biometric technologies, but also should place limitations on the use of data for the nonconsensual creation of templates and databases.

Finally, the FTC should give careful consideration to the use of technologies that purport to identify individuals on the basis of social categories or status, such as race, sexuality, criminality, or proxies for those categories, as well as technologies that purport to predict social outcomes, such as recidivism or job success.[72] The bases for these technologies are often disproven theories that connect physical characteristics to social status, and their potential for discriminatory misuse is high.[73] In drafting its trade regulations, the FTC should consider studying these technologies and the ways in which their uses could be considered unfair or deceptive.

(43) To what extent, if at all, should new trade regulation rules impose limitations on companies' collection, use, and retention of consumer data? Should they, for example, institute data minimization requirements or purpose limitations, i.e., limit companies from collecting, retaining, using, or transferring consumer data beyond a certain predefined point? Or, similarly, should they require companies to collect, retain, use, or transfer consumer data only to the extent necessary to deliver the specific service that a given individual consumer explicitly seeks or those that are compatible with that specific service? If so, how? How should it determine or define which uses are compatible? How, moreover, could the Commission discern which data are relevant to achieving certain purposes and no more?

As discussed above, the Commission's rules should shift the burden of mitigating and preventing privacy risks from individuals to businesses. Previous efforts by Department of Commerce agencies have been guided by that principle. In 2018, NTIA requested comments on several high-level goals for privacy legislation, a process that was part of a White House-driven

---

[71] *See, e.g.*, Jon Porter, *Facebook and LinkedIn are Latest to Demand Clearview Stop Scraping Images for Facial Recognition Tech,* The Verge (Feb. 6, 2020), https://www.theverge.com/2020/2/6/21126063/facebook-clearview-ai-image-scraping-facial-recognition-database-terms-of-service-twitter-youtube.

[72] Some scholars have dubbed these technologies "physiognomic artificial intelligence," linking them to heavily discredited pseudoscience of past eras. Luke Stark and Jevan Hutson, *Physiognomic Artificial Intelligence*, 32 Fordham Intellectual Property, Media & Entertainment Law Journal 922, (2021) https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1804&context=iplj.

[73] *See, e.g., Id.;* Sarah Myers West et al., *Discriminating Systems: Gender, Race and Power in AI,* AI Now Institute (2019), https://ainowinstitute.org/discriminatingsystems.pdf; Os Keyes, *The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition*, Proceedings of the ACM on Human-Computer Interaction 2018, Vol 2, Issue CSCW, 1-22.

undertaking to modernize U.S. data privacy policy.[74] Simultaneously, NIST began a public and open collaboration process to develop a voluntary framework to help organizations manage privacy risks.[75] Published in January 2020, the framework is used by organizations of all sizes, across all sectors, around the world.[76] Themes from each of those efforts are worth FTC consideration as it explores possible privacy rules.

In particular, the FTC should consider adopting rules to minimize the collection and retention of information; hold businesses accountable for the purpose which the personal data has been collected, maintained or used; and require security safeguards to manage the risk of disclosure or harmful uses of personal data.

Data minimization requirements draw on a long-established consensus among privacy experts: The less data a company collects, the less data can fall prey to unauthorized access. Even the Privacy Act of 1974, which governs the collection and use of personal information by the U.S. government, starts out with a basic premise that agency records will include "only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[77] Today, many expert agencies worldwide have made it clear that this is a fundamental element to data protection. NIST guidance embraces the concept of minimizing data collection.[78] Europe's General Data Protection Regulation (GDPR) also makes use of the data minimization concept in numerous places.[79] Some states, such as Virginia, have adopted privacy legislation with data minimization requirements.[80] Related to that, companies should only keep data for as long as it is actively needed or that which is necessary for authentication (such as confirming identity to secure an account and preventing unauthorized access to it).

In addition, NTIA suggests that the FTC consider adopting rules that impose purpose limitations for data gathered in certain contexts. For example, data gathered to provide services should be limited for providing those services. In particular, personal data should not be shared with third parties— including affiliates in a different business line—without a reason related to the initial purpose of collection, or, in a more limited manner, purely for authentication and security

---

[74] NTIA, *NTIA Seeks Comment on New Approach to Consumer Data Privacy*, Press Release (Sept. 25, 2018), https://www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy.
[75] NIST, *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0* (Jan. 16, 2020), https://doi.org/10.6028/NIST.CSWP.01162020; *see also*, NIST, *Development Archive*, https://www.nist.gov/privacy-framework/development-archive.
[76] *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0* (National Institute of Standards and Technology, 2020), available at https://doi.org/10.6028/NIST.CSWP.01162020.
[77] 5 U.S.C. § 552a(e)(1).
[78] Sean Brooks et al., *An Introduction to Privacy Engineering and Risk Management in Federal Systems* (NIST 8062), NIST (Jan. 2017), https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf (discussing in various parts how to implement data minimization practices).
[79] GDPR Art.5(1) (c); *see also,* Cal. Civ. Code §1798.100(c).
[80] Va. Code. Ann. § 59.1-574. California's privacy law ties data retention to a company's disclosure of how long it would retain or use data, but cautions that "a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose." Cal. Civ. Code §1798.100(a)(3). General Duties of Businesses that Collect Personal Information.

purposes. Participation in the advertising marketplace or the data aggregation marketplace should be considered a distinct purpose from providing any other "service" to a consumer.[81] This concept permeates modern privacy law. For example, the California Privacy Rights Act requires that business data practices for consumer personal information "be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed," or "another disclosed purpose… compatible with the context" of that collection.[82]

Finally, privacy cannot exist without security. While NTIA cautions the FTC that detailed standards can quickly become outdated due to technological shifts, some basic requirements for securing data should be in place for every business that gathers it. Such practices are well-established in certain sectors. Examples include regulations stemming from the Gramm Leach Bliley Act in the financial sector, and HIPAA's rules for certain entities in the healthcare sector. These have helped provide a basic level of security requirements for entities covered by the relevant rules.[83] Some broader privacy laws, such as the GDPR, includes requirements for data security safeguards.[84] If information is accessed by unauthorized parties, then all efforts to ensure it is used and disposed of properly become meaningless. The FTC should adopt basic data security requirements.

