How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking

January 26, 2022

Executive Summary

Unfair data collection practices and surveillance have eroded consumer privacy, and this ever present and unwanted observation constitutes a substantial injury to consumers. This paper argues that the Federal Trade Commission (FTC) should use its Section 5 unfairness authority to establish a Data Minimization Rule to prohibit all secondary data uses with limited exceptions, ensuring that people can safely use apps and online services without having to take additional action. It also lays out two additional options to consider should the FTC decline to prohibit all secondary uses: prohibit specific secondary data uses, such as behavioral advertising or the use of sensitive data; or mandate a right to opt out of secondary data use, including through global opt-out controls and databases.

Additionally, to supplement this Data Minimization Rule, the FTC should adopt data transparency obligations for primary use of data; civil rights protections over discriminatory data processing; nondiscrimination rules, so that users cannot be charged for making privacy choices; data security obligations; access; portability; correction; and deletion rights. In addition, the FTC should prohibit the use of dark patterns with respect to data processing.

The FTC has wide authority to issue prescriptive rules in order to forestall business practices that can cause consumer injury. With respect to judicial interpretation, the courts generally give broad deference to expert agencies' interpretation of their substantive statutes, and these privacy regulations are likely to withstand First Amendment scrutiny.

Table of contents

I. Introduction

In the absence of comprehensive privacy rules, the surveillance of internet users has become omnipresent over the last thirty years and the profiling, targeting, and monetizing of consumers' online behaviors has become endemic.[1] The Federal Trade Commission ("FTC" or "Commission") has explored this problem in numerous workshops and studies,[2] and the European Union (EU), through the General Data Protection Regulation (GDPR), and some states, such as California through the California Consumer Privacy Act (CCPA), have begun to establish baseline privacy protections.[3] Those protections, however, are largely procedurally focused, with far too little substantive protection. Crucially, there is no comprehensive federal privacy law in the United States that allocates responsibilities with respect to user data, restricts data collection and use, or establishes standards for data security, access, or accountability. The FTC has brought a number of important privacy enforcement actions against companies for violating general purpose consumer protection law or sectoral privacy legislation, but those actions have not been successful in comprehensively reforming industry practices. The President of the United States recently emphasized the need for federal guidelines to rein in data collection, use, and disclosure: His executive order encouraged the FTC to pursue a rulemaking to address "unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy."[4]

To address unfair surveillance and data collection practices that endanger consumer privacy and autonomy, it is necessary to limit wide scale tracking and profiling of consumers online. One of the core principles underlying modern privacy and data protection laws, the data minimization principle, provides that data should only be collected, used, or disclosed as reasonably necessary to provide the service requested by a consumer. People should be able to use the internet and apps, including for work and school, with their privacy protected by default. They should be able to take advantage of new technologies and services without fear that their choices and behaviors will be logged and tracked by other companies or used against

---

[1] Kaveh Waddell, *California Privacy Law Prompts Companies to Shed Consumer Data*, Consumer Reports (Feb. 11, 2020), https://www.consumerreports.org/privacy/california-privacy-law-ccpa-prompts-companies-to-shed-consumer-data/.

[2] *See, e.g.*, *Protecting Consumers in the Next Tech-ade: A Report by the Staff of the Federal Trade Commission*, Fed. Trade Comm'n (Mar. 2008), http://www.ftc.gov/os/2008/03/P064101tech.pdf*; Self-Regulatory Principles For Online Behavioral Advertising, Behavioral Advertising Tracking, Targeting, & Technology,* Fed. Trade Comm'n Staff Report (Feb. 2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf; *Protecting Consumer Privacy in an Era of Rapid Change: A Framework for Businesses and Policymakers*, Fed. Trade Comm'n (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[3] Regulation (EU) 2016/679 (General Data Protection Regulation), https://gdpr-info.eu/; Cal. Civ. Code § 1798.100 et seq.

[4] Executive Order on Promoting Competition in the American Economy (July 9, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/.

their interests. As the FTC begins to consider potential privacy rules in response to the President's executive order, it should prioritize restrictions that address and limit data collection as well as secondary uses and disclosure of the data that is amassed and stored.

This paper argues the FTC should promulgate a Data Minimization Rule under the unfairness prong of Section 5 to regulate secondary data processing. We present three different possible approaches for how the FTC could draft such a rule, and provide legal justification, as well as the policy considerations, for each path:

- Prohibit all secondary data uses with limited exceptions;
- Prohibit specific secondary data uses, such as behavioral advertising or the use of sensitive data; or
- Mandate a right to opt out of secondary data use, including through global opt-out controls and databases.

Of these options, we believe that the first — prohibiting secondary use with narrow carveouts — would be the most effective in safeguarding consumers' expectations and fundamental right to privacy. However, we also offer alternative paths that, while less expansive, could still offer robust protections to consumers without constantly burdening them with privacy choices and consent requests.

In addition, we propose that the FTC draft additional rules for consumers, consistent with the Fair Information Practices Principles, to better ensure data privacy and security. These provisions could be formulated in tandem with a Data Minimization Rule, or as part of separate proceedings:

- Establish data transparency obligations for primary use of data;
- Establish civil rights protections over discriminatory data processing;
- Establish nondiscrimination rules, so that users cannot be charged for making privacy choices;
- Establish data security obligations;
- Secure access, portability, correction, and deletion rights over data collected about a consumer; and
- Prohibit the use of dark patterns around data processing.

The FTC has over the last twenty years exercised regulatory authority under Section 5 of the FTC Act to limit unfair and deceptive privacy practices, but the Commission has not established comprehensive rules to prevent and limit privacy injuries. The FTC has ample authority to pursue such a rulemaking under Section 5. Courts have made clear that the FTC has broad authority to define unfair trade practices on a discretionary basis, and thus the power to address the substantial privacy harms caused by behavioral advertising and the related excessive collection, use, and disclosure of user data. In its privacy cases over the last twenty years, the FTC established that businesses can be liable when they collect, use, or disclose data in ways that exceed consumers' expectations. Further, recent FTC enforcement actions

highlight the breadth of privacy injuries that fall under the FTC's Section 5 authority. For example, the FTC's complaint and consent order with Zoom Video Communications showed that even potential exposure of personal data (and thus the risk of injury) can constitute a substantial injury, as can the circumvention of a platform's privacy settings.[5]

This paper will first discuss the problem to be solved — the wholesale erosion of privacy in recent years. It will then analyze the FTC's legal authority to issue regulations under its Section 5 unfairness authority. While the FTC has only used this authority sparingly, it has wide discretion in using this power to issue prescriptive rules to forestall business practices that can cause consumers substantial injury.

We then present the three potential options for a Data Minimization Rule to limit companies' secondary use of consumers' personal information, along with an analysis of how each could be justified under the FTC's Section 5 authority. Next, we discuss other attributes of privacy law and how they would be justified under unfairness as well. Finally, we discuss potential judicial review of FTC privacy rules, describing how the courts generally give broad deference to expert agencies' interpretation of their substantive statutes, and why privacy regulations are likely to withstand First Amendment scrutiny.

II. Problem Statement: Unwanted Surveillance Harms Consumers

Consumers are constantly tracked: online, through their use of apps, and in the physical world, via cameras and the like. This information reveals consumers' most sensitive characteristics, including health conditions, sexual orientation, sexual activities, gender, political affiliations, and union membership, and is transferred to hundreds, if not thousands, of different companies, typically without their knowledge or consent.[6] The current "notice and choice" regime, in which consumers are expected to read extensive privacy policies and make "all or nothing" decisions about whether to use an online service or app, makes it impossible for consumers to meaningfully participate in the market while protecting their privacy. Even if consumers had the time to read every privacy policy and statement, they would in most cases come away with woefully incomplete information. Such policies tend to be vague and expansive, designed to protect a company from liability rather than inform privacy-conscious consumers. In many cases, the companies themselves have not decided to whom data will be sold and the purposes for which it will be used. It is impossible for consumers to assess the cost of a loss of control over their personal information, or to determine a value and "trade" their data for goods or services.

Fundamentally, much data processing — notably much *secondary data processing*, or processing not directly in service of fulfilling a consumer's request — fundamentally violates consumers' right to privacy — the "right to be let alone," as articulated by Samuel Warren and

[5] Compl., *In the Matter of Zoom Video Communications, Inc.*, Comm'n File No. 1923167 (Nov. 9, 2020).
[6] *See, e.g.*, Letter from Access Now et al., to Chair Khan and Commissioners Chopra, Slaughter, Phillips, and Wilson (Aug. 4, 2021), https://www.lawyerscommittee.org/wp-content/uploads/2021/08/FTC-civil-rights-and-privacy-letter-Final-1.pdf.

Louis Brandeis.[7] This concept has been incorporated into federal privacy laws like the Privacy Act of 1974. It has been further developed by scholars, including Helen Nissenbaum, who has argued that much data disclosure and secondary use betrays the original purpose of the collection and expectations of individuals, which she describes as *contextual integrity*. Indeed, intrusion upon seclusion has long been recognized as a privacy tort, and consumers will always have a legitimate interest in constraining unnecessary processing of their data.

As such, rather than focus entirely on specific injuries tied to the collection and use of data, the FTC should recognize that the unwanted observation, through excessive data collection and use, is harmful in and of itself. It necessarily subjects consumers to the risk of data breaches, employee misuses, unwanted secondary uses, inappropriate government access, and can have a chilling effect on consumers' willingness to adopt new technologies, and to engage in free expression.[8] Privacy scholars Danielle Citron and Daniel Solove have identified myriad privacy harms that go beyond economic and physical harm that stem from secondary data processing, including psychological harms, reputational damage, and restricting or unduly influencing consumers' choices.[9] Given companies' strong incentives to continue to freely collect data, self-regulation has not been and will never be sufficient to protect consumers against these harms. And with the ever-growing sophistication of technology, without policy intervention, unwanted, unexpected, and ultimately disadvantageous (to individuals) surveillance will only become more widespread.

The tracking implemented by platforms like Google and Facebook is not technically necessary to rendering services, and it assaults long-held norms surrounding privacy. For instance, letter writing has long been a private activity, protected by law. Americans have a legally protected interest in the confidentiality of their postal mail and their telephonic conversations. Google's implementation of email, however, sought to track both content and the identity of communicating parties in a way that would violate criminal statutes if performed in the postal mail or telephone. For another example, consider search: the librarian who would assist a patron in finding information owed a duty of confidentiality to the patron and could not retain transactional records of book borrowing. Google's implementation of search turns this on its head, making information retrieval a commercial transaction, even where the user seeks knowledge of medical conditions.

At a time where it often feels like the country is deeply divided on policy issues, polls repeatedly show that Americans are unified on privacy. In a survey recently conducted by the Future of Technology Commission, a staggering eighty-six percent agreed that "it should be illegal for private companies to sell or share information about people no matter what" and only forty-six percent agreed that it would be okay for companies to "sell consumers' data as long as

---

[7] Samuel Warren and Louis Brandeis, *The Right to Privacy*, Harvard L. Rev. IV (5): 193–220 (Dec. 15, 1890), https://archive.org/details/jstor-1321160/page/n1/mode/2up.
[8] Justin Brookman and G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, https://cdt.org/wp-content/uploads/2018/08/September-2013-Brookman-Hans-Why-Collection-Matters.pdf
[9] Danielle Keats Citron and Daniel Solove, *Privacy Harms*, GWU Legal Studies Research Paper No. 2021-11 (Feb. 2021), https://ssrn.com/abstract=3782222.

they are transparent about how the data is used and make it clear to consumers."[10] Americans don't want companies to put more disclosures in privacy policies, they want them to stop trafficking in personal data. And the number of consumers, and the amount of personal information, implicated by companies' data practices is staggering. 90% of consumers reported that the internet has been either "essential or important" to them during the first year of the Covid-19 crisis and associated lockdowns.[11] The average consumer spends nearly seven hours online each day.[12] According to a recent FTC report, one ISP alone has 370 million consumer relationships (compared to a US population of nearly 330 million).[13] Yet another ISP, according to the report, served one trillion ad requests each month.[14]

The risk of security incidents and breaches is amongst the strongest rationales for limiting unnecessary collection of personal information. Security incidents and breaches[15] are commonplace. As former FBI Director Robert S. Mueller quipped, "There are only two types of companies: Those that have been hacked and those that will be hacked." What this means is that companies that collect personal information routinely fail to live up to their security responsibilities and allow information to be acquired by hackers and hostile governments. In many cases, this information is not only stolen by hackers, but also uploaded to Torrent files, where they are available to anyone. Constella Intelligence found evidence of over 8,500 separate breaches — concerning 12 billion records — circulating on dark web services in 2020.[16]

Because companies routinely fail to implement even basic security precautions (despite legal obligations to do so), and because even sophisticated technical powerhouses such as Google fall victim to intrusions[17] that result in total collapse of confidentiality, companies collect data at the peril of the consumer. Companies enjoy the benefit of data collection activities while externalizing the costs of insecurity. Furthermore, consumers have no ability to evaluate

---

[10] Benson Strategy Group, *Future of Tech Commission: Tech Attitudes Survey (July 20, 2021 - July 29, 2021)*, https://d2e111jq13me73.cloudfront.net/sites/default/files/uploads/pdfs/bsg_future_of_technology_topline_c1-1.pdf.

