Organisation for Economic Co-operation and Development

DAF/COMP/WD(2024)29

Unclassified

English - Or. English

10 June 2024

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

Cancels & replaces the same document of 10 June 2024

The intersection between competition and data privacy – Note by the United States

13 June 2024

This document reproduces a written contribution from the United States submitted for Item 8 of the 143rd OECD Competition Committee meeting on 12-14 June 2024.

More documents related to this discussion can be found at www.oecd.org/competition/intersection-between-competition-and-data-privacy.htm

Antonio CAPOBIANCO
Antonio.Capobianco@oecd.org, +(33-1) 45 24 98 08

JT03545758

United States[1]

1. Introduction

1. As an agency with the dual missions of enforcing the antitrust and consumer protection laws, the United States Federal Trade Commission ("FTC") believes it is uniquely positioned to share its experiences addressing business practices that raise complex and intertwined privacy and competition policy issues with the joint roundtable session of the OECD Competition Committee and the Data Governance and Privacy Working Party of the Committee on Digital Economy Policy.

2. Digitization of the economy has produced important innovations and conveniences. At the same time, it has also created incentives for businesses to engage in constant surveillance of consumers, including, among many other things, tracking their page views, app activity, screen taps, mouse hovers, and geolocation—even their footsteps within retail stores—and then either selling the data or using it for their own purposes. Often, consumers are unaware that firms are collecting, selling, and otherwise exploiting these types of data. For example, the FTC recently filed a lawsuit alleging that a data broker sold geolocation data from hundreds of millions of mobile devices without consumers' knowledge that could be used to track individuals' visits to potentially sensitive locations, including health clinics, places of worship, domestic violence centers, and addiction recovery facilities.[2] These mass surveillance practices can not only violate consumers' privacy, but they can harm competition too. Firms may use personal data to attain or entrench market power, exploit their market power by extracting excessive personal data, or extract data to raise entry barriers or compete unfairly. The FTC is undertaking multiple initiatives designed to address the harms from business practices involving commercial surveillance, whereby companies collect vast troves of consumer information, much of which consumers do not proactively share and may be collected, used, or sold in ways consumers do not expect.

3. This paper begins by describing the practice and implications of the business of commercial surveillance and identifying key implications for privacy and competition. Next, it explains how the FTC combines its dual authority, tools, and expertise to address mass surveillance in digital markets. It then summarizes the FTC's recent efforts to establish substantive privacy protections and disrupt the incentives at the root of mass surveillance. Finally, it identifies how a more comprehensive approach to data protection may spur greater competition in digital markets, including with regard to safeguarding personal data as well as more broadly.

2. Mass Surveillance in Digital Markets Raises Many Privacy and Competition Concerns

4. Corporations in all sectors of the U.S. economy are using technologies to accumulate massive amounts of data on Americans. These data are often individualized and granular, capturing not only information that consumers proactively share, but also

[1] This contribution was prepared by the United States Federal Trade Commission.

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

information that, unbeknownst to them, is collected. This includes their location, keystrokes, the amount of time their mouse hovers over certain items, videos and products they viewed, and the various apps and websites they use and when they use them.3 Firms collect these and other data to feed algorithms used for many purposes, including personalizing ads, recommending products, generating content (e.g., text, image, video), and, in some cases, even approving or denying applications for credit, employment, and housing.4 Because such algorithms have a virtually unlimited appetite for data—including both historical data about prior activity and real-time information—many firms that use them are devising a myriad of technologies and strategies to harvest even more and newer data.5 These mass surveillance tools and practices raise significant and often interrelated privacy and competition concerns. To address both concerns, the FTC's experience reflects the benefits of applying data protection and competition principles to address these growing threats to both consumers and competition.

5. Firms engaged in mass surveillance often rely on lengthy, jargon-filled privacy policies that contain a disclaimer that the policies are subject to change at will, and that do not actually limit how they use and handle consumers' data.6 As a result, users are unable to make informed decisions nor provide meaningful consent to a firm's data practices. Additionally, long, complex privacy policies inappropriately place the burden of protecting privacy on users, who lack both the time to read endless disclosures as well as sufficient context to decipher opaque terms. Moreover, even if consumers did attempt to parse this burdensome legalese, they often would have no way of rejecting the unwanted data practices other than to forgo use of the internet—an unrealistic option in the modern era. As a result, the notice-and-consent framework fails to protect consumers from mass surveillance practices. From a competition perspective, it is nearly impossible for users to compare these types of privacy policies, either on their face or how they are implemented, making it harder for a firm that is focused on privacy to differentiate itself and win a user's business.