(vi) Automated Decision-Making Systems

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

An automated decision-making system (ADS) is a process to automate in whole or in part a decision or policy, usually by means of data analysis and prediction.[85] Specifically, the mechanisms include, "predicting, scoring, analyzing, classifying, demarcating, recommending, allocating, listing, ranking, tracking, mapping, optimizing, imputing, inferring, labeling, identifying, clustering, excluding, simulating, modeling, assessing, merging, processing, aggregating, and/or calculating."[86] ADS can produce many benefits by matching people with appropriate goods and services at scale, for example appropriate medical care, employment, housing, credit, and other opportunities. At the same time, ADS can create harms at scale in these very same areas by denying people those opportunities because of discrimination, error,

[81] *See, e.g.,* Center for Democracy & Technology, Federal Communications Commission Empowering Broadband Consumers Through Transparency, CG Docket No. 22-2, Reply Comment at 3.
[82] Cal. Civ. Code §1798.100(c), General Duties of Businesses that Collect Personal Information.
[83] *See, e.g.,* Securities and Exchange Commission, Final Rule, Privacy of Consumer Financial Information (Regulation S-P), 17 C.F.R. Part 248, https://www.sec.gov/rules/final/34-42974.htm.
[84] *See, e.g.*, Art. 25 GDPR - Data protection by design and by default, https://gdpr.eu/article-25-data-protection-by-design.
[85] *See, e.g.,* Rashida Richardson, *Defining and Demystifying Automated Decision Systems,* 81 Md. L. Rev. 785, 795 (2022) (proposing a comprehensive and narrow definitions for government ADS, but which can be adapted for all ADS).
[86] *Id.* For other discussions of ADS, *see* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 8-10 (2014).

unfair data governance practices, and other defects in the development and implementation of the systems.[87]

The Commission has issued guidance to businesses on the use of "AI and algorithms"[88] and has conducted a public hearing on how ADS could impact competition and consumer protection.[89] In addition, Commissioner Rebecca Kelly Slaughter has written about algorithms and economic justice, outlining various ADS-related harms.[90] The benefits and harms of ADS were included in discussions of privacy, equity, and civil rights by panelists at NTIA's listening sessions on the topic, which will be followed by a forthcoming Request for Comment.[91]

Among the specific ADS-related risks posed to individuals are:

- **Bias risks.** The ADS model is trained on or uses data that is biased with respect to protected characteristics, or otherwise fits into a biased decision-making structure, resulting in disparate impact that harms members of the protected groups.[92] There have been many examples of this harm in the hiring context where job applicants face online screening that uses ADS to score applicants based on their facial expressions or word choices. When the ADS is trained on data derived from white faces, certain kinds of speech and facial expressions, or other skewed data sets, it may penalize applicants of color and others who don't conform to the training data.[93] This kind of bias also frequently turns up in health care determinations where women, minorities, and other groups under-represented in the training data can be offered sub-optimal services.[94]

---

[87] Andrew Smith, Using Artificial Intelligence and Algorithms, FTC Business Guidance Blog, April 8, 2020, https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms.
[88] *Id.*
[89] FTC, FTC Hearing #7: The Competition and Consumer Protection Issues of Algorithms, Artificial Intelligence, and Predictive Analytics, Nov. 13-14, 2018, https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms.
[90] 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, 56 (August 2021), https://yjolt.org/sites/default/files/23_yale_j.l._tech._special_issue_1.pdf. (using the term "algorithmic justice" to describe civil rights protections that "limit the dangers of algorithmic bias and require companies to be proactive in avoiding discriminatory outcomes.").
[91] NTIA, *NTIA Virtual Listening Sessions on Personal Data: Privacy, Equity, and Civil Rights*, Jan. 3, 2022, https://www.ntia.doc.gov/other-publication/2022/ntia-virtual-listening-sessions-personal-data-privacy-equity-and-civil-rights.
[92] *See, e.g.,* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Calif. L. Rev. 671, 673-76 (2016); Pauline T. Kim, *Big Data and Artificial Intelligence: New Challenges for Workplace Equality*, 57 U. Louisville L. Rev. 313, 321 (2019); Rashida Richardson et al., *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U L. Rev. 193 (2019).
[93] *See* Ifeoma Ajunwa, *An Auditing Imperative for Automated Hiring,* 34 Harv. J.L. & Tech. 1, 7 (2021) http://dx.doi.org/10.2139/ssrn.3437631.
[94] *See, e.g.,* 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.

- **Risks of error.** Apart from producing discriminatory results, the ADS may be erroneous in other ways and fails to work as represented and/or intended, resulting in harm.[95] Predictive models can be wrong in many ways and for many reasons. For example, during the COVID crisis, algorithmic models were not very effective in predicting disease developments and managing logistics because the models were so inexact. Because of "bad datasets, automated discrimination, human failures, and a complex global context," ADS models "failed to deliver…in diagnosing Covid, predicting its course through a population, and managing the care of those with symptoms."[96] Banks successfully use ADS to detect credit card fraud and governments use it to detect fraud in programs they oversee.[97] But when those fraud detection models are wrong, people can erroneously lose financial entitlements, with devastating effects for the most vulnerable. This has happened in Idaho, Indiana, Arkansas, and Michigan when those states' ADS falsely flagged Medicaid fraud and wrongfully withheld benefits from millions of residents.[98]
- **Economic risks.** ADS can contribute to competition and individual economic harms by, for example, helping dominant market players to act anti-competitively through obfuscated collusion or by personalizing pricing.[99] The UK's Competition Markets Authority provides many examples of how personalized pricing based on factors such as an individual's location can result in higher prices for those targeted.[100]
- **Legal process risks.** The ADS and related institutional structures deny people the right to challenge or opt out of decisions, resulting in harm.[101] Most of the reported legal process harms have arisen in the context of public sector ADS, because this is where process rights are most developed. For example, when an ADS produced inexplicable demotion and termination decisions about Houston public school teachers, the Houston Federation