[11] Colleen McClain et al., *The Internet and the Pandemic*, Pew Research Ctr. (Sept. 1, 2021), https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/.

[12] Simon Kemp, *Digital 2021 April Global Statshot Report*, Data Reportal (Apr. 21, 2021), https://datareportal.com/reports/digital-2021-april-global-statshot.

[13] *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers: An FTC Staff Report*, Fed. Trade Comm'n at 33 (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.

[14] *Id.*

[15] *See* Mahmood Sher-Jan**,** *Is it an incident or a breach? How to tell and why it matters,* IAPP (Feb. 28, 2017), https://iapp.org/news/a/is-it-an-incident-or-a-breach-how-to-tell-and-why-it-matters/ These are two distinct kinds of spills of personal information. Security incidents are revelations of user information that do not require notice to users and regulators. Security breaches are those incidents that require notice under state laws and other regulations.

[16] *2021 Identity Breach Report*, Constella Intelligence at 5, https://info.constellaintelligence.com/2021-identity-breach-report.

[17] *See* Nicole Perlroth, *This Is How They Tell Me The World Ends: The Cyberweapons Arms Race* (2021) (describing the "Aurora" hack).

security practices of companies and no defenses against hacks and dumps of their personal information. The most efficacious countermeasure for this peril is the limitation of how much and what data may be collected.

For these reasons, it is essential that the FTC pursue a privacy rulemaking to establish meaningful data minimization. Below, we outline the FTC's authority to pursue such a rule, lay out three possible approaches to minimizing data processing, and discuss key additional protections, such as transparency obligations for primary data use; civil rights protections; non-discrimination to prevent charging consumers for exercising their privacy rights; data security, access, portability, correction and deletion rights; and a prohibition on dark patterns.

III. The FTC's Authority to Promulgate Unfair Trade Practices Rules

The Federal Trade Commission is broadly charged with prohibiting unfair trade practices, which include "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[18] "Unfair methods of competition" and "unfair or deceptive acts and practices" are separate legal authorities; while the FTC has traditionally viewed privacy issues through the lens of "unfair and deceptive," the FTC has in some ways broader (if untested) authority under "unfair methods of competition," including the ability to use Administrative Procedure Act rulemaking.[19] Last year, the advocacy group Accountable Tech filed a petition with the FTC asking the agency to ban surveillance advertising under its "unfair methods of competition" authority.[20] This paper focuses instead on the FTC's powers under "unfair and deceptive acts and practices," the traditional source of the FTC's privacy jurisprudence. Ultimately, however, our goal is to see the enactment of a robust Data Minimization Rule and related privacy protections; if the FTC decides it has a stronger case to justify such rules under "unfair methods of competition," we would strongly support such an effort.

Under its authority to prevent unfair and deceptive practices,[21] the Commission is specifically authorized to issue trade regulation rules "which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce[.]"[22] As will be discussed below, this rulemaking authority is more constrained than traditional APA rulemaking, but the FTC nonetheless has broad discretion to issue regulations that proscribe "prevalent" business practices that cause consumers significant injury. A violation of a trade regulation rule constitutes an unfair or deceptive act or practice unless the Commission provides otherwise in the rule.[23]

---

[18] 15 U.S.C. § 45(a)(1).
[19] Rohit Chopra and Lina Khan, *The Case for "Unfair Methods of Competition" Rulemaking*, 87 U Chi. L. Rev. 357 (2020).
[20] Accountable Tech, *Petition for Rulemaking to Prohibit Surveillance Advertising* (Sept. 28, 2021), https://accountabletech.org/wp-content/uploads/Rulemaking-Petition-to-Prohibit-Surveillance-Advertising.pdf [hereinafter Accountable Tech Rulemaking Petition].
[21] 15 U.S.C. § 45(a)(2).
[22] 15 U.S.C. § 57a(a)(1)(B).
[23] 16 C.F.R. § 1.8(a).

Congress has also charged the Commission with promulgating non-binding "interpretive rules and general statements of policy with respect to unfair or deceptive acts or practices in or affecting commerce" and also "rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce[.]"[24] Under Section 5(m)(1)(A) of the FTC Act, the FTC can pursue civil monetary penalties against any firm that knowingly violates a trade regulation rule with respect to unfair or deceptive acts or practices.[25] Finally, pursuant to its Penalty Offense Authority, the Commission may seek monetary penalties "against a party that engages in conduct it knows has been determined to be unlawful in a Commission order"[26] so long as the order is final and not a consent order.[27]

Below is a table of the FTC's authorities to promulgate unfair trade practice rules.

FTC's Authority	Legal Basis	Legal Effect
Unfair and Deceptive Practices ("UDAP") Power	The FTC is charged with prohibiting unfair trade practices, which include "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[28]	The Commission is empowered to prevent such practices.[29]
Trade Regulation Rules Power	The FTC is specifically authorized to issue trade regulation rules "which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce[.]"[30]	A violation of a trade regulation rule constitutes an unfair or deceptive act or practice unless the Commission provides otherwise in the rule.[31]
Authority of Commission to prescribe rules and general statements of policy	Congress has charged the Commission with promulgating "interpretive rules and general statements of policy with respect to unfair or deceptive acts or practices in or affecting commerce" and also "rules which define with specificity	"These guidance documents are not substantive rules and do not have the force or effect of law. They are administrative interpretations of the statutes and rules administered by the

[24] 15 U.S.C. § 57a(a)(1)(A)-(B).
[25] 15 U.S.C. § 45(m)(1)(A).
[26] Rohit Chopra & Samuel A.A. Levine, *The Case for Resurrecting the FTC Act's Penalty Offense Authority* (Oct. 29, 2020), 169 U. Pa. L. Rev. 1, 12-13 (forthcoming 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721256; *See* 15 U.S.C. § 45(m)(1)(B).
[27] 15 U.S.C. § 45(m)(1)(B).
[28] 15 U.S.C. § 45(a)(1)
[29] 15 U.S.C. § 45(a)(2).
[30] 15 U.S.C. § 57a(a)(1)(B).
[31] 16 C.F.R. § 1.8(a).

	acts or practices which are unfair or deceptive acts or practices in or affecting commerce[.]"[32]	Commission, and they are advisory in nature."[33]
Penalty Offense Authority	The Penalty Offense Authority "allows the Commission to seek penalties against a party that engages in conduct it knows has been determined to be unlawful in a Commission order[,]" so long as the order is final and not a consent order.[34]	"In order to trigger this authority, the Commission can send companies a 'Notice of Penalty Offenses.' This Notice is a document listing certain types of conduct that the Commission has determined, in one or more administrative orders (other than a consent order), to be unfair or deceptive in violation of the FTC Act. Companies that receive this Notice and nevertheless engage in prohibited practices can face civil penalties of up to $43,792 per violation."[35]
FTC Act Section 5(m)(1)(A) Authority	This authority allows the FTC to seek penalties against parties who have violated a Commission rule "with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule."	The FTC can pursue civil monetary penalties against any firm that knowingly violates a trade regulation rule with respect to unfair or deceptive acts or practices.[36]

The FTC is tasked with using these broad and flexible authorities to address emerging and evolving injuries. The FTC has historically brought most of its privacy cases under its *deception* authority; however, in such cases, the FTC must demonstrate that an offender misled consumers. As a result, companies are incentivized to not make affirmative privacy representations, leading to evasive privacy policies and other consumer-facing statements that provide consumers little concrete information. The FTC has wider authority to rein in bad privacy behaviors under its unfairness prong. Here the FTC Act provides that an act or practice is unfair

[32] 15 U.S.C. § 57a(a)(1)(A)-(B).
[33] *Guidance Documents*, Fed. Trade Comm'n, https://www.ftc.gov/enforcement/guidance.
[34] Chopra and Levine, *supra* note 26 at 12-13.
[35] *Notice of Penalty Offenses*, Fed. Trade Comm'n, https://www.ftc.gov/enforcement/penalty-offenses.
[36] 15 U.S.C. § 45(m)(1)(A).

when it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[37] Per the Ninth Circuit Court of Appeals, "In determining whether consumers' injuries were reasonably avoidable, courts look to whether the consumers had a free and informed choice."[38] But courts have made clear that the Commission's unfairness authority is not limited to "situations involving deception, coercion, or withholding of material information."[39]

Courts have had few opportunities to review the scope of FTC unfairness rules since the Commission issued its Policy Statement in 1980. Since its enactment, the FTC has promulgated only seven rules under Magnuson-Moss ("Mag-Moss") that are active today.[40] Though not used frequently, the Commission has previously promulgated an unfair practices rule to prevent optometrists from withholding contact lens and eyeglass prescriptions from patients, known as the "Eyeglass Rule."[41] The rule prohibits an ophthalmologist or optometrist from "Fail[ing] to provide to the patient one copy of the patient's prescription immediately after the eye examination is completed," from "[c]ondition[ing] the availability of an eye examination to any person on a requirement that the patient agree to purchase any ophthalmic goods from the ophthalmologist or optometrist," and from other related practices that deny the patient the ability to use their prescription in the best way they see fit.[42] This rule ensures that consumers can "comparison shop when buying prescription eyewear," and is not tied to any deceptive practice.[43] The FTC would similarly have the ability to promulgate rules that prevent online firms from subjecting consumers to unwanted tracking and behavioral advertising that would deprive them of the ability to use and enjoy internet services while maintaining their privacy.

In those few cases where courts have reviewed the scope of the FTC's unfairness authority, courts have made clear that Congress delegated "broad discretionary authority" to the Commission to "define unfair trade practices on a flexible, incremental basis."[44] Given its broad delegation of authority to define unfairness, the Commission has the power to address online data collection, tracking, profiling, and behavioral advertising practices that subject consumers

---

[37] 15 U.S.C. § 45(n).
[38] *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1158 (9th Cir. 2010), *as amended (*June 15, 2010); *See Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 976 (D.C. Cir. 1985).
[39] *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d at 978.
[40] Jeffrey S. Lubbers, *It's Time to Remove the "Mossified" Procedures for FTC Rulemaking*, 83 Geo. Wash. L. Rev. 1979, 1997 (2015); *See* Ophthalmic Practice Rules (Eyeglass Rule), 16 C.F.R. ch. I, subch. D, pt. 456 (1992; last amended 2004); *See* Labeling and Advertising of Home Insulation, 16 C.F.R. ch. I, subch. D, pt. 460 (1979; last amended 2019); *See* Credit Practices, 16 C.F.R. ch. I, subch. D, pt. 444 (1984); *See* Used Motor Vehicle Trade Regulation Rule, 16 C.F.R. ch. I, subch. D, pt. 429 (1984; last amended 2014); *See* Funeral Industry Practices, 16 C.F.R. ch. I, subch. D, pt. 453 (1994); *See* Business Opportunity Rule, 16 C.F.R. ch. I, subch. D, pt. 437 (2011); *See* Disclosure Requirements and Prohibitions Concerning Franchising, 16 C.F.R. ch. I, subch. D, pt. 436 (2007).
[41] 16 C.F.R. § 456.2.
[42] 16 C.F.R. § 456.2.
[43] Leslie Fair, *A prescription for complying with the Eyeglass Rule*, Fed. Trade Comm'n, (Dec. 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/12/prescription-complying-eyeglass-rule.
[44] *Id*. at 967.

to significant privacy injuries. There is precedent for the FTC to promulgate a trade rule under its enforcement authority to prohibit unfair acts and practices in an industry.

The scope of privacy injuries, as with other injuries redressable under the FTC Act, is broad and varied. Courts have found that "businesses can cause direct consumer harm as contemplated by the FTC Act in a variety of ways. In assessing that harm, [courts] look of course to the deceptive nature of the practice, but the absence of deceit is not dispositive."[45] The FTC has detailed many categories of consumer privacy harms that can give rise to actions and regulations under Section 5, including informational injuries from privacy and security incidents.[46] In the Commission's Informational Injury Workshop Report, the FTC outlined both market-based injuries, such as financial costs to the consumer, which can be objectively measured, and non-market injuries, which can be harder to objectively measure, that harm consumer privacy.[47] Some examples include medical identity theft, doxing, disclosure of private information, thwarted expectations and choices, and erosion of trust.[48] The privacy injuries caused by surveillance advertising are substantial, and these business practices fall within the scope of the Commission's Section 5 authority.