6. The potential profits from mass surveillance incentivize firms to continually weaken their privacy policies.7 For firms that offer consumers "zero-price" products, the

[3] Lina M. Khan, Chair, Fed. Trade Comm'n, Remarks of Chair Lina M. Khan As Prepared for Delivery IAPP Global Privacy Summit 2022, at 6 (Apr. 11, 2022), https://www.ftc.gov/news-events/news/speeches/remarks-chair-lina-m-khan-prepared-delivery-iapp-global-privacy-summit-2022.

[4] Lina M. Khan, Chair, Fed. Trade Comm'n, Remarks of Chair Lina M. Khan Regarding the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking (Aug. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Statement%20of%20Chair%20Lina%20M.%20Khan%20on%20Commercial%20Surveillance%20ANPR%2008112022.pdf.

[5] *See, e.g.*, *Generative AI Raises Competition Concerns*, FED. TRADE COMM'N TECH. BLOG (June 29, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns ("established companies are more likely to have developed and honed proprietary data collection tools and technologies for acquiring or scraping data.").

[6] Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74. 77 (2018); Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1885-86 (2013).

[7] *See* Chris J. Hoffnagle, *Reflections on the NC JOLT Symposium: The Privacy Self-Regulation Race to the Bottom*, 5 N.C. J.L. & TECH. 213, 215 (2004) ("Self-regulation shields companies from accountability and encourages a race to the bottom. It gives little incentive to design products with privacy in mind.").

incentive to monetize more user data is especially high.8 While firms in many industries engage in excessive data collection, the digital advertising business model, in particular, has led firms to surreptitiously change their privacy policies so that they can collect more data and use them in new and unanticipated ways. For instance, a firm that provides a service by collecting limited user data and has a policy that commits it to certain privacy protections may soon encounter business opportunities requiring that it collect more user data, such as selling data to a third party or using data to develop other services.9 The firm faces a tradeoff: pursuing those opportunities or remaining faithful to its existing commitments. With the incentives to profit from the extraction of excessive consumer data, firms are likely to renege on their original privacy commitments or obtain "consent" from users through dark patterns, which are digital design practices that may be used to trick or manipulate users into making choices that they would not otherwise have made.10 While dark patterns are used in many industries, in the context of privacy policies, common dark patterns include burying key terms within dense documents or designing privacy settings or consent prompts in a manner that intentionally steers consumers toward the setting that leads to the lowest protections and the collection of more personal information.11 The following image, reproduced from the FTC's "Bringing Dark Patterns to Light" report,

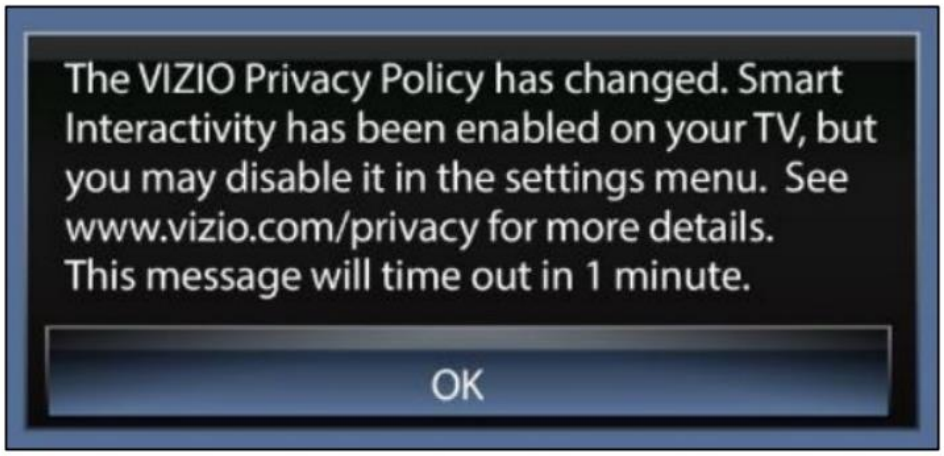
[8] *See* Lina M. Khan, Chair, Fed. Trade Comm'n, Remarks Regarding the 6(b) Orders Concerning Deceptive Advertising on Social Media, at 1 (Mar. 16, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/remarks-of-chair-lina-m-khan-regarding-the-social-media-ad-fraud-6b-final.pdf ("[S]everal of these platforms generally earn their revenue at least in part through behavioral advertising, whereby a platform will collect data on users in order to be able to target them with personalized ads. These platforms' bottom lines depend on user engagement, which tends to result in a business focus on tactics that boost traffic and time spent on the platform.").