[95] *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, 48 (2019) (reporting on study that showing flawed conclusions based on biometric data).
[96] Bhaskar Chakravorti, *Why AI Failed to Live Up to Its Potential During the Pandemic*, Harvard Business Review, (Mar. 17, 2022), https://hbr.org/2022/03/why-ai-failed-to-live-up-to-its-potential-during-the-pandemic.
[97] *See, e.g.,* U.S. Gov't Accountability Off., GAO-19-115, *Supplemental Nutrition Assistance Program: Disseminating Information on Successful Use of Data Analytics Could Help States Manage Fraud Risks* (Oct. 02, 2018).
[98] *See* Michele Gilman, *AI Algorithms Intended to Root Out Welfare Fraud Often End Up Punishing the Poor Instead*, The Conversation, Feb. 14, 2020, https://theconversation.com/ai-algorithms-intended-to-root-out-welfare-fraud-often-end-up-punishing-the-poor-instead-131625.
[99] *See, e.g.,* Michal S. Gal, *Algorithms as Illegal Agreements*, 34 Berkeley Tech. L.J. 67, 67 (2019); Slaughter et al., *supra* n. 90, at 32-54).
[100] *See* UK Competition and Markets Authority, *Algorithms: How They Can Reduce Competition and Harm Consumers*, 33-36(Jan. 19, 2021) at 30-36, https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers#theories-of-harm.
[101] *See, e.g.,* Hannah Bloch-Wehba, *Access to Algorithms*, 88 Fordham L. Rev. 1265 (2020) (discussing the risks to legal process in the context of public ADS).

of Teachers members asked to examine the systems but were denied access purportedly because of the ADS vendor's trade secret claims.[102]

- **Opacity risks.** The ADS denies people the ability to know how decisions were made that affect them, resulting in harm.[103] Algorithmic opacity, or what is known as the algorithmic "black box" problem, deprives people of their ability to understand and therefore respond autonomously to algorithmic decisions. This loss of agency is itself a harm. Some of these harms are non-economic, such as when an ADS promotes media content to people that disinforms or hurts them.[104] Other harms are economic. The FTC's consideration of Dark Patterns surfaced algorithmic models that manipulate choice architectures so that people are pushed into economic decisions they would not freely choose.[105] The EU's Dark Patterns Report provides this example:

  > Online platforms and traders gather data and then test different nudges. They see the reaction and steadily feed the information into machine learning algorithms that produce improved and refined nudges in a self-propelling cycle that is beneficial to them but may be detrimental for consumers.[106]

- **Positional power risks.** The ADS harms people by steering them into positions of reduced power vis-à-vis employers, governments, vendors, educators, landlords, and other users of the ADS in part because of asymmetrical information, opacity, and the lack of recourse to contest erroneous decisions.[107] Pervasive workplace surveillance and/or platform management of "gig" workers provides data for ADS that can shape working conditions, opportunities, and compensation. For example, Uber has linked the quality and quantity of work available to drivers to a performance management tool that is hidden from drivers.[108] They do not know the basis for performance assessment and therefore cannot protest or bargain around the management decisions.

---

[102] Rashida Richardson et al., *Litigating Algorithms: Challenging Government Use of Algorithmic Decision Systems*, AI Now Inst., Ctr. On Race, Ineq. & Law, & Elec. Frontier Found., at 10 (Sept. 2019). *See also Hous. Fed'n Teachers., Loc. 2415 v. Hous. Indep. Sch. Dist*., 251 F. Supp. 3d 1168 (S.D. Tex. 2017) (denying school district's motion for summary judgment on procedural due process claims, but leaving trade secrets claims intact).

[103] *See, e.g.,* Jenna Burrell, *How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, (Sept. 15, 2015), http://dx.doi.org/10.2139/ssrn.2660674.

[104] *See, e.g*., Jeremy Wright & Sajid Javid, Online Harms White Paper 42 (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online Harms White_Paper.pdf [https://perma.cc/BN3Q-R9RS].

[105] FTC Staff Report, *Bringing Dark Patterns to Light,* Sept. 2022, https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

[106] Francisco Lupiáñez-Villanueva et al., *Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation: Final Report*, European Commission, Directorate-General for Justice and Consumers (May 2022), at 20, https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418.

[107] *See, e.g.,* Ari Ezra Waldman, *Power, Process, and Automated Decision-Making*, 88 Fordham L. Rev. 613 (2019).

[108] Worker Info. Exchange, *Managed by Bots: Data-Driven Exploitation in the Gig Economy* (Dec. 2021), https://www.workerinfoexchange.org/wie-report-managed-by-bots.

Marginalized and historically disadvantaged communities bear disproportionate risk of harm.[109] ADS systems may reify and amplify historic biases against protected groups in the allocation of goods and services. This has been evident, for example, in hiring-related ADS that discriminates against women and other groups,[110] in housing-related ADS that discriminates against communities of color,[111] and in educational-related ADS that discriminates against people based on facial expressions or physical movements.[112] People who are economically vulnerable are also more vulnerable to ADS harms and those harms may be especially severe. For example, the state of Michigan used an ADS system to detect fraud connected with unemployment benefits and erroneously suspended benefits for tens of thousands of people, forcing many into bankruptcy and penury.[113] Children are also at disproportionate risk of harm from ADS, for example when these systems erroneously limit their educational opportunities[114] or recommend family service interventions based on faulty risk modeling.[115]

(60) To what extent, if at all, should new rules forbid or limit the development, design, and use of automated decision-making systems that generate or otherwise facilitate outcomes that violate Section 5 of the FTC Act? Should such rules apply economy-wide or only in some sectors? If the latter, which ones? Should these rules be structured differently depending on the sector? If so, how?