The recent enforcement action against Zoom Video Communications ("Zoom") shows that even *potential* exposure of personal data can constitute a substantial injury, as can the circumvention of privacy-enhancing capabilities in consumers' browsers and other devices. For example, the FTC filed a complaint and entered into a consent order with Zoom regarding Zoom's failure to properly secure communications in its services. The FTC held that the secret implementation of a web server onto users' computers, which circumvented Safari browser safeguards, was an unfair and deceptive trade practice.[49] But other FTC[50] and state Attorney General[51] privacy enforcement cases have been predicated on the notion that unwanted collection of personal information was intrinsically harmful.

The FTC has recently explained that data security injuries can be privacy injuries. In her dissenting statement in the Zoom settlement, Commissioner Slaughter explained that the FTC needs to go further to ensure that consumer privacy is protected, noting that the order "requires Zoom only to establish procedures designed to protect user *security* and fails to impose any requirements directly protecting user *privacy*." As Commissioner Slaughter explained, "[t]oo often we treat data security and privacy as distinct concerns that can be separately preserved. In reality, protecting a consumer's privacy and providing strong data security are closely

[45] *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1156 (9th Cir. 2010), *as amended* (June 15, 2010).
[46] *FTC Informational Injury Workshop*, Fed. Trade Comm'n, (Oct. 2018), https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.
[47] *Id.* at n.1.
[48] *Id.* at 1-3.
[49] Compl., *In the Matter of Zoom Video Communications, Inc.*, Comm'n File No. 1923167 (Nov. 9, 2020).
[50] Compl., *In the Matter of Sears Holdings Management Corp.*, Comm'n File No. 0823099 (Sept. 9, 2009).
[51] Assurance of Voluntary Compliance, *In the Matter of Pointroll Inc.* (Dec. 10, 2014), https://portal.ct.gov/-/media/AG/Press_Releases/2014/20141211OAGDCPPointRollAVCpdf.pdf.

intertwined, and when we solve only for one we fail to secure either."[52] She further explained that "the reason customers care about security measures in products like Zoom is that they value their privacy."[53] Thus, the FTC has recently articulated the importance of addressing privacy harms and it is therefore appropriate for the FTC to promulgate a trade regulation rule to protect consumers against business practices that invade their privacy.

Because the FTC has a broad toolkit that it can employ to protect consumers against general harms, the FTC is uniquely suited to prevent these injuries. According to privacy scholars Danielle Citron and Daniel Solove, "[T]he FTC is able to focus on harm to consumers generally, which allows it to look to harm in a broader manner than most tort and contracts cases, which involve specific individuals."[54] Moreover, as explained by privacy scholars Woodrow Hartzog and Daniel Solove, "[T]he FTC is so critical in the modern privacy regulatory scheme" because "it is has a considerably broad and diverse toolkit from which to fashion remedies which allows the commission to redress non-traditional forms of harm, balance data protection against countervailing interests in ways that other areas of law are currently unable to do, and create proactive solutions like those that rely upon design obligations to decrease risks of privacy and security harms ex ante."[55] While calling the FTC the "Lynchpin of U.S. Data Protection Law[,]" academics have highlighted that "[r]apid technological change continues to vex courts and lawmakers or leave consumers vulnerable to privacy harms."[56]

Because incremental injuries that affect many people can be substantial and because their negative impacts can materialize over time, "The FTC can regulate with a much different and more flexible understanding of harm that one focused on monetary or physical injury."[57] A practice causes "substantial injury" when it may cause serious harm to a small number of individuals or relatively small harms to many individuals.[58] According to Citron and Solove:

> For many privacy harms, the injury may appear small when viewed in isolation, such as the inconvenience of receiving an unwanted email or advertisement or the failure to honor people's expectation that your data would not be shared with third parties. But when done by hundreds or thousands of companies, the harm adds up. Moreover, these small harms are dispersed among millions (and sometimes billions)

---

[52] Commissioner Rebecca Slaughter, *Dissenting Statement of Commissioner Rebecca Kelly Slaughter In the Matter of Zoom Video Communications, Inc.*, Comm'n File No. 1923167 (Nov. 9, 2020*)* at 1, 3.
[53] *Id.* at 3.
[54] Citron & Solove, *supra* note 9, at 17. *See also* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 Geo. Wash. L. Rev. 2230, 2284.
[55] Hartzog & Solove, *supra* note 54, at 2276.
[56] *Id.* at 2266.
[57] *Id.*, at 2233–34.
[58] See Cobun Keegan & Calli Schroeder, *Unpacking Unfairness: The FTC's Evolving Measures of Privacy Harms*, 15 J.L. Econ. Pol'y 19, 27 (2019), https://jlep.net/home/wp-content/uploads/2019/01/JLEP-Volume-15-1.pdf (citing Letter from Federal Trade Commission to Senators Ford and Danforth (Dec. 17, 1980), appended to International Harvester 104 F.T.C. 949, 1070 (1984), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness).

> of people. Over time, as numerous people are each inundated by a swarm of small harms, the overall societal impact is significant.[59]

Privacy and data security cases show that the harms of violations often cause broad societal, as well as individual, harm and the "FTC has better tools than those that exist in many other areas of law to address this kind of impact."[60]

The FTC has brought a significant number of enforcement actions in privacy cases over the last twenty years, and in all cases the Commission has established that consumers expect businesses that collect their data to limit its unauthorized dissemination and use, and that when businesses violate that expectation, they are potentially liable.[61]

> The greatest potential for establishing a robust unfairness test lies in an explicit acknowledgment of the intrinsic value of personal data. The fact that an entity did not sell consumers' personal data in a particular case, but nevertheless violated consumers' established privacy expectations, should not prevent an unfairness case when the value of the data collected, exposed, or shared can in fact be established with reference to the millions of data-fueled transactions taking place every day.[62]

The "core of fairness in the privacy context" is the premise that data collectors must "refrain from sharing consumer's sensitive or confidential data with unknown third parties." [63]

IV. Establishing a Data Minimization Rule Under Section 5 of the FTC Act

Arguably the most important element of any privacy legislation is how to constrain — or to empower consumers to constrain — secondary use of their information, including the transfer and use of that data for advertising. Primary uses of data — processing that is necessary to provide the functionality by consumers — is typically understandable and noncontroversial.[64] For example, a company may collect a person's mailing address to send them a product they ordered or to process a credit card transaction. On the other hand, secondary use of data is often not well understood, and the benefits often do not accrue directly to consumers — indeed, in many cases, the uses seem downright adversarial or antithetical to people's interests, only serving the interests of companies. Much of the privacy controversy[65] in recent years and motivation for regulation[66] has centered around businesses' disclosure of personal data to data

[59] Citron & Solove, *supra* note 9, at 3-4.
[60] Hartzog & Solove, *supra* note 54, at 2283.
[61] Keegan & Schroeder, *supra* note 54, at 32.
[62] *Id.* at 38.
[63] *Id.* at 34.
[64] That is not to say there should be no rules around primary data processing, but they likely should be considerably less stringent than the rules around secondary — especially adversarial — uses. See *infra* Section V.A-B ("Primary Use Transparency," "Civil Rights").
[65] *See, e.g.*, Farhad Manjoo, *Tackling the Internet's Central Villain: The Advertising Business*, N.Y. Times (Jan. 31, 2018), https://www.nytimes.com/2018/01/31/technology/internet-advertising-business.html.
[66] Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley—And Won*, N.Y. Times (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html

brokers and for online advertising. As described above, intrusion upon seclusion has long been recognized as a privacy tort, and consumers have a legitimate interest in constraining functionally unnecessary processing of their data.

For years, the Federal Trade Commission embraced a policy of "notice-and-choice" — companies would publish privacy policies outlining their data processing activities, and consumers would be deemed to have chosen to accept those practices as a condition of using the site.[67] In practice, however, few consumers actually read privacy policies,[68] and when they do, the policies typically include limited practical information.[69] As a practical matter, notice and choice delivers neither notice nor choice.[70] Few would argue that consumers are better off under this regime.

Balancing user autonomy with hard-and-fast rules for secondary processing can be quite challenging in practice. Legislative proposals to limit secondary uses of personal data have typically applied either "opt-in" or "opt-out" frameworks — a requirement that companies must either ask for affirmative permission for secondary processing, or that they must give consumers the ability to turn off secondary processing. Both models can be flawed in practice: opt-in models can overwhelm consumers with constant requests for permission, as many websites have done in response to European privacy law. Companies may use dark patterns to coax consumers already weary so they click "OK" to cede permission for any and all uses. Meanwhile opt-out regimes such as the CCPA are both difficult to use and wildly impractical if one is to protect oneself in any meaningful way, if consumers have to manually opt out of secondary use for every website, app, or business they interact with, which can amount to thousands of organizations.[71] As a result of both approaches, consumers are forced to take too many steps to safeguard their data. A better model would either constrain data processing to conform to expected privacy norms, or to at least empower consumers to make simple, universal choices regarding their personal information.

Privacy regulation has struggled to find the appropriate role for user choice. Rather than advocating for one particular solution, this paper presents three different approaches for how the Federal Trade Commission could regulate secondary data processing through rulemaking

("Mactaggart's proposal instead took aim at the so-called third-party market for personal data, in which companies trade and sell your information to one another, mostly without your knowing about it.").

[67] *Privacy Online: A Report to Congress*, Fed. Trade Comm'n (June 1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[68] Aleecia M. McDonald, Robert W. Reeder, Patrick Kelley, Lorrie Faith Cranor, *A Comparative Study of Online Privacy Policies and Formats* at 6, https://www.robreeder.com/pubs/PETS2009.pdf.

[69] *See, e.g.*, Florencia Marotta-Wurgler, *Understanding Privacy Policies: Content, Self-Regulation, and Markets,* NYU Law and Economics Research Paper No. 16-18 at 4 (Jan. 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2736513.

[70] *See, e.g.*, Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, Harvard University Press (2018); Neil Richards, *Why Privacy Matters*, Oxford University Press (2021).

[71] *Consumer Reports Study Finds Significant Obstacles to Exercising California Privacy Right*s, Consumer Reports (Oct. 1, 2020), https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-significant-obstacles-to-exercising-california-privacy-rights/.

interpreting the unfairness prong of Section 5 of the FTC Act. *All three models were developed to minimize the burden on consumers to safeguard their personal information*:

- Prohibit all secondary data uses with limited exceptions;
- Prohibit specific secondary data uses, such as behavioral advertising or the use of sensitive data; or
- Mandate a right to opt out of secondary data use, including through global opt-out controls and databases.

The authors of this paper recommend the first approach — to prohibit all secondary uses with limited exceptions — but offer the other approaches as alternatives that could still provide meaningful privacy protections to consumers. We describe these three models in more detail below.

A. Prohibit most secondary processing by default

One option is to ban most secondary use and third-party disclosure, while explicitly carving out certain exceptions. This approach relies heavily on the principle of data minimization by limiting data processing to what is reasonably necessary to achieve the consumer's specific purpose for dealing with the company or organization.[72] This is the approach taken by several recent bills, including Senator Sherrod Brown's Data Accountability and Transparency Act of 2020,[73] California Assemblymember Buffy Wicks's Minimization of Consumer Data Processing Act,[74] New York Assemblymember Ron Kim's It's Your Data Act,[75] as well as Consumer Reports' model state privacy bill.[76]

Many privacy advocates had traditionally argued for requiring *consent* for secondary uses. However, experiences with manipulative European cookie consent interfaces and other consent dialogs designed to nudge (or confuse) consumers into granting permission for expansive permission has led to some rethinking.[77] While long boilerplate contracts and license agreements may purport to obtain consent for all sorts of unwanted data processing, it is difficult to argue that consumers have made a conscious and deliberate choice to allow it.

---

[72] It should go without saying that monetizing data in order to fund a service should not be interpreted as "reasonably necessary" to provide a service requested by a consumer.
[73] Data Accountability and Transparency Act of 2020, https://www.banking.senate.gov/404?notfound=download/brown_2020-data-discussion-draft;%20california.
[74] The Minimization of Consumer Data Processing Act, CA AB 3119 (2020), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB3119.
[75] It's Your Data Act, NY A. 3586 (2021), https://www.nysenate.gov/legislation/bills/2021/A3586.
[76] *Model State Data Privacy Act*, Consumer Reports (Feb. 2021), https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/.
[77] *Most Cookie Banners are Annoying and Deceptive. This Is Not Consent,* Privacy International (May 21, 2019), https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent.