[9] *See, e.g.*, Press Release, Fed. Trade Comm'n, Developers of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data (Jan. 13, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about ("Flo disclosed health data from millions of users of its Flo Period & Ovulation Tracker app to third parties that provided marketing and analytics services to the app, including Facebook's analytics division, Google's analytics division, Google's Fabric service, AppsFlyer, and Flurry.").

[10] Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises (Nov. 29, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep-privacy-promises ("In December 2009, Facebook changed its website so certain information that users may have designated as private – such as their Friends List – was made public. They didn't warn users that this change was coming, or get their approval in advance."); Press Release, Fed. Trade Comm'n, FTC Finalizes Order with 1Health.io Over Charges it Failed to Protect Privacy and Security of DNA Data and Unfairly Changed its Privacy Policy (Sept. 7, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-finalizes-order-1healthio-over-charges-it-failed-protect-privacy-security-dna-data-unfairly ("The FTC also charged that the company in 2020 changed its privacy policy by retroactively expanding the types of third parties with which it could share consumers' data without notifying affected consumers or obtaining their consent."); *see also* Press Release, Fed. Trade Comm'n, FTC Takes Action Against Amazon for Enrolling Consumers in Amazon Prime Without Consent and Sabotaging Their Attempts to Cancel (June 21, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-takes-action-against-amazon-enrolling-consumers-amazon-prime-without-consent-sabotaging-their ("Amazon used manipulative, coercive, or deceptive user-interface designs known as "dark patterns" to trick consumers into enrolling in automatically-renewing Prime subscriptions.").

[11] FED. TRADE COMM'N, BRINGING DARK PATTERNS TO LIGHT 22-23, 25-26 (2022), https://www.ftc.gov/reports/bringing-dark-patterns-light.

shows a common tactic that businesses use to get users to "consent" to privacy policy changes.[12]



7. As firms hoover up more and more data that can be tied to individuals, the likelihood and potential consequences of errors increase.[13] For example, feeding inaccurate data into algorithms may inappropriately deny individuals important opportunities, such as credit, employment, and housing.[14] This problem is not theoretical; there are real and substantial harms when businesses use mass surveillance irresponsibly. For example, the FTC recently obtained an order prohibiting the third-largest national drugstore chain, Rite Aid, from using artificial intelligence-based facial recognition technology to surveil customers in its retail pharmacy stores.[15] From 2012 to 2020, Rite Aid used facial

[12] *Id.* at Fig. 9.

[13] Press Release, Fed. Trade Comm'n, FTC Stops Debt Collector's Alleged "Debt Parking" Scheme, Requires It to Delete Debts It Placed on Consumers' Credit Reports (Nov. 30, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/11/ftc-stops-debt-collectors-alleged-debt-parking-scheme-requires-it-delete-debts-it-placed-consumers; *see also* Mary Madden et al., *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 WASH. UNIV. L. REV. 53, 63 (2017), https://journals.library.wustl.edu/lawreview/article/3193/galley/20026/view/ at 63 ("At the same time, these databases are plagued with outdated, inaccurate, and incomplete data. As a result, thousands of people have been denied benefits to which they would otherwise be entitled.").

[14] *See* Press Release, Fed. Trade Comm'n, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (Aug. 11, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices ("As a result, commercial surveillance practices may discriminate against consumers based on legally protected characteristics like race, gender, religion, and age, harming their ability to obtain housing, credit, employment, or other critical needs."); Fact Sheet, Fed. Trade Comm'n, Fact Sheet on the FTC's Commercial Surveillance and Data Security Rulemaking 2 (Aug. 11, 2022), https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking ("These flaws often stem from the design process, such as the use of unrepresentative datasets, faulty classifications, or flawed problem analysis, a failure to identify new phenomena, and lack of context and meaning.").

[15] Press Release, Fed. Trade Comm'n, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without. The FTC's complaint details how, based on false facial recognition matches, Rite Aid employees inappropriately took action against the individuals who had triggered the supposed matches, including subjecting them to increased

recognition technology to identify customers who purportedly may have been engaged in shoplifting and other problematic behavior. However, the FTC alleged that Rite Aid failed to take reasonable measures to prevent harm to consumers who were erroneously accused by employees of wrongdoing because the technology falsely identified them as matching someone who had previously been identified as a shoplifter or troublemaker. To settle these charges, Rite Aid agreed to a ban on facial recognition technology for surveillance purposes for five years and strict safeguards