As the FTC has noted, it has decades of experience enforcing legal prohibitions related to ADS across sectors.[116] These include Section 5 of the FTC Act (forbidding "unfair or deceptive acts or practices in or affecting commerce" including through the use of ADS), the Fair Credit Reporting Act (regulating decision-making around employment, housing, credit, insurance and other benefits including through the use of ADS), and the Equal Opportunity Act (forbidding use

[109] *See generally*, Nicol Turner Lee et al., *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms*, Brookings Institution (May 22, 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms.
[110] *See generally*, Miranda Bogen, *All the Ways Hiring Algorithms Can Introduce Bias***,** Harvard Business Review, (May 06, 2019), https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias*;see also* Anja Lambrecht and Catherine Tucker, *Algorithmic Bias? An Empirical Study of Apparent Gender-Based Discrimination in the Display of STEM Career Ads*, Management Science 2019 65:7, 2966-2981.
[111] *See, e.g.,* Emmanuel Martinez and Lauren Kirchner, *The Secret Bias Hidden in Mortgage-Approval Algorithms*, The Markup (Aug. 25, 2021), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.
[112] *See, e.g.,* Lindsey Barrett, *Rejecting Test Surveillance in Higher Education* (July 29, 2021). 1 Mich. St. L. Rev. (forthcoming 2023), https://ssrn.com/abstract=3871423 (identifying the harms of automated proctoring).
[113] *See, e.g.,* Joanna Redden et al., *Automating Public Services: Learning from Cancelled Systems*, Carnegie Trust UK, 2022, https://www.carnegieuktrust.org.uk/publications/automating-public-services-learning-from-cancelled-systems (describing the Michigan Integrated Data Automated System and others).
[114] *See, e.g*., Tom Simonite, *Meet the Secret Algorithm That's Keeping Students Out of College*, Wired (July 10, 2020), https://www.wired.com/story/algorithm-set-students-grades-altered-futures.
[115] *See, e.g.,* Turner Lee et al, *supra* n. 109 (describing several decisions around the world to cancel use of family services predictive algorithms because of erroneous and/or biased outcomes, including the Illinois Department of Children and Family Services' decision to stop use of the Rapid Safety Feedback system).
[116] Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FTC Business Guidance Blog (Apr. 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

of a biased ADS that results in illegal discrimination around credit decisions). The recent use of algorithmic disgorgement as a remedy in the case of illegal data practices connected to ADS is a promising way to hold companies accountable and to deter future illegal practices.[117]

The FTC should adopt rules to mitigate the risk of harms from ADS to clarify which practices are illegal, foster practices that reduce the development and use of ADS most prone to produce illegal practices, and deter the deployment of such ADS. In addition to codifying the FTC's enforcement decisions, these rules incentivize processes to reduce ADS risks and can complement the AI Risk Management Framework being developed by the Commerce Department's National Institute of Standards and Technology.[118] Specifically, the FTC should adopt rules to forbid or limit the use of ADS in ways that result in violations of Section 5 of the FTC Act, including practices that discriminate unlawfully against members of protected groups; impose economic harms on consumers and workers; and harm especially vulnerable people (which includes historically marginalized communities, the poor, the elderly, and children).

FTC rules should incentivize due diligence and harm reduction strategies throughout the lifecycle of an ADS, beginning with its design and through implementation. At the same time, the FTC should not adopt rules that are too prescriptive about technology design. Prescriptive limitations on the use of specific systems are likely to become over- or under-inclusive due to the speed of technology development. On the other hand, rules that encourage or mandate disclosure about ADS design, risk assessment, and risk mitigation are likely to reduce the risk profile of evolving ADS. Such rules are also likely to create harm-prevention reflexivity within both the ADS development and deployment sectors.

Other jurisdictions have already adopted a harm-prevention approach, especially for public entities. For example, the Canadian federal government's Treasury Board of Canada Secretariat issued a directive on ADS[119] and implemented an Algorithmic Impact Assessment questionnaire for federal procurement to help government agencies "assess and mitigate the impacts associated with deploying an automated decision system."[120] The UK has adopted a draft algorithmic transparency standard that prompts all agencies using ADS to evaluate and disclose the potential for harm.[121]

---

[117] *See, e.g.,* Decision and Order at 4–5, Everalbum, Inc., 2021 WL 118892 (F.T.C. Jan. 11, 2021), https://www.ftc.gov/system/files/documents/cases/everalbum_order.pdf; *see also* Final Order at 4, Cambridge Analytica, LLC, F.T.C. File No. 1823107 (F.T.C. Dec. 6, 2019), https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_orderpublic.pdf.

[118] NIST, *AI Risk Management Framework: 2nd Draft*, Aug. 18, 2022, https://www.nist.gov/itl/ai-risk-management-framework.

[119] Government of Canada, Directive on Automated Decision Making, R.S.C. 1985, c F-11 (Can.).

[120] *Algorithmic Impact Assessment*, Gov't. Of Can. (Mar. 22, 2021), https://open.canada.ca/aia-eia-js. *See generally*, Teresa Scassa, *Administrative Law and the Governance of Automated Decision Making: A Critical Look at Canada's Directive on Automated Decision Making*, 54 U.B.C. L. Rev. 251 (2021) (critiquing Canada's Directive on Automated Decision Making).

[121] UK Government, *UK Government Publishes Pioneering Standard for Algorithmic Transparency*, Central Digital and Data Office, Press Release (Nov. 29, 2021), https://www.gov.uk/government/news/uk-government-publishes-pioneering-standard-for-algorithmic-transparency.

Another set of regulatory approaches jurisdictions around the world, including U.S. states, are incorporating ADS regulation into data governance or data privacy regulation. That is the approach of the EU's GDPR, which regulates ADS to the extent that protected data is involved. Article 22 gives data subjects the right not to be subject to "solely automated" decisions if they produce "legal effects" for that person or "significantly affect" them.[122] GDPR places certain restrictions on the use of some kinds of personal data in ADS, such as race or ethnic origin[123] and it requires that data subjects be notified of ADS, including "meaningful information about the logic involved, as well as the significance of the envisaged consequences of such processing for the data subject."[124] Brazil's Lei Geral de Proteção de Dados takes a similar data protection approach to ADS regulation.[125] The new California Privacy Protection Agency is adopting regulations "governing access and opt-out rights with respect to businesses' use of automated decision-making technology," including providing meaningful information about the logic of the decision and the likely outcome with respect to the consumer.[126] Colorado,[127] Virginia,[128] and Connecticut[129] state privacy laws also each address ADS and give individuals information about and rights to opt out of ADS in certain circumstances.