An approach that broadly prohibits secondary uses arguably avoids these problems raised by opt-in frameworks, as user consent is insufficient to justify secondary processing: instead processing is limited to (1) what is reasonably necessary to fulfill the consumer's request and (2) other specific use cases as defined by the statute.

Policymakers do not want to subvert consumer free will. If a consumer in fact does want to share data with a company, that should be their choice. However, it should be the *primary purpose* of an interaction: if Google offers a product whereby Google offers to track users around the web in exchange for showing tailored ads, consumers can freely choose to participate in such a program. However, Google should not purport to obtain consent for tracking as part of a consumer's use of an unrelated product, such as Gmail. This framework is designed to enable processing and sharing of personal data that reflects the *volition of the consumer*, instead of permissions obtained under the fiction of informed consent.

To justify such an approach under the FTC's prohibition on unfair business practices, the FTC would have to adopt an expansive interpretation of privacy injury, that unwanted observation and data processing is inherently harmful. The FTC has adopted such a framework in the past: for example, in its 2017 settlement with Vizio, the FTC alleged that collecting and disclosing television viewing data without user permission was likely to cause those users substantial injury.[78] While the FTC emphasized that such viewing data is inherently "sensitive," it is not clear that television viewing behavior is inherently more personal than any other activity. It would be difficult to argue that purchases or web browsing, for example, is any less revealing and sensitive than information about television programming viewed. More to the point, so much of the information collected is as revealing and sensitive as our intellectual habits (like television viewing) including even seemingly prosaic information like our purchase of alcohol swabs because our everyday purchases and interactions often reveals our health conditions (for instance, Type 1 diabetics use alcohol swabs), sexual orientation, gender, close relationships, and other intimate information.

It is worth noting that the FTC may have a stronger case to prohibit secondary *collection* and *retention* of personal information, as those necessitate companies possessing personal data that they wouldn't otherwise, exposing consumers to potential exposure or misuse. Secondary *use* of already collected and retained data does not generate such additional risk of injury, though the use itself may well be deemed offensive, adversarial, or harmful (see *infra* Section IV.B ("Prohibit specific secondary uses").

In any event, the FTC should have no difficulty demonstrating that secondary data processing is "prevalent" as required for Section 18 rulemaking. Framing the harms of tracking

[78] Compl., *Fed. Trade Comm'n, v. Vizio, Inc.*, No. 2:17-cv-00758 (Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf; *VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges it Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent*, Fed. Trade Comm'n (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

broadly makes the prevalence inquiry easier, though many narrower rulemakings, such as only on targeted advertising, would also easily satisfy this test.

While recognizing that data collection and disclosure gives rise to inherent intrusions and risk, most would agree that some exceptions to a general prohibition on secondary processing are functionally necessary and can be crafted in ways to minimize intrusion and risk. Data security, analytics, product improvement, and, potentially, first-party marketing[79] are common exceptions in privacy legislation, though additional measures should be included to constrain these exceptions and to ensure that they do not swallow the general rule:

- Processing for these purposes should be limited to what is reasonably necessary to achieve the secondary purpose and proportionate to the privacy intrusion.[80]
- Service providers who process data on behalf of a consumer should segment the data from other clients, and should be prohibited from engaging in secondary uses of their own.[81]
- Secondary processing should, where possible, be limited to data already collected and retained for a primary purpose in order to minimize new risk of secondary exposure or misuse.
- Platforms that facilitate communication or interactions among other companies — such as ISPs and social media companies — should generally be considered "third parties" with regard to the interaction between a consumer and other companies.

The narrower the allowed secondary uses, the higher the FTC's burden will be to argue that the remaining universe of prohibited uses is harmful. Certain uses — such as for security and fraud prevention — provide concrete benefits that may well countervail the injuries associated with surveillance.

Advertising firms likely would argue that the economic benefits of ad targeting would also outweigh injuries resulting from unwanted surveillance, though estimates of these benefits vary widely, as do estimates of to whom those benefits accrue.[82] Under Section 5, only the benefits

---

[79] The CR model privacy bill allows for first-party marketing with an opt out. *See Model State Data Privacy Act*, Consumer Reports (Feb. 2021), https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/. Other advocates have largely called for the prohibition of any targeting advertising. See *International coalition calls for action against surveillance-based advertising*, Norwegian Consumer Council (Jun. 22, 2021), https://www.forbrukerradet.no/side/new-report-details-threats-to-consumers-from-surveillance-based-advertising/.

[80] *See, e.g.*, Mark Zuckerberg, *The Facts About Facebook*, Wall St. J. (Jan. 24, 2019), https://www.wsj.com/articles/the-facts-about-facebook-11548374613 (arguing that Facebook needs the ability to use information from cross-site web traffic for fraud deterrence).

[81] It may be reasonable to allow service providers the ability to engage in their own narrow secondary uses — such as service improvement — but they should certainly be prohibited from using other parties' data for purposes such as their own marketing.

[82] *See, e.g.*, Veronica Marotta et al., *Who Benefits from Targeted Advertising?*, Carnegie Mellon University, https://www.ftc.gov/system/files/documents/public_comments/2015/10/00037-100312.pdf; Howard Beales, *The Value of Behavioral Advertising*, https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00117/544506-00117.pdf.

that accrue to *consumers* or *competition* are relevant for consideration. As demonstrated in the Accountable Tech petition, there is a strong argument that the behavioral advertising model has led to the consolidation of market power by giant technology companies such as Google and Facebook.[83] Those two companies are also the biggest beneficiaries of secondary data collection, as they collect data from more third-party websites and mobile applications than any other business.[84]

Advertising firms would also likely argue that free online content is funded by secondary data collection, though ads have supported online content for decades, and few online ads were precisely targeted until recent years.[85] It is not clear that incrementally much more content is available because of behavioral ads, and if so what the quality and marginal value to consumers of such content is.[86] One recent report from Carnegie Mellon — presented at the FTC's PrivacyCon — found that individually targeted ads only increased publishers' advertising revenue by 4%, with an incremental increase of revenue of approximately $0.00008 per ad.[87] Even assuming some degree of value, it may not be enough to offset the harms and loss of utility that consumers experience as a result of profligate data disclosure and secondary processing.

B. Prohibit specific secondary uses

Another approach to privacy rulemaking would be to prohibit certain secondary uses of data, rather than prohibit all secondary uses by default and then claw back certain acceptable uses. This is the approach taken, for example, by the Center for Democracy & Technology model bill, which prohibits the processing of biometrics, geolocation, and cross-device tracking for secondary purposes.[88] One significant downside of this approach is that it presumes a less expansive conception of privacy injury — namely, that intrusion on seclusion and the risks posed by additional data storage are not intrinsically harmful and in and of themselves justify

---

[83] Accountable Tech Rulemaking Petition, *supra* note 20.
[84] Justin Brookman et al., *Cross-Device Tracking: Measurement and Disclosures*, Proceedings on Privacy Enhancing Technologies, 2017 (2):133–148, https://www.petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf; Steve Englehardt and Arvind Narayanan, *Online Tracking: A 1-million-site Measurement and Analysis*, https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf ; Altaweel, Good, and Hoofnagle, *Web Privacy Census*, Technology Science (Dec. 14, 2015), https://techscience.org/a/2015121502/.
[85] Statement of Justin Brookman Director, Privacy and Technology Policy, Consumers Union, Before the House Subcommittee on Digital Commerce and Consumer Protection, Understanding the Digital Advertising Ecosystem (June 14, 2018), https://advocacy.consumerreports.org/wp-content/uploads/2019/07/Brookman-Testimony-June-14-2018.pdf.
[86] Eric Zeng et al., *Bad News: Clickbait and Deceptive Ads on News and Misinformation Websites,* ConPro Workshop on Technology and Consumer Protection (2020), https://homes.cs.washington.edu/~yoshi/papers/ConPro_Ads.pdf.
[87] Veronica Marotta, Vibhanshu Abhishek, & Alessandro Acquisti, *Online Tracking and Publishers' Revenues: An Empirical Analysis*, Workshop on the Economics of Information Security (2019), https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.
[88] *Federal Baseline Privacy Legislation Discussion Draft*, Center for Democracy & Technology (Dec. 13, 2018), https://cdt.org/collections/federal-privacy-legislation/.

policy intervention. At the very least it sublimates the intrinsic harms of privacy invasion to other, more specific harms. On the other hand, focusing regulation on specific practices that lead to greater injuries to consumers may be more likely to withstand legal challenges to a privacy rule.

To justify such an approach under unfairness, each of the specific uses must be tied to substantial injuries, those injuries must not be reasonably avoidable by consumers, and the injuries must not be outweighed by countervailing benefits to consumers or competition. Some examples of specific harmful practices that some have called to be prohibited include:

- Discriminatory use of data that deprives consumers of opportunities based on protected characteristics (see *infra* Section V.B ("Civil Rights"))
- Tracking users across different devices
- Personalization based on sensitive attributes
- Facial recognition and other biometric identification
- Collection and use of intimate information — about the human body, health, innermost thoughts and searches, sex, sexuality, and gender, and close relationships[89]
- Disclosure of personal information of minors (or children under the age of 13)

Surveillance Advertising

One obvious candidate for specific use restriction is targeted advertising. In recent months, several privacy advocates have called upon regulators to specifically ban surveillance advertising.[90] Recently, Accountable Tech petitioned the FTC to ban surveillance advertising under its unfair methods of competition authority, arguing that targeted ads perpetuate discrimination, exploit kids and teens, fuel extremism and misinformation, and advantage the largest technology companies over rivals.[91]

By banning targeted advertising instead of the underlying data collection and retention associated with it, the FTC would be relying not upon intrusion upon seclusion and the risks associated with data storage, but that the manipulation and coercion associated with ads fueled by data profiles are injuries meriting a prohibition.

This prohibition could focus specifically on cross-context targeted advertising — that is, the targeting of ads based on a consumer's activity across different websites, apps, and physical locations. Such "behavioral advertising" has been the bugbear of privacy advocates for

[89] Danielle Keats Citron, *A New Compact for Sexual Privacy*, 62 Wm. & Mary L. Rev. 1763 (2021), https://scholarship.law.wm.edu/wmlr/vol62/iss6/2; *see also* Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (W.W. Norton, Penguin Vintage UK forthcoming 2022).
[90] *International coalition calls for action against surveillance-based advertising*, Norwegian Consumer Council (Jun. 22, 2021), https://www.forbrukerradet.no/side/new-report-details-threats-to-consumers-from-surveillance-based-advertising/.
[91] Accountable Tech Rulemaking Petition, *supra* note 20.

years.[92] Moreover, state level comprehensive privacy legislation — both enacted and proposed — has generally targeted cross-context ad targeting rather than first-party marketing.[93] However, many privacy groups have made more aggressive calls for regulation in recent years, arguing that a prohibition on targeting should extend to first-party data sets as well, pointing to large technology companies like Google and Facebook that have the ability to amass substantial personal data sets even without supplementing them with third-party data.[94]

Under either approach, while the injuries alleged, for example, in the Accountable Tech petition are undoubtedly substantial, the FTC would need to demonstrate the extent to which of those injuries are attributable to targeted advertising. If that case is made, it would be difficult to argue that such injuries are readily avoidable by consumers — most Americans do not currently have the legal right to turn off ad targeting. Even when consumers do have the ability to opt out of targeting — either under state law or due to self-regulation — those tools turn out to be confusing, incomplete, and impractical for consumers to use at scale.[95] A Consumer Reports study on the efficacy of CCPA opt-out rights, for example, found that consumers tasked with opting out of data sales from just one data broker were often frustrated and unable to meaningfully limit sale or associated cross-context targeting.[96]

As with the approach of broadly banning secondary use, opponents would likely argue that the economic benefits of ad targeting outweigh the injuries to consumers. However, the same counterarguments apply as well: that targeted advertising appears to be harmful to consumers, harmful to competition as the benefits flow primarily to large internet companies, and that free online content long predates the prevalence of targeted display ads.[97]

---

[92] Center for Democracy and Technology et al., *Re: In advance of the FTC Town Hall, "Ehavioral Advertising: Tracking, Targeting, and Technology," to be held November 1-2, 2007 in Washington, D.C.*, https://cdt.org/wp-content/uploads/privacy/20071031consumerprotectionsbehavioral.pdf.

[93] *E.g.*, Cal. Civ. Code § 1798.100 et seq.; Washington SB 5062 (2021), Amendment by Committee on Civil Rights & Judiciary, https://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Amendments/House/5062-S2%20AMH%20CRJ%20H1373.1.pdf.

[94] It is worth noting, however, that these two companies are also the largest aggregators and users of third-party data. *See, e.g.*, Justin Brookman et al., *Cross-Device Tracking: Measurement and Disclosures, Proceedings on Privacy Enhancing Technologies*, 2017 (2):133–148, https://www.petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf; Steve Englehardt and Arvind Narayanan, *Online Tracking: A 1-million-site Measurement and Analysis*, https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf ; Altaweel, Good, and Hoofnagle, *Web Privacy Census,* Technology Science (Dec. 14, 2015), https://techscience.org/a/2015121502/.