The FTC should study the impact of these data protection approaches on ADS harm reduction. If they are positive, that sort of approach—yoking ADS regulation to data protection regulation—might be a promising avenue for rulemaking.

(v) Discrimination based on Protected Categories

(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)?

The FTC's approach to harms raised by commercial surveillance should be comprehensive and, as much as possible, avoid sectoral divisions that may prove to be underinclusive and age poorly. As an inherent component of that comprehensive approach, the FTC should incorporate heightened protections for protected classes as warranted to address particular vulnerabilities of those classes.[130] The Biden Administration has indicated that, for example, when addressing the

[122] Regulation 2016/679 2016 O.J. (L 119) 1 (EU), Art. 22. The European Data Protection Board has interpreted Article 22 to prohibit ADS processes, unless it is authorized by applicable law; is necessary for entry into or performance of a contract; or is based on the data subject's "explicit consent." https://ec.europa.eu/newsroom/article29/items/612053/en.
[123] Art. 22(4).
[124] Art. 13(2)(f), 15(1)(h).
[125] Government of Brazil, Lei Geral de Proteção de Dados, Law. No. 13,709, Aug. 14, 2018, https://lgpd-brazil.info.
[126] California Civil Code, § 1798.185(a)(16); California Privacy Protection Agency, Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01-21), Sept. 22, 2021.
[127] Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1306(3) (2021).
[128] Virginia Consumer Data Privacy Act, Va. Code § 59.1-577(C) (2021).
[129] Connecticut Data Privacy Act, P.A. 2215 (2022).
[130] *See, e.g.*, Turner Lee et al., *supra* n. 109; Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of the 1st Conference on Fairness,

impact of discriminatory algorithmic decision-making systems, it is essential that protected classes receive sufficient safeguards to ensure that these systems do not work against them.[131]

In evaluating and addressing harms to groups that are particularly vulnerable, the FTC should also contemplate the impact to groups outside of protected categories. For example, federal and state laws generally do not consider people who experience poverty a class protected from discrimination.[132] Yet, those who are low-income may be victims of significant discriminatory "targeting, exclusion, and surveillance" as a result of their socioeconomic status—in part precisely because the legal system does not afford them similar protection as members of protected categories, and responses to systematic discrimination may not always cover the specific impact to those groups.[133] Furthermore, commenters during NTIA's December 2021 listening sessions on privacy, equity, and civil rights raised concerns about the disproportionate harm that data collection and processing can have on historically marginalized and excluded communities, including those outside of officially protected classes, such as people who receive public benefits, unhoused people, sex workers, and "gig" or contract workers.

Therefore, NTIA urges the FTC, as part of a comprehensive approach to address the difficult issues raised by commercial surveillance practices, to work to mitigate harms to vulnerable groups, whether or not they are recognized as protected classes under the law. This should be done in acknowledgement of the complex intersectional nature of marginalized identities (that is, understanding that individuals may identify simultaneously with several protected and non-protected groups) and in light of the potentially mutable nature of group affiliation.

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

As noted in our executive summary and throughout this comment, NTIA supports the promulgation of trade regulations that provide comprehensive limitations and protections on commercial surveillance practices, with heightened protections where warranted—for example, by considering the particular needs of marginalized or vulnerable populations. Given the increasing complexity of algorithmic decision-making systems and their ubiquity in everyday life, NTIA believes that restrictions on discrimination based on protected categories can ultimately improve the transparency, reliability, and fairness of how such systems operate for all individuals, as well as for members of protected categories. New requirements that make businesses more conscientious of how their automated decision-making systems function, add or

---

Accountability and Transparency, in Proceedings of Machine Learning Research 81:77-91 (2018), https://proceedings.mlr.press/v81/buolamwini18a.html; James A. Allen, *The Color of Algorithms: An Analysis and Proposed Research Agenda for Deterring Algorithmic Redlining*, 46 Fordham Urb. L.J. 219 (2019), https://ir.lawnet.fordham.edu/ulj/vol46/iss2/1; Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR 8280 NIST (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[131] The White House, *Readout of White House Listening Session on Tech Platform Accountability*, *supra* n. 6.

[132] *See* Michele E. Gilman, *Expanding Civil Rights to Combat Digital Discrimination on the Basis of Poverty*, (May 10, 2022), at 2, SMU Law Review (forthcoming), Univ. of Baltimore Sch. of Law, Legal Studies Research Paper https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105801.

[133] *See generally, id*.

substitute human review for decisions that provoke the greatest concerns, and other mechanisms to improve transparency and due process will help mitigate all kinds of erroneous and undesirable automated outcomes, not only those directly affected by biased data or models.

Automated decision-making systems theoretically promise more fairness and equity by eliminating or mitigating human bias.[134] While much of the discussion of the effectiveness and fairness of algorithmic decision-making systems correctly focuses on the impact to members protected categories, the use, results, and impacts of these systems is not just limited to members of those groups. For example, individuals who are not members of a protected category may experience incorrect assessments or results made on faulty or inaccurate data, which can lead to unexpected but drastic and burdensome consequences even on relatively simpler algorithmic models.[135] Moreover, even when algorithmic decision-making systems have a specific, ascertainable discriminatory impact (typically, but not necessarily, against a protected category), their use may also impart broader, systemic harms detrimental to society as a whole—for example, by helping promote mis- and disinformation and inhibiting greater competition in the digital environment.[136] As methods to effectively evaluate algorithmic systems for equity and fairness continue to develop,[137] trade regulations that address how algorithmic decision-making systems discriminate against members of protected categories can benefit all consumers. Trade