[95] Statement of Justin Brookman, Director, Consumer Privacy, Center for Democracy & Technology, Before the U.S. Senate Committee on Commerce, Science, and Transportation Hearing on "A Status Update on the Development of Voluntary Do-Not-Track Standards" at 3 (Apr. 24, 2013), https://cdt.org/wp-content/uploads/pdfs/Brookman-DNT-Testimony.pdf.

[96] *Consumer Reports Study Finds Significant Obstacles to Exercising California Privacy Right*s, Consumer Reports (Oct. 1, 2020), https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-significant-obstacles-to-exercising-california-privacy-rights/.

[97] *Id.*

C. Mandate compliance with opt-outs (including universal opt-out settings and databases)

Finally, the FTC might require companies to honor universal opt-out requests for secondary (non-necessary) processing. Under this model, any secondary processing would be allowable by default, however consumers would be legally entitled to turn off either specific categories of secondary process, or all secondary processing (with some exceptions). This is the model so far adopted in states such as California, Virginia (VCDPA), and Colorado (CPA), as well as federal legislation proposed by Senator Ron Wyden.[98] The bulk of other state legislative proposals introduced in recent years follows this model as well. Such an approach should be considered the *bare minimum* that could be done to address secondary data processing — otherwise, consumers would not be able to practically take action to constrain unwanted secondary processing.

For opt-out rights to be functionally usable by consumers, they must be scalable. An opt-out regime can only work if consumers can opt out universally from secondary processing across entire platforms with simple tools. In the absence of a default prohibition on most secondary data use, the FTC should (1) mandate that companies need to comply with platform-level opt-outs such as Global Privacy Control (GPC), IoS Limit Ad Tracking, and Do Not Track (DNT). For other types of data processing, the FTC could also (2) set up a registry of identifiers — such as email addresses, phone number, etc. — for users to globally opt out of the disclosure or secondary processing of those identifiers and any linked information.

Under an opt-out model, companies should be legally obligated to honor browser privacy signals, such as Do Not Track or the Global Privacy Control as an opt out of secondary data uses, so that consumers can stop secondary processing of their personal information to every company with which their browser interacts in a single step. Otherwise, consumers would have to opt out individually at hundreds, if not thousands, of different websites, which is not practical. For unauthenticated data not associated with a specific person, platform-level controls are the most efficient manner to globally convey opt-out requests.

This is the approach taken in newly-adopted legislation in California and Colorado. For example, California law requires companies to honor browser privacy signals, as well as requests submitted by authorized agents, as a valid opt out of sale under the California Consumer Privacy Act. The California Attorney General's office recently updated their guidance to clarify that companies must honor the Global Privacy Control specifically — a CCPA-compliant browser signal that conveys a "Do Not Sell" command — as an opt out. Further, they have sent enforcement letters to companies that are not honoring GPC.[99] The California Privacy

---

[98] Cal. Civ. Code § 1798.100 et seq.; Colorado S. 21-190 (2021), https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf; Virginia S. 1392 (2021), https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392; S. 1444 § 6 (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1444.

[99] Kate Kaye, *California's Attorney General Backs Call for Global Privacy Control Adoption with Fresh Enforcement Letters to Companies*, Digiday (July 16, 2021), https://digiday.com/marketing/californias-

Rights Act (Proposition 24) adds the requirement to honor browser privacy signals to the text of the statute.[100] The Colorado Privacy Act, which will go into effect in 2023, also requires companies to honor browser privacy controls as an opt out of processing for the purposes of sale and targeted advertising.[101]

Opting out one-by-one is particularly impractical because under the CCPA, which has an opt-out model, many companies have developed complicated and onerous opt-out processes. Some companies ask consumers to go through several different steps to opt out. In some cases, the opt outs are so complicated that they have actually prevented consumers from stopping the sale of their information.[102] This is expected to improve, as the California Attorney General has since prohibited the use of dark patterns in opt-out processes, and is stepping up their enforcement efforts. Nevertheless, in the absence of a ban of most secondary use, it is important for consumers to have (at least) a one-step option for stopping the secondary use of their information.

Second, the FTC could create and house a Do Not Sell registry, modeled on the popular Do Not Call (DNC) registry, that businesses would be required to check before selling consumer data tied to those identifiers. The Commission would collect consumers' identifiers, such as emails and phone numbers, and companies would pay in order to consult the list (thus ensuring that companies seeking to sell data would absorb the costs for the operation of the website). Consumers could add their identifiers to the registry through a public portal, much like Do Not Call. This would enable consumers to easily and globally express their preferences to opt-out of the sale of data tied to specific identifiers (or hashes of specific identifiers). Companies would be required to check this database before disclosing or tracking based on consumers' information, much as they do today for the DNC registry. The DNC registry currently includes 244.3 million active registrations, indicating that this is an easy way for consumers to opt out of telemarketing messages.[103] On the other hand, compliance with Do Not Call has been inconsistent given the ease of creating difficult-to-trace voice-over-internet calls. One downside of a registry approach would be to make such identifiers publicly available to bad faith actors and more susceptible to spam. The rule would need to be paired with aggressive FTC enforcement as well as technical measures to remediate registry access and misuse.

Such a registry approach would work in tandem with Global Privacy Controls — a registry would only govern data sets tied to persistent real-world identifiers, but would also

---

attorney-general-backs-call-for-global-privacy-control-adoption-with-fresh-enforcement-letters-to-companies/.

[100] Cal. Civ. Code § 1798.135(e).

[101] Colorado S. 21-190 (2021), https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf.

[102] Kaveh Waddell, *California's New Privacy Rights Are Tough To Use, Consumer Reports Study Finds* Consumer Reports (Mar. 16, 2021), https://www.consumerreports.org/privacy/californias-new-privacy-rights-are-tough-to-use/.

[103] *National Do Not Call Registry Data Book FY 2021*, Fed. Trade Comm'n at 5 (Nov. 2021), https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2021. The efficacy of the DNC registry is also limited by the fact that it only applies to telemarketing, and that it does not hinder scammers, debt collectors, and others in their communications.

govern offline data transactions. Global Privacy Controls would apply to data tied only to pseudonymous or short-term identifiers, but in many cases only apply to the platform that is sending the signals, such as a browser.[104] Senator Ron Wyden, in his privacy bill, the Mind Your Own Business Act, outlines a similar system to facilitate global opt outs through registries as well as persistent opt-out signals for both unauthenticated and authenticated data.[105]

Mandating compliance with opt-out requests would rely upon similar theories of unfairness discussed in the previous two sections — that unwanted surveillance or specific prohibited practices lead to substantial injuries to consumers, that they are not reasonably avoidable, and they are not offset by countervailing benefits to consumers or competition.

By only prohibiting secondary processing upon the objection of a user, the FTC may be on even stronger ground, as in each case the consumer has evinced that they experience some loss of utility due to such processing. The FTC also has previous precedent for the proposition that evading platform-level privacy settings such as the Global Privacy Control is unfair and deceptive. For example, as noted above, the FTC's recent Zoom settlement held that circumventing platform privacy protections is inherently harmful.[106]

Finally, a Data Minimization Rule could rely on a combination of approaches (B) and (C) — that is, certain data practices could be prohibited as a matter of law, and users would have the ability to opt out of certain other secondary processing. Or the agency could require opt-in consent for certain secondary data processing, though as discussed earlier, privacy law should not encourage companies to bombard consumers with requests for secondary data collection and use. The FTC might decide there was a stronger case for banning certain practices by default, but certain others only with consent or when a consumer has affirmatively asserted an objection. Again, however, such an approach would minimize the inherent invasiveness of secondary data processing, and would potentially leave consumers exposed to unwanted and unnecessary data practices.

V. Other Privacy Protections That Should be Implemented Through Section 5 of the FTC Act

A. Primary Use Transparency

As opposed to secondary use, primary use is likely to be more intuitive and less objectionable to users. As such, it merits less strict regulation than secondary use. While some privacy models have argued that consumers should provide explicit consent even for primary use, such an approach has significant drawbacks.[107] As virtually every consumer interaction

[104] However, if a company receives a Global Privacy Control signal tied to data authenticated to a real-world identifier, it could be obligated to apply the user's opt-out choice to data on other platforms.
[105] S. 1444, § 6 (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1444.
[106] Compl., *In the Matter of Zoom Video Communications, Inc.*, Comm'n File No. 1923167 (Nov. 9, 2020) at ¶ 34-53, https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint.pdf.
[107] *See, e.g.*, New York S. 6701 (2021), https://www.nysenate.gov/legislation/bills/2021/s6701.

involves some degree of data processing, consumers would be overwhelmed with privacy information and choices. This torrent of consent interfaces could make it difficult for consumers to distinguish between commonplace, expected data processing and requests to engage in processing for new, potentially unwanted, activities. Consumers would likely become enured to giving consent in order to go about their lives. The frequent use of dark patterns in opt-in interfaces, for example those used to comply with the GDPR, ePrivacy Directive, and CCPA, pose further challenges to obtaining meaningful consumer consent. It is possible — though certainly debatable — that these consent dialogs would give consumers more information and relatively empower them to make decisions in the marketplace, but the countervailing cost of subjecting consumers to dozens of privacy choices in a given day would likely offset any benefits.

However, a privacy rulemaking may still dictate some heightened degree of transparency around even primary use. If a certain activity involves processing especially sensitive data in potentially nonintuitive ways, a privacy rule could provide some obligation to ensure that consumers understand the consequences of the transaction they have initiated.[108] Such disclosures should be the exception and not the rule, however. This requirement could be justified under the FTC's unfairness authority: failing to provide heightened disclosure around potentially and unexpected processing of certain data could easily lead to unexpected and unavoidable injuries for a consumer. An obligation to provide such heightened transparency has precedent in the Funeral Rule. The FTC clarified, under its Section 5 authority, that "it is an unfair or deceptive act or practice for a funeral provider to fail to furnish accurate price information disclosing the cost to the purchaser for each of the specific funeral goods and funeral services used in connection with the disposition of deceased human bodies..."[109] It requires funeral homes to provide clear, accurate information in an itemized list, to better enable consumers to compare offerings from multiple providers.[110] Given the heightened sensitivity of the transactions and the vulnerability of the consumers involved, these labeling requirements are particularly appropriate.

Further, the FTC should establish some documentation requirements for all processing behaviors. Privacy policies should not be intended for consumers, who cannot reasonably be expected to read these complicated disclosures, but for intermediaries like ratings services, the press, academics, and regulators. Consumers dislike reading privacy policies,[111] but they serve a real purpose. Because there are no requirements for these disclosures, and because most FTC privacy cases are predicated upon a specific misstatement in a privacy policy or

---

[108] For example, the Colorado Privacy Act requires opt-in consent for the processing of a limited category of sensitive data, though that rule is not limited to scenarios where consumers would be likely to be surprised or offended by the data processing. Colorado S. 21-190 § 6-1-1308(7) (2021), https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf.
[109] 16 C.F.R. § 453.2.
[110] Robert Benincasa, *You Could Pay Thousands Less For A Funeral Just By Crossing The Street*, NPR (Feb. 17, 2017), https://www.npr.org/2017/02/07/504020003/a-funeral-may-cost-you-thousands-less-just-by-crossing-the-street.
[111] Aleecia M. McDonald, Robert W. Reeder, Patrick Kelley, Lorrie Faith Cranor, *A Comparative Study of Online Privacy Policies and Formats* at 6, https://www.robreeder.com/pubs/PETS2009.pdf.

elsewhere, companies tend to make privacy policies as expansive as possible, so as to shield themselves from lawsuits and other enforcement actions.[112] To address this problem, privacy policies must provide reasonably detailed information about practices. These transparency requirements for primary use fall squarely within the FTC's authority to issue rules to prevent unfair practices, since they merely provide information to the marketplace, providing accountability for companies' practices; the FTC could consider instituting a size threshold for such privacy policy requirements to excuse small businesses who may not have the resources or sophistication to provide such documentation.

B. Civil Rights

Primary data processing should also be constrained to ensure that it is not discriminatory in nature.[113] In recent years, it has become clear that the issues of privacy and civil rights are directly related. Companies have access to more and more data points about consumers and have a greater ability to provide differential experiences, offers, and advertisements to smaller and smaller segments of the population. Even if this segmentation is not explicitly based on protected characteristics such as race and gender identity, companies may (intentionally or inadvertently) use proxies for these factors that result in unfair treatment. Moreover, even when there is no intention to discriminate, black box algorithms can produce discriminatory results by replicating patterns of inequity that are already present in societal data inputs. This segmentation is often done through algorithms that are inherently difficult for external observers to test and hold accountable — especially when companies take affirmative measures to frustrate researchers testing for potential bias.[114]

Ad targeting based on this data can perpetuate historic patterns of discrimination and unequal outcomes among protected classes.[115] For example, the Department of Housing and Urban Development has charged Facebook for targeting housing advertisements based on protected categories like race and religion.[116] These targeting systems have been used to

---

[112] *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, Fed. Trade Comm'n, at 61 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[113] *See, e.g.*, Gaurav Laroia, David Brody, *Privacy Rights Are Civil Rights. We Need to Protect Them* (Mar. 14, 2019), https://www.freepress.net/our-response/expert-analysis/insights-opinions/privacy-rights-are-civil-rights-we-need-protect-them; *The Online Civil Rights and Privacy Act of 2019*, Free Press Action and the Lawyers' Committee for Civil Rights Under Law, Section 3(a) (Mar. 11, 2019), https://www.freepress.net/sites/default/files/2019-03/online_civil_rights_and_privacy_act_of_2019.pdf.

[114] *See, e.g.*, Letter from Acting Director of the Bureau of Consumer Protection Samuel Levine to Facebook (Aug. 5, 2021), https://www.ftc.gov/news-events/blogs/consumer-blog/2021/08/letter-acting-director-bureau-consumer-protection-samuel.

[115] *See Letter from Lawyers' Committee for Civil Rights Under the Law et al. to Chair Lina Khan and Commissioners Chopra, Slaughter, Phillips, and Wilson,* Fed. Trade Comm'n (Aug. 4, 2021), https://www.lawyerscommittee.org/wp-content/uploads/2021/08/FTC-civil-rights-and-privacy-letter-Final-1.pdf.

[116] *Sec'y of Hous. & Urban Dev. v. Facebook, Inc.*, No 01-18-0323-8, 1, Charge of Discrimination, FHEO No. 01- 18-0323-8 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.

interfere with elections and fuel voter suppression efforts and to carry out disinformation campaigns that undermine public trust.[117] Further, some data brokers provide this information to employers, landlords, and others, while evading the Fair Credit Reporting Act, giving consumers next to no control over these uses.[118] The increasing use of automated decision-making can further exacerbate these problems, as opaque algorithms, often trained on historical data, can perpetuate existing inequalities.[119]

As part of a set of privacy protections, the FTC should formalize a rule stating that companies are prohibited from discriminating against protected classes in the offering of economic opportunities or online public accommodations.[120] This prohibition on discrimination should apply to both intentional discrimination and practices that produce a discriminatory disparate impact. Such a rule should include a typical disparate impact analysis,[121] which involves (1) the demonstration of a disparate impact on the basis of a protected characteristic, (2) an opportunity for a respondent to articulate a substantial, legitimate, and nondiscriminatory purpose for the practice, and (3) if there is a legitimate purpose, a showing that a less discriminatory alternative is available or that the purpose is pretextual. This disparate impact standard is well established in case law and is well understood by businesses — for example, all businesses must already comply with this standard in their employment practices, pursuant to Title VII of the Civil Rights Act of 1964.[122]

Such a rule is straightforward to justify under the FTC's unfairness authority. Practices that have an otherwise unjustified disparate impact on protected classes' access to economic opportunities or public accommodations are undoubtedly harmful.[123] The FTC has found that injuries that fall specifically or disproportionately on disadvantaged classes are covered by Section 5, such as its recent settlement with Bronx Honda over charging higher prices to Black

---

[117] *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, Fed. Trade Comm'n (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[118] *Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA*, Fed. Trade Comm'n (June 12, 2012), https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed; *Big Data, A Big Disappointment for Scoring Consumer Credit Risk*, Nat'l Consumer Law Ctr. at 26 (Mar. 2014), https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf.

[119] *See* Erin Simpson & Adam Conner, *How to Regulate Tech: A Technology Policy Framework for Online Services*, Ctr. for Am. Progress (Nov. 16, 2021) (discussing the extensive literature on civil rights harms caused by automated decision-making systems, biometric surveillance, amplification of civil-rights suppressing content, and reification of prejudice), https://www.americanprogress.org/article/how-to-regulate-tech-a-technology-policy-framework-for-online-services/.

[120] Kristen Clarke and David Brody, *It's time for an online Civil Rights Act*, The Hill (Aug. 3, 2018), https://thehill.com/opinion/civil-rights/400310-its-time-for-an-online-civil-rights-act.

[121] *See* Title VI Legal Manual, Dep't of Justice (Apr. 22, 2021) at Section VII, https://www.justice.gov/crt/book/file/1364106/download.

[122] 42 U.S.C. § 2000e, *et seq*.

[123] Elisa Jillson, *Aiming for truth, fairness, and equity in your company's use of AI*, Fed. Trade Comm'n (Apr. 19, 2021), https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai ("[R]esearch has highlighted how apparently 'neutral' technology can produce troubling outcomes – including discrimination by race or other legally protected classes… [H]ow can we harness the benefits of AI without inadvertently introducing bias or other unfair outcomes?").

and Latino customers.[124] It is difficult to imagine how such discrimination would be avoidable by consumers, particularly when the source of such discrimination is a black box algorithm or other data practice that lacks transparency. Unfairness's third prong should be satisfied by the disparate impact test, which evaluates whether a discriminatory behavior can be justified by a substantial, legitimate, and nondiscriminatory purpose, as well as whether such purpose can be achieved by less harmful alternatives.

C. Nondiscrimination

Privacy regulation should also prohibit businesses from providing differential treatment to consumers who opt out of or do not consent to targeted offers, or the sale of information about customer habits to third-party data brokers. Consumers will be less likely to exercise their privacy rights if businesses charge them for doing so. Such practices sometimes occur under the guise of loyalty programs[125] — in 2013, for example, CVS asked consumers to waive their HIPAA rights in return for participation in the ExtraCare rewards program.[126]

Instead, privacy should be recognized as an inalienable and fundamental right, not merely an asset to be bartered away. Further, charging consumers for privacy could have a disparate impact on the economically disadvantaged and members of protected classes who may not be able to afford the luxury of paying for fundamental privacy rights. (These rules should not, however, inhibit true loyalty programs that keep track of consumer purchases in order to incentivize repeat business, where the data collection and usage is strictly necessary for the fundamental purpose of the program, and which falls squarely within consumers' expectations for primary use.)

Particularly where consumers have few choices, market forces fail to impose sufficient constraints on companies from penalizing exercising privacy rights. Low-income consumers may feel coerced into granting unfettered access to and use of their personal information for targeting or other purposes. For example, from 2013 to 2016, AT&T charged users who did not agree to the use of their internet data for ad targeting around $30 per month — a significant portion of the monthly charge for internet service.[127]

---

[124] Compl. for Permanent Injunction and other Equitable Relief, Fed. Trade Comm'n, v. Liberty Chevrolet, Inc., No. 20-CV-3954 (May 27, 2020), https://www.ftc.gov/system/files/documents/cases/bronx_honda_complaint_0.pdf; Statement of Commissioner Rohit Chopra In the Matter of Liberty Chevrolet, Inc., Comm'n File No. 1623238 (May 27, 2020), https://www.ftc.gov/system/files/documents/public_statements/1576002/bronx_honda_final_rchopra_bronx_honda_statement.pdf.

[125] Chloe Liu, *CVS, Walgreens, and Rite Aid Loyalty Programs Compared: How to Get the Best Deals (Without the Mile-Long Receipts)*, N.Y. Times Wirecutter (May 24, 2021), https://www.nytimes.com/wirecutter/money/drugstore-loyalty-programs/.

[126] David Lazarus, *CVS thinks $50 is enough reward for giving up healthcare privacy*, L.A. Times (Aug. 15, 2013), https://www.latimes.com/business/la-xpm-2013-aug-15-la-fi-lazarus-20130816-story.html.

[127] Jon Brodkin, *AT&T to end targeted ads program, give all users lowest available price*, ArsTechnica (Sept. 30, 2016), https://arstechnica.com/information-technology/2016/09/att-to-end-targeted-ads-program-give-all-users-lowest-available-price/.

A prohibition on discriminatory treatment would recognize that forcing consumers to choose between unwanted sharing and use of their information on the one hand, and higher prices or inferior service on the other hand, constitutes an injury that consumers would understandably want to avoid. Privacy should be treated as an intrinsic right with positive societal externalities for free expression and experimentation, and policies that incentivize individuals to waive privacy will lead to worse outcomes.[128]

Some state privacy measures already put limits on the most exploitative practices, but still have loopholes that could permit inappropriate charges for exercising privacy rights. The CCPA includes language prohibiting discrimination "against a consumer because the consumer exercised any of the consumer's rights under this title[,]" including by denying goods or services, or charging a different price or providing a different level or quality of goods or services for doing so.[129] However, confusingly, it notes that a company may do so if it is "is reasonably related to the value provided to the business by the consumer's data[,]"[130] and if such incentives programs are not unfair or usurious. CPRA adds to the measure a clarification that loyalty programs are permitted under the CCPA.[131] Virginia[132] and Colorado[133] have similar language prohibiting non-discrimination but allowing certain incentives programs. (In contrast, pending privacy legislation in Washington State includes consensus language that prohibits the disclosure of personal information to third parties pursuant to loyalty programs).[134]

D. Data security

The accumulation of consumer data — from the consumer directly, scraped from public sources, and purchased from data brokers — creates serious security risks.[135] Data collection, retention, and inadequate internal controls also leave users vulnerable to employees who abuse their power. Uber, Facebook, and NSA employees have used location data in order to stalk the objects of their romantic interest.[136] The Federal Trade Commission arguably has the strongest

---

[128] *See, e.g.*, Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 Columbia L. Rev. 6 (Oct. 2017), https://ssrn.com/abstract=3058835; *See also* Accountable Tech Rulemaking Petition, *supra* note 20 at 25-35, on the harms associated with unrestricted data collection, use, and sharing.
[129] Cal. Civ. Code § 1798.125(a)(1).
[130] *Id. at* § 1798.125(a)(2).
[131] Cal. Civ. Code § 1798.125(a)(3).
[132] VA SB 1392 § 59.1-574(A)(4) (2021), https://lis.virginia.gov/cgi-bin/legp604.exe?211+ful+SB1392ES1+pdf.
[133] CO S. 21-190 § 6-1-1308(1)(c)-(d), https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf.
[134] WA SB 5062 (2021).
[135] Brookman and Hans, *supra* note 8.
[136] Alex Hern, *Uber Employees 'Spied on Ex-Partners, Politicians and Beyonce,'* The Guardian (Dec. 13, 2016), https://www.theguardian.com/technology/2016/dec/13/uber-employees-spying-ex-partners-politicians-beyonce; Siobahn Gorman, *NSA Officers Spy On Love Interests*, Wall St. J. (Aug. 23, 2013), https://www.wsj.com/articles/BL-WB-40005; Karen Hao, *Review: Why Facebook Can Never Fix Itself*, MIT Technology Review (Jul. 21, 2021), https://www.technologyreview.com/2021/07/21/1029818/facebook-ugly-truth-frenkel-kang-nyt/.

grounds in implementing *security obligations* as part of a privacy rule. Since 2005,[137] the Commission has brought 80 cases alleging that companies' failure to use reasonable security measures to safeguard data constitutes unfair business practice.[138] As the FTC has alleged in cases against InfoTrax[139] and SkyMed,[140] retention of the data puts users at risk for data breach, is largely unavoidable by consumers as the data resides on a company's servers, often unbeknownst to them, and is not offset by countervailing benefits if the data deletion processes are reasonably cost effective.

Clearly, breaches are particularly harmful with respect to sensitive data, but there should be protections over less sensitive data too. For example, a security glitch exposed users' private tweets for more than four years; though that would not count as personal information under many state data security and data breach notification laws, inadvertent disclosure could have significant reputational damage to consumers.[141] Indeed, the FTC has a stronger need to mandate data security as consumers may find it difficult to plead Article III standing for security violations where the harms are unknown or difficult to articulate.[142] The scope of the FTC's authority to articulate and pursue bad security practices is not so constrained.

The second two parts of the unfairness test are easily met. Security breaches are certainly unavoidable from the consumer perspective — the company's own practices are responsible for such breaches. Not only are companies better positioned than consumers to engineer security solutions, but in the case of data brokers and credit bureaus (such as Equifax), consumers do not have a choice as to whether their information is collected. In the case of certain internet-connected devices, consumers could use resources such as Consumer Reports to choose more secure products, but nevertheless, there are significant information asymmetries that prevent consumers from consistently and effectively making choices to protect their data.