---

[134] *See, e.g.*, Ifeoma Ajunwa, *The Paradox of Automation as Anti-Bias Intervention*, 41 Cardozo L. Rev. 1671, 1673 n.1 (2020), http://cardozolawreview.com/wp-content/uploads/2020/10/1.-Ajunwa.41.5.6.FINAL-3.pdf ("Algorithms or automated systems are often seen as fair because they are 'claimed to rate all individuals in the same way, thus adverting discrimination.'"), *citing* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash L. Rev. 1, 4 (2014). Indeed, some have argued that, provided the right legal and regulatory system, algorithmic systems themselves could potentially be tailored and serve to better detect discrimination. *See, e.g.*, Jon Kleinberg et al., *Algorithms as Discrimination Detectors*, 117 PNAS 48 (2020), https://www.pnas.org/doi/full/10.1073/pnas.1912790117; Jon Kleinberg et al., *Discrimination in the Age of Algorithms*, 10 J. Legal Analysis 113 (2019), https://academic.oup.com/jla/article/doi/10.1093/jla/laz001/5476086.

[135] *See, e.g.*, Eileen Guo & Karen Hao, *This is the Stanford Vaccine Algorithm That Left Out Frontline Doctors*, MIT Technology Review (Dec. 21, 2020), https://www.technologyreview.com/2020/12/21/1015303/stanford-vaccine-algorithm.

[136] *See* Rebecca Kelly Slaughter et al., *supra* n. 90; *see also* Kristine Phillips and Brian Fung, *Facebook Admits Social Media Sometimes Harms Democracy*, The Washington Post (Jan. 22, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/01/22/facebook-admits-it-sometimes-harms-democracy ("In recent months, the company has admitted, using internal research as well as academic reports, that consuming Facebook passively tends to put people in a worse mood. On the heels of that analysis, Facebook last week announced major changes to its algorithm that will reduce the presence of companies and brands on the platform in a bid to restore a focus on human relationships.") (internal hyperlink omitted).

[137] *See, e.g.*, Chelsea Barabas et al., *Studying Up: Reorienting the Study of Algorithmic Fairness Around Issues of Power*, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency 167, 168 (2020), https://doi.org/10.1145/3351095.3372859 ("To grapple with the full social and ethical implications of data-intensive algorithmic systems, we must develop more robust methodological frameworks that enable data scientists to reflect on how their research practices and design choices influence and distort the insights generated from their work."); Shea Brown et al., *The Algorithm Audit: Scoring the Algorithms that Score Us*, 8 Big Data & Society 1 (Jan. 2021), https://doi.org/10.1177/2053951720983865. *See also* Solon Barocas et al., *Designing Disaggregated Evaluations of AI Systems: Choices, Considerations, and Tradeoffs*, Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society at 368 (2021), https://doi.org/10.1145/3461702.3462610 (discussing how AI system design choices influences results and choices that will be obtained); Kenneth Holstein et al, *Improving Fairness in Machine Learning Systems: What do Industry Practitioners Need?*, Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems at 1 (2019), https://doi.org/10.1145/3290605.3300830.

regulations that respond to discrimination against members of protected categories should be seen as an inherent component of, not as a substitute for, a regulatory approach that is comprehensive and serves everyone.

(vi) Consumer Consent

(73) The Commission invites comment on the effectiveness and administrability of consumer consent to companies' commercial surveillance and data security practices. Given the reported scale, opacity, and pervasiveness of existing commercial surveillance today, to what extent is consumer consent an effective way of evaluating whether a practice is unfair or deceptive? How should the Commission evaluate its effectiveness?

In the case of commercial surveillance practices, consent will rarely, if ever, serve as a reliable indication of a consumer's informed acceptance of risks that consumer protection experts deem normatively tolerable, and should not be used as a sole or primary support for the legitimacy of a trade practice.

The inability of consent to reliably communicate informed acceptance is directly relevant to analysis of consumer behavior in connection with a potentially deceptive trade practice. As discussed in answers to other questions, individuals face too many data collection and use decisions each day to devote the necessary time to understand the relevant risks, and the risks are rarely disclosed in a manner conducive to the reader's informed evaluation, whether due to vague and opaque descriptions of relevant practices, or the underlying complexity of the risks being described. Even if those risks were sufficiently disclosed, many privacy risks are diffuse and attenuated to a degree that the human brain is cognitively disposed to evaluate them inaccurately.[138] In cases where individuals do reach the decision that a given service or product would create greater risks or harms than benefits, an alternative service or product often does not exist or is highly impracticable to identify and use.[139] Under these conditions, the approach of the reasonable consumer is to provide consent when requested by a digital product or service, and to move on with one's day.

Resignation to privacy invasions is also relevant to an evaluation of reasonableness.[140] Becoming accustomed to a lack of control over one's information can produce an expectation of powerlessness that should not be interpreted as the unreasonable failure of a consumer to

---

[138] *See* Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting*, in Economics Of Information Security 165, 172–73 (L. Jean Camp & Stephen Lewis eds., 2004) (describing "bounded rationality," or limitations on the ability of individuals to accurately evaluate risk in complex scenarios such as the potential harms of consenting to data collection; "hyperbolic discounting," or the human tendency to favor immediate gratification and underestimate the impact of remote risks; and explaining the role of both cognitive phenomena in undermining the ability of individuals to accurately evaluate the potential harms of privacy decisions.)

[139] *See, e.g.*, Kashmir Hill, *I Cut the 'Big Five' Tech Giants from My Life. It Was Hell*, Gizmodo (Feb. 7, 2019), https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194 (documenting the difficulty of finding alternatives for the wide array of commonly-used consumer services offered by Apple, Google, Microsoft, and Amazon).

[140] Solove, *supra* n.25 at 45-49 (describing how the demands on individuals to manage their own privacy risks and the futility of their efforts can produce resignation to privacy invasions and summarizing relevant literature).

evaluate a transaction, but the unsurprising result of an ecosystem that has incentivized complex and ubiquitous data collection practices.