The FTC's reasonableness standard addresses the third element of the unfairness test — companies need not take unduly burdensome measures, the costs of which outweigh any likely benefits to consumers. Indeed, the standard is flexible enough so that any measures taken are appropriate to the company's unique circumstances. As Andrea Arias of the FTC

---

[137] *BJ's Wholesale Club Settles FTC Charges: Agency Says Lax Security Compromised Thousands of Credit and Debit Cards*, Fed. Trade Comm'n (Jun. 16, 2005), https://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges; *DSW Inc. Settles FTC Charges: Agency Says Company Failed to Protect Sensitive Customer Data*, Fed. Trade Comm'n (December 1, 2005), https://www.ftc.gov/news-events/press-releases/2005/12/dsw-inc-settles-ftc-charges.

[138] *Federal Trade Commission 2020 Privacy and Data Security Update*, Fed. Trade Comm'n at 3 (2021), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf.

[139] Compl., *FTC v. Infotrax Systems L.C.*, at ¶ 10 (Jan. 6, 2020), https://www.ftc.gov/system/files/documents/cases/162_3130_infotrax_complaint_clean.pdf.

[140] Compl., *FTC v. SkyMed International, Inc.*, at ¶ 12(e) (Dec. 16, 2020), https://www.ftc.gov/system/files/documents/cases/skymed_-_complaint.pdf.

[141] Sam Schechner, *Twitter Data Case Sparks Dispute, Delay Among EU Privacy Regulators*, Wall St. J (Aug. 20, 2020), https://www.wsj.com/articles/twitter-data-case-sparks-dispute-delay-among-eu-privacy-regulators-11597921201?mod=article_inline.

[142] *See, e.g.*, *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021).

pointed out, "[T]he touchstone of the FTC's approach to data security has been reasonableness—that is, a company's data security measures must be reasonable in light of the volume and sensitivity of information the company holds, the size and complexity of the company's operations, the cost of the tools that are available to address vulnerabilities, and other factors. Moreover, the FTC's cases focus on whether the company has undertaken a reasonable process to secure data."[143] For example, in its 2020 Privacy & Data Security Update, the FTC explained that in each of their data security cases from that year, the Commission directed the company to "implement a comprehensive security program, obtain robust biennial assessments of the program, and submit annual certifications by a senior officer about the company's compliance with the order."[144] Such requirements should be the baseline for any company collecting consumers' data, given the widespread incidence of data breaches.

Arguably the most difficult question on data security rules is how prescriptive to make them. In our view, a data security rule should have a comprehensive definition of personal information that includes online accounts and biometric data; require companies to implement, maintain, and keep up-to-date reasonable security protections and a reasonable security program appropriate to the nature of the information, to protect the information (and any such device) from unauthorized access, destruction, use, modification, or disclosure, with administrative, physical, and technical safeguards; and retention limits. The goal should be to provide companies with adequate direction without being so prescriptive that it is overly burdensome and outdated within a few years.

Some security provisions within privacy legislation are barely one line long, essentially restating the FTC's *de facto* reasonableness standard.[145] The advantage of such a standard is flexibility over time and lack of burden on the FTC to revise guidance in light of changing technology. On the other hand, especially in light of the Equifax data breach, policymakers have sought to provide companies with more specific guidance as to what constitutes reasonable security. For example, the New York Department of Financial Services (NYDFS) recently adopted stringent data security requirements for financial institutions, including annual penetration testing and bi-annual vulnerability assessments, limits on access privileges, and a requirement to designate a chief information security officer who is responsible for the company's security program.[146] The FTC has recently updated its Safeguards Rule with more specific security requirements, consistent with the NYDFS regulation, including placing limits on

[143] Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, Fed. Trade Comm'n Business Blog (Aug. 31, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc.
[144] *Federal Trade Commission 2020 Privacy and Data Security Update*, Fed. Trade Comm'n at 3-4 (2021), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf.
[145] VA SB 1392 § 59.1-574(A)(3) (2021), https://lis.virginia.gov/cgi-bin/legp604.exe?211+ful+SB1392ES1+pdf.
[146] 23 CRR-NY § 500.0 et seq., https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011.

internal access to data, new encryption requirements, and a requirement to establish a chief security officer.[147]

E. Access, portability, correction, and deletion

Privacy frameworks often include provisions giving consumers the right to access, delete, and correct data related to them in the possession of companies. Access rights give accountability and transparency into corporate practices, while correction and deletion rights give consumers some degree of control over data held by companies. Access, correction, and deletion rights have been a core element of European privacy law dating back to the Data Protection Directive, and have been reinforced by the enactment of the Global Data Protection Regulation. Recently enacted state statutes — the CCPA, VCDPA, and CPA — all include access and deletion provisions, and upon adoption of new California provisions under Proposition 24, all will provide a right of correction. (Privacy legislation adopted in Nevada did not include any of these elements — only a weak opt out of data sales.)[148]

To justify mandating data access under its unfairness authority, the FTC could make the plausible case that not knowing what data companies have about them puts consumers at risk of data exposure, and prevents them from making informed choices among market participants. As discussed above, collection and retention of consumer data leaves consumers vulnerable to data breaches and misuse of information by employees, who can use their privileged access to sensitive information to manipulate users.[149] Providing access to that data gives consumers more control over such data — depending on what the consumer finds, they might want to delete, correct, or request to opt out; move their business elsewhere; or potentially report concerns to regulators. Without these access rights, consumers are unable to effectively make decisions about their data in the marketplace.

Existing state privacy laws also typically nod to data portability in their access provisions. For example, the CCPA requires businesses to provide electronic data "in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance."[150] Such provisions are important in giving consumers further control over their data, and greater ability to make choices in the marketplace over their preferred platforms. If the FTC can make a case that access rights forestall injuries stemming from not knowing where data about them is stored, it can also make the case that such data needs to be provided in a commonly-used and accessible format.

The other elements of unfairness are easier to demonstrate for mandating access rights: any injury resulting from not knowing what data is stored about them is certainly unavoidable by

---

[147] *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches*, Fed. Trade Comm'n (Oct. 27, 2021), https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial.
[148] NRS 603A.345, https://www.leg.state.nv.us/nrs/nrs-603a.html.
[149] Adrian Chen, *GCreep: Google Engineer Stalked Teens, Spied on Chats*, Gawker (Sept. 14, 2010) http://gawker.com/5637234/gcreep-googleengineer-stalked-teens-spied-on-chats.
[150] Cal. Civ. Code § 1798.100(d).

consumers, as consumers are otherwise ignorant or potential risk and not empowered to take action. As for countervailing benefits, there are costs associated with providing data access, though those costs are incrementally less for each additional data subject making a request. There also may be costs associated with providing access to derived inferences as well — in that they may cast insight on proprietary algorithms that could be co-opted by others — however, those costs likely do not outweigh the significant value in giving consumers transparency into how companies are classifying and targeting them, especially if such ad targeting implicates job or housing opportunities.

Most of the harms covered by the rules proposed by this paper should not face significant challenge on the premise that the harms are not "prevalent" (as is required by Section 18). In response to privacy law in Europe and states like California, companies have had to develop systems to comply with data access requests. If as a matter of course most companies offer access to those same systems to residents of other states, then a case could be made that deprivation of data access is not, in fact, prevalent. The FTC could conduct an informal inquiry into this empirical question prior to initiating the rulemaking process.

In some cases, the case for correction may be more difficult than the case for access or deletion where there are no clear consequences related to the incorrect information. Receiving untargeted marketing does not seem like a compelling injury. If the data is internal, there are no clear reputational losses, though the data could still potentially embarrass someone if it were later breached or disclosed. FCRA grants correction rights for data that could impact credit and employment,[151] and it would be appropriate to extend correction rights, at the very least, to all scenarios where the data could lead to significant legal effects. The Supreme Court adopted a skeptical view of the harms associated with inaccurate data in cases such as Spokeo[152] and Transunion,[153] though the test for Article III standing is different from the test for unfairness, and the fact patterns in both those cases were somewhat idiosyncratic.

Finally, the FTC would have a strong case to mandate deletion rights for non-necessary data sets as part of an unfairness privacy rulemaking. As discussed *supra*, getting rid of old data that serves no useful purpose should be properly considered as part of a company's data security obligations.[154] For other data that still retains some potential benefit, consumers still are at risk to data exposure or misuse so long as it remains saved. If a user wishes to delete information associated with their account or profile, in many cases it will be difficult to make the argument that there is a countervailing benefit associated with retaining the data against her wishes. Certainly some data should be exempted from deletion rights as is the case under CCPA and other privacy laws — consumers for example are not entitled to delete the fact that

[151] 15 U.S.C. § 1681i.
[152] *Spokeo, Inc.. v. Robins*, 578 U.S. 330 (2016).
[153] *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021).
[154] Compl., *FTC v. SkyMed International, Inc.*, No. 1923140 at ¶ 12(e) (Dec. 16, 2020), https://www.ftc.gov/system/files/documents/cases/skymed_-_complaint.pdf.

they owe a merchant.[155] But for many if not most data sets, the FTC can reasonably argue that failure to respond to deletion requests constitutes an unfair business practice.

F. Prohibition on the use of dark patterns

Finally, any privacy rulemaking could be accompanied by regulations specifically prohibiting the use of "dark patterns" to subvert consumer choice and autonomy. In response to GDPR and the ePrivacy Directive, many companies have resorted to cookie consent interfaces that strongly steer users to granting blanket consent to tracking and that make turning off certain tracking considerably more difficult. While the approaches outlined in this paper are designed to minimize the role of consent and user choice, there is no way to wholly remove individual autonomy from any privacy framework — not should there be. If secondary uses are prohibited, a company may make a pitch for using data for a different primary purpose. If a user globally opts out, a company may be able to ask for an exception. Guardrails must be implemented to ensure that such prompts do not overwhelm or confuse users as an end run around the protections of a Data Minimization Rule.

There is increased precedent on the state level for prohibitions on the use of dark patterns — a prohibition in the CCPA regulations on the use of dark patterns in opt outs;[156] a prohibition in CCPA as amended by Proposition 24, on the use of dark patterns in obtaining consent to opt back into the disclosure of their information,[157] in the Colorado Privacy Act,[158] and in California's new Genetic Information Privacy Act.[159] The measures use similar language, prohibiting interfaces or processes designed with the substantial effect of subverting or impairing user choice. While this is an important first step, to be effective a rulemaking would likely need to be more prescriptive, specifying how privacy disclosures and user interfaces should look. There may be some cost to innovation, but standardization and narrower options would better serve consumers in the long run.

VI. Judicial Review of FTC Unfairness Rules

Federal Trade Commission unfair trade practice rules promulgated under Section 5 of the FTC Act are subject to judicial review in the D.C. Circuit.[160] The Magnuson-Moss Act empowers the FTC to enforce its trade regulation rules.[161] The Mag-Moss rulemaking process contains procedural requirements that are greater than the notice-and-comment requirements of

---

[155] *See*, for example, significant exemptions in the CCPA's right to delete, including to "Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information" Cal. Civ. Code §1798.105(d)(9).
[156] Cal. Code Regs tit. 11 § 999.315(h).
[157] Cal. Civ. Code §1798.140(h).
[158] CO S. 21-190 (2021) § 6-1-1303(5)(c), https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf.
[159] CA SB 41 (2021) § 2(b)(6), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202120220SB41.
[160] 15 U.S.C. § 57a(e); *See generally Am. Fin. Servs. Ass'n v. F.T.C.*, 767 F.2d 957 (D.C. Cir. 1985).
[161] 15 U.S.C. § 57b(a)(1).

the Administrative Procedure Act ("APA").[162] First, the agency must publish an advanced notice of proposed rulemaking describing the topic area for rulemaking, Commission objectives, and regulatory options.[163] The public is then invited to comment on the initial notice.[164] If the FTC finds that the unfair and deceptive practices covered by the proposed rulemaking are "prevalent," it then submits notice to Congress[165] and then must publish a more detailed notice of proposed rulemaking "stating with particularity the text of the proposed rule, including any alternatives."[166] Then, the agency must "conduct an informal hearing at which any interested person can present his position orally or by documentary submission or both, subject to such Commission rules as may tend to avoid unnecessary costs and delay."[167] If the FTC decides that it "must resolve disputed issues of material fact necessary to fair decisionmaking on the record as a whole," Section 18 "entitles interested persons to offer such rebuttal submissions or to conduct (or to have the Commission conduct) such cross-examination of witnesses as the Commission deems appropriate and necessary for a full and true disclosure of facts pertinent to the disputed issues."[168] Finally, the FTC publishes the final rule, along with a statement justifying the rule along with an economic analysis of its effects.[169]

In reviewing a trade regulation rule promulgated by the FTC, an appellate court's role is to "determine if the Commission's finding is supported by substantial evidence on the record as a whole[,]" and not "to reweigh the evidence de novo to determine how we would have resolved the matter."[170] There will likely not be a successful challenge to the proposed rule on the grounds of an insufficient rulemaking process, such as the FTC blocking the introduction of evidence because the extensive rulemaking process will provide the FTC with substantial evidence and provide interested parties the opportunity to submit input.