Similarly, the limited efficacy of consent in the modern data ecosystem should be appropriately accounted for in evaluations of unfair trade practices. The expectation that "consumers will survey the available alternatives, choose those that are most desirable, and avoid those that are inadequate or unsatisfactory"[141] is repudiated by a market distorted by information asymmetries and lack of consumer choice.

(79) To what extent should new trade regulation rules prohibit certain specific commercial surveillance practices, irrespective of whether consumers consent to them?

It is a basic consumer protection principle that certain transactional conditions are coercive enough, exist within a sufficiently asymmetrical imbalance of power, and have a sufficient likelihood of injury to the less powerful party that interpreting that party's consent to the transaction as anything other than the product of those circumstances would legitimize predation.[142] This principle should certainly apply to particularly concerning commercial surveillance practices, such as harmful practices that individuals cannot avoid, or those that accompany services for which an individual has no reasonable alternative. The Commission should evaluate what kinds of commercial surveillance practices might be noxious enough to warrant prohibition regardless of whether or not consumers consent to them.

Factors that could inform the identification of such practices might include the severity of the potential harm for individuals, including physical or financial injury, acute mental distress or anxiety, or substantially increased risk of those harms. An example of a corresponding practice would be the facile collection or sharing of location information, as it can enable stalking.[143] Another factor might be whether the potential harm is more prevalent or more severe among members of a protected class, such as a racial minority group. The use of facial recognition technologies could merit scrutiny on that basis, given repeated demonstrations of higher error rates for people of color (particularly Black and Indigenous communities).[144] An additional factor could be whether the potential harm could limit access to a protected right, such as

---

[141] *See*, *e.g. Letter to Senators Ford and Danforth* (Dec. 17, 1980), https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness.
[142] *See*, *e.g. id.* ("[I]t has long been recognized that certain types of sales techniques may prevent consumers from effectively making their own decisions, and that corrective action may then become necessary.").
[143] *See, e.g.,* Warzel and Thompson, *supra* n. 56.
[144] NIST, *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 [https://perma.cc/A3CD-K624]; Joy Buolamwini and Timnit Gebru, *supra* n. 130; Inioluwa Raji and Joy Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*, Proceedings of the 2019 Conference on AI, Ethics, & Society 1- 5, https://dl.acm.org/doi/10.1145/3306618.3314244; Joy Buolamwini, *When the Robot Doesn't See Dark Skin*, N.Y. Times (June 21, 2018), https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html [https://perma.cc/CZ32-ERFJ]; Os Keyes, *supra* n. 72.

targeting people seeking information about how to exercise their right to vote or obtain reproductive care with misinformation intended to stymie their efforts.[145]

Other factors might include whether the method of obtaining consent provided individuals with clear and meaningful information in an accessible location and format, or if consent to an invasive practice was required to use the rest of the service, descriptions of the collection and use practices are not available in the languages spoken in areas where the company does business, or made available in an impracticable format for the product or service, such as a device with a tiny interface; and whether an individual had a meaningful alternative to the service, where the alternative is not burdensome or punitive to exercise.

Given the demonstrable deficits of consent as an indication of informed acceptance of appropriate risks, the Commission should not take the presence of consent to a practice as reliable evidence that it is normatively desirable, nor as persuasive evidence against a finding that a company's practices are deceptive or unfair. While determining the best approach to these questions will require a careful inquiry into complex and nuanced questions, it is certainly an endeavor worthy of the Commission's attention.

(vii) Notice, Transparency, and Disclosure

(c) What Should Companies Provide Notice of or Disclose?

(93) To what extent do companies have the capacity to provide any of the above information? Given the potential cost of such disclosure requirements, should trade regulation rules exempt certain companies due to their size or the nature of the consumer data at issue?

As has been broadly acknowledged throughout recent discussions of domestic privacy reforms, small businesses often lack the resources to hire compliance lawyers or to expand the responsibilities of other employees to adapting their business practices to new legal responsibilities.[146] Complex or novel compliance questions demand additional time and expertise that is harder to locate and retain. The Biden administration is deeply committed to ensuring that its consumer protection efforts keep the needs of small businesses in mind, in keeping with its

[145] Consider advertisements targeted to individuals who searched for voter registration deadlines or identification requirements for websites with false information intended to prevent them from registering correctly, or advertisements targeted to people seeking abortions for websites that attempt to direct them to crisis pregnancy centers in the guise of providing the care they seek. *See generally,* Jennifer Korn, *Facebook and TikTok are approving ads with 'blatant' misinformation about voting in midterms, researchers say*, CNN Business (Oct. 21, 2021), https://www.cnn.com/2022/10/21/tech/facebook-tiktok-misinfo-ads/index.html; Justin Sherman, *The Data Broker Caught Running Anti-Abortion Ads—to People Sitting in Clinics*, Lawfare (Sept. 19, 2022), https://www.lawfareblog.com/data-broker-caught-running-anti-abortion-ads%E2%80%94-people-sitting-clinics.

[146] *See, e.g.*, Testimony of Even Engstrom, Executive Director, Engine Advocacy and Research Foundation, Senate Commerce, Science & Transportation Committee, Subcommittee on Manufacturing, Trade, and Consumer Protection (Mar. 26, 2019), https://www.commerce.senate.gov/services/files/949F1FC8-DC28-4760-9F47-6CB925A1549E; Business Roundtable, *Framework for Consumer Privacy Legislation* https://s3.amazonaws.com/brt.org/privacy_report_PDF_005.pdf ("Care should be given to how or if small companies that do not process much personal data or engage in low risk processing of data should be covered, with consideration of how those companies may be covered under existing law.").

commitment to promoting greater competition in consumer technology services and other industries.