A. Deference to Agency Interpretations

A party can challenge an FTC-promulgated rule under Mag-Moss or the APA.[171] A court may set aside a Mag-Moss rule if it "finds that the Commission's action is not supported by substantial evidence in the rulemaking record" or if the court finds that the FTC "precluded disclosure of disputed material facts which was necessary for fair determination by the Commission of the rulemaking proceeding taken as a whole" by refusing or limiting the petitioner's cross-examination or rebuttal submissions.[172] The rulemaking record requires "the rule, its statement of basis and purpose, the transcript required by subsection (c)(5), any written submissions, and any other information which the Commission considers relevant to such

---

[162] 5 U.S.C §§ 556–57.
[163] 15 U.S.C. § 57a(b)(2)(A)(1).
[164] 15 U.S.C. § 57a(b)(2)(A)(2).
[165] 15 U.S.C. § 57a(b)(2)(C).
[166] 15 U.S.C. § 57a(b)(1).
[167] *Ass'n of Nat. Advertisers, Inc. v. F.T.C.*, 617 F.2d 611, 614 (D.C. Cir. 1979) (citing 15 U.S.C. § 57a(c)).
[168] *Id.* at 614–15 (citing 15 U.S.C. § 57a(c)).
[169] 15 U.S.C. § 57a(d)(1).
[170] *Thompson Med. Co. v. F.T.C.*, 791 F.2d 189, 196 (D.C. Cir. 1986).
[171] *See* 15 U.S.C. § 57a(e)(3); *see also* 5 U.S.C. § 706(2).
[172] 15 U.S.C. § 57a(e)(3)(A).

rule."[173] Any privacy rule promulgated and challenged under Mag-Moss will thus survive judicial scrutiny so long as the FTC's rulemaking record supports the FTC's determinations and the FTC provides sufficient cross-examination and rebuttal submission opportunities.

"Judicial review of an administrative agency's decision is authorized by the APA."[174] The APA provides that a court "may only set aside agency action that is 'arbitrary, capricious, an abuse of discretion or otherwise not in accordance with law.'"[175] The D.C. Circuit has discussed the arbitrary and capricious standard, opining that the "arbitrary and capricious review requires us to consider whether the FTC action is supported by reasoned decisionmaking,"[176] "whether the agency 'relied on factors which Congress [did] not intend[ ] it to consider,'"[177] and "whether the Rule was promulgated in 'observance of procedure required by law[.]'"[178] The FTC has satisfied the arbitrary and capricious standard when its decision is based "upon consideration of the relevant factors" and is "adequately explained in the administrative record to allow judicial review."[179] Under the FTC's rulemaking procedure, the proposed trade regulation rule would have to be supported by reasoned decisionmaking demonstrated in the formal rulemaking process as is required by the APA, and the FTC would articulate a connection between facts and conclusions. The proposed rule would rely on the FTC's mandate to protect consumers from injuries under §45(n) and could not rely on factors that Congress did not intend for it to consider. The proposed Data Minimization Rule would not be considered arbitrary or capricious because it would be based in reason and supported by evidence provided in the notice and comments period of the rulemaking process.

When an agency interprets an ambiguous statute, their interpretation will be given deference unless it is impermissible. In *New York State Bar Association v. Federal Trade Commission*, the D.C. District Court stated**,** "A challenge to an agency's interpretation of a statute that it administers is subject to deferential review under *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.,* 467 U.S. 837, 104 S.Ct. 2778, 81 L.Ed.2d 694 (1984)[.]"[180] The *Chevron* test is applicable to APA challenges under 5 U.S.C. § 706(2)(C).[181] "Under the well known *Chevron* test… the Court must first examine 'whether Congress has directly spoken to the precise question at issue.'"[182] Further, the Court notes, "It is fair to assume generally that Congress contemplates administrative action with the effect of law when it provides for a relatively formal administrative procedure tending to foster the fairness and deliberation that

[173] 15 U.S.C. § 57a(e)(1)(B).
[174] *Mueller v. England*, 404 F. Supp. 2d 51, 55 (D.D.C. 2005) (citing 5 U.S.C. §§ 701–706).
[175] *Id.* (citing 5 U.S.C. § 706(2)(A)).
[176] *Pharm. Rsch. & Mfrs. of Am. v. F.T.C.*, 790 F.3d 198, 204 (D.C. Cir. 2015) (citing *Allentown Mack Sales & Serv., Inc. v. NLRB,* 522 U.S. 359, 374, 118 S.Ct. 818, 139 L.Ed.2d 797 (1998)).
[177] *Id.* (quoting *Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.,* 463 U.S. 29, 43 (1983)).
[178] *Id.* (quoting 5 U.S.C. § 706(2)(D)).
[179] *Dr. Pepper/Seven-Up Companies, Inc. v. F.T.C.*, 991 F.2d 859, 864 (D.C. Cir. 1993).
[180] *New York State Bar Ass'n v. F.T.C.*, 276 F. Supp. 2d 110, 115 (D.D.C. 2003).
[181] *Id.* at 117.
[182] *Id.* (quoting *Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837, 842-43 (1984)).

should underlie a pronouncement of such force."[183] Next, if the statute is ambiguous or silent with respect to a particular provision, "the question for the court is whether the agency's answer is based on a permissible construction of the statute."[184] The FTC's rulemaking process, which includes notice and comment opportunities, provides a formal administrative procedure. A trade rule regulation promulgated by the FTC under 5 U.S.C. § 45 authority will therefore be granted *Chevron* deference by courts if there is an ambiguity under 5 U.S.C. § 45. With respect to § 45, "substantial injury," "reasonably avoidable," and "countervailing benefits to consumers or competition" may be ambiguous as applied to online behavioral advertising.

The flexible standard of the FTC's unfairness authority will allow the FTC to promulgate privacy rules because courts will give substantial deference to the FTC's factual conclusions and legal interpretations. A legal challenge to an unfairness rule promulgated by the FTC will focus on the three-part test in the statute. As stated previously, an act or practice is unfair when it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[185] As detailed earlier, privacy harms are substantial injuries and the FTC should use its authorities to address these harms under its unfairness authority. The unfairness standard is not rigid and Congress envisioned that the FTC would "develop[] and refin[e] its unfair practice criteria on a progressive, incremental basis."[186] This standard, coupled with the procedural requirements of the Mag-Moss rulemaking process, show that so long as the FTC determines that the online surveillance of internet users is a substantial injury that consumers cannot reasonably avoid without countervailing benefits to consumers or competition, and follows the procedural requirements of the Mag-Moss rulemaking process, the rule will withstand a judicial challenge. There is no question that Congress has clearly delegated rulemaking authority to the FTC that encompasses broad scale commercial regulations with vast economic and political significance[187] and that the FTC has exercised those powers effectively over more than one hundred years.

B. Privacy Rules Can Be Crafted to Withstand First Amendment Scrutiny

Agency actions that restrict or penalize speech are potentially subject to challenge under the First Amendment.[188] The level of scrutiny applied to a law or regulation subject to a First Amendment challenge depends on the type of activity restricted and the impact of the restriction on protected speech. For example, restrictions that only have "indirect impacts on speech" are

---

[183] *United States v. Mead Corp.*, 533 U.S. 218, 230, (2001) ("Cf. *Smiley v. Citibank (South Dakota), N. A.,* 517 U.S. 735, 741, (1996) (APA notice and comment 'designed to assure due deliberation'")).
[184] *Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837, 843 (1984).
[185] 15 U.S.C. § 45(n).
[186] *Am. Fin. Servs. Ass'n v. F.T.C.*, 767 F.2d 957, 978 (D.C. Cir. 1985).
[187] The Supreme Court has recently raised questions about whether such "major questions" can be addressed through administrative rulemaking absent a clear statement from Congress. *See Alabama Ass'n of Realtors v. HHS*, 594 U.S. ___, ___, (slip op. at 6), 141 S. Ct. 2485, 2489 (2021). But here the FTC's authority to promulgate unfair trade practices rules was expressly endorsed by Congress when the unfairness policy statement was codified in the Federal Trade Commission Act Amendments of 1994, Pub. L. 103-312, 108 Stat. 1691, 1695 (1994) (codified at 15 U.S.C. § 45(n)).
[188] *Matal v. Tam*, 137 S. Ct. 1744, 1763–64 (2017).

subject to rational basis review.[189] Even regulations that directly restrict commercial speech are only subject to "relaxed" or "intermediate scrutiny" under *Central Hudson*,[190] which provides that the speech must "at least concern lawful activity and not be misleading; the government interest [must be] substantial; the regulation must directly advance the governmental interest asserted, and the regulation must not be more extensive than is necessary to serve the interest."[191]

Courts have held that the government's interest in protecting privacy is substantial.[192] Courts have repeatedly upheld statutes and regulations that aim to protect informational privacy interests.[193] Indeed, courts have rejected challenges to the Fair Credit Reporting Act and Gramm-Leach-Bliley Act privacy requirements on the grounds that businesses seeking to sell "information about individual consumers and their credit performance" are given "reduced constitutional [speech] protection" under the private commercial speech doctrine.[194] The D.C. Circuit has also upheld the application of opt-in rules to limit downstream uses of personal information.[195] When considering whether the restriction is "no more broad or no more expansive than necessary to serve [the government's] substantial interests," the "only condition is that the regulation is proportionate to the interests sought to be advanced."[196]

VII. Conclusion

The pervasive collection and use of personal data online for secondary purposes causes substantial harm to consumers. The FTC should promulgate a Section 5 unfair trade practices rule to prohibit these widespread and harmful surveillance practices. The Commission has broad authority under Section 5 to address these issues and there are several different ways that they could craft them. We believe that the most effective rule would be a blanket prohibition on most secondary use and third party disclosure with narrow exceptions. This would ensure that consumers are not subjected to unwanted surveillance and unfair data practices.

---

[189] *Barr v. Am. Ass'n of Political Consultants, Inc.*, 140 S. Ct. 2335, 2349 (2020) (Breyer, J., concurring in the judgment with respect to severability and dissenting in part). *See Glickman v. Wileman Bros. & Elliott, Inc.*, 521 U.S. 457, 469–70 (1997).
[190] *Central Hudson Gas & Elec. Corp. v. Pub. Svc. Comm'n of N.Y.*, 447 U.S. 557 (1980).
[191] *Nat'l Cable & Telecomm. Ass'n v. FCC*, 555 F.3d 996 (D.C. Cir. 2009) (internal quotation marks omitted).
[192] *Trans Union Corp v. FTC ("Trans Union I")*, 245 F.3d 809, 818 (D.C. Cir. 2001).
[193] *See, e.g.*, *Nat'l Cable & Telecommunications Ass'n v. F.C.C.*, 555 F.3d 996, 1002 (2009) (upholding the Telecommunications Act privacy rules); *Mainstream Mktg. Servs. Inc. v. FTC*, 358 F.3d 1228, 1246 (10th Cir. 2004) (upholding the Do Not Call Registry rules); *Nat'l Fed. of the Blind v. FTC*, 420 F.3d 321 (4th Cir. 2005) (same); *Trans Union LLC v. FTC ("Trans Union III")*, 295 F.3d 42 (D.C. Cir. 2002) (upholding the Gramm-Leach-Bliley Act privacy protections); *Trans Union I*, 245 F.3d at 818–19 (upholding the Fair Credit Reporting Act prohibition on selling target market lists).
[194] *Trans Union I*, 245 F.3d at 818 (quoting *Dun & Bradstreet, Inc. v. Greenmass Builders, Inc.*, 472 U.S. 729 762 n.8 (1985)).
[195] *Trans Union Corp. v. FTC ("Trans Union II")*, 267 F.3d 1138, 1143 (D.C. Cir. 2001); *Nat'l Cable & Telecommunications Ass'n v. F.C.C.*, 555 F.3d 996, 1001-02 (2009).
[196] *Nat'l Cable & Telecommunications Ass'n v. F.C.C.*, 555 F.3d 996, 1002 (2009).

Organization Descriptions

Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

EPIC is an independent, nonprofit organization that has been focusing public attention on emerging privacy and civil liberties issues since 1994. EPIC works at the intersection of policy, advocacy, and litigation to protect privacy, freedom of expression, and democratic values in the information age. EPIC files briefs in cutting edge privacy cases, files comments and petitions with federal and state regulatory agencies, and provides expert advice to policymakers and lawmakers.