At the same time, concerns raised about small businesses throughout consumer privacy reform discussions have not always been very specific, which complicates efforts to evaluate or address them. The viability of small businesses is important for a healthy, competitive economy, but policy choices intended to promote their success should not ignore that small businesses can still engage in harmful data practices. With those considerations in mind, the FTC should examine the threshold assumptions and criteria underlying any proposals designed to promote competition by shielding small businesses from undesirable compliance burdens. Important areas of focus could include the basis for popular size thresholds chosen for lessened compliance obligations; the relative efficacy of drafting choices intended to mitigate undesirable burdens for small businesses, such as longer periods before particular provisions enter into force, the opportunity to cure a first-time offense, specific guidance resources, or free access to counsel; what data is available to support analysis of these questions with appropriate rigor; and what data is still needed.

The Commission should also consider how competition objectives can be served by certain privacy reforms (as discussed elsewhere in these comments). It would belie the purpose of consumer protection reforms to enact new rules that assumed that small businesses cannot engage in undesirable privacy practices, or that the consumer harms that result do not merit redress due to the size of the business that caused them.

Certain modifications to how new trade regulation rules treat businesses of a sufficiently small size could prevent undesirable obstacles for small businesses and competition without unduly hampering the efficacy and coherence of the new rules. Such a balance will require a careful, transparent, and rigorous accounting for the size parameters that would qualify a business for such modifications and analysis of those modifications would be effective. Enforcement discretion will also play an important role, and is likely to serve as a natural protection for the important public policy goal of avoiding creating impracticable compliance requirements for small businesses while protecting privacy.

(94) How should the FTC's authority to implement remedies under the Act determine the form or substance of any potential new trade regulation rules on commercial surveillance? Should new rules enumerate specific forms of relief or damages that are not explicit in the FTC Act but that are within the Commission's authority? For example, should a potential new trade regulation rule on commercial surveillance explicitly identify algorithmic disgorgement, a remedy that forbids companies from profiting from unlawful practices related to their use of automated systems, as a potential remedy? Which, if any, other remedial tools should new trade regulation rules on commercial surveillance explicitly identify? Is there a limit to the Commission's authority to implement remedies by regulation?

The FTC should explicitly include algorithmic disgorgement in its rules and consider what other creative strategies it might employ to divest companies engaged in unfair or deceptive practice of ill-gotten gains.

Reorienting current incentives in the digital ecosystem that promote pervasive data collection should be a key goal of the Commission's trade regulation rules, and algorithmic disgorgement addresses a significant problem in a machine-learning-driven tech sector: if a company is found to have obtained consumer data through unfair or deceptive means, how can the FTC sufficiently ensure that such data does not enable future profit?[147] Once data has been processed and insights derived from it, limiting further use of the data without also limiting use of the algorithm would have minimal effect.[148] Consider a company that illegally obtained a competitor's blueprint for a new product mold and was required to turn over the products it had already made, but not the mold it created from the stolen blueprint, or any subsequent products the mold created—the company would forfeit the most immediate benefits of its wrongdoing, but not the long-term and ongoing benefits to come. If the FTC determines that a company trained a machine-learning algorithm through the use of unfair or deceptive trade practices, appropriate remedies might include ordering the destruction of the data obtained to train the model, the data the model produced, the model itself, and any subsequent algorithms produced from those materials.

The FTC needs to draw clear lines around the application of such a rule, and how it would affect third parties (e.g., if improperly collected data were sold or shared with a third party for the development of an algorithm, would they then also be required to delete these derived algorithms, even if done in good faith).[149] But these issues can be thoughtfully addressed, and should not present insurmountable obstacles to the use of algorithmic disgorgement as a remedy.

Should limitations to the Commission's authority to require algorithmic disgorgement or other important remedies be identified,[150] these limitations should be carefully considered by Congress as potential areas for legislative reform. These might include constraints on the Commission's ability to take law enforcement action against harmful practices, including by obtaining monetary relief with a meaningful deterrent value or making the victims of damaging data practices whole. Congress could adopt legislation that would complement and clarify existing law, such as by codifying particular practices as unfair and/or deceptive and giving the FTC APA rulemaking authority. Such legislation could augment the FTC's powers to challenge conduct

---

[147] More deftly put, "[t]his innovative enforcement approach should send a clear message to companies engaging in illicit data collection in order to train AI models: Not worth it." Rebecca Kelly Slaughter et al., *supra* n. 90.

[148] Tiffany Li, *Algorithmic Destruction*, Southern Methodist University Law Review (*forthcoming* 2022 http://dx.doi.org/10.2139/ssrn.4066845 (describing the FTC's use of algorithmic disgorgement as a remedy, situating it in the FTC's previous use of non-algorithmic disgorgement remedies prior to its consent orders with WW International, Inc./Kurbo, Inc. and Everalbum, Inc., and noting that algorithmic disgorgement would prevent unjust enrichment more effectively than data deletion orders alone).

[149] *Id.*, at 23-4 (describing complexities inherent to some algorithmic disgorgement remedies); Protocol Enterprise Team, *How to Kill an Algorithm,* Protocol (March 17, 2022), https://www.protocol.com/newsletters/protocol-enterprise/ftc-algorithmic-disgorgement-japan-chips?rebelltitem=3#rebelltitem3 (same).

[150] *See, e.g.* Prepared Statement Of The Federal Trade Commission, *The Urgent Need To Fix Federal Trade Commission: Section 13(B) Of The FTC Act Before The Committee On Energy And Commerce Subcommittee On Consumer Protection And Commerce* (April 27, 2021), https://www.ftc.gov/system/files/documents/public_statements/1589400/p180500house13btestimony04272021.pdf; FTC, *FTC Report to Congress on Privacy and Security* (Sept. 13, 2021), at 10, https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf.

efficiently and effectively. And it could give the FTC the ability to adopt rules more quickly than the FTC's current general powers allow. In addition, Congress could re-evaluate some restrictions on the FTC's authority in cases where the utility of such restrictions has been undermined by technological developments, such as the exclusion of common carrier activity from the FTC Act.

Respectfully submitted,

Alan Davidson

Assistant Secretary of Commerce for Communications and Information and NTIA Administrator

National Telecommunications and Information Administration
1401 Constitution Avenue, NW
Washington DC 20230
(202) 482-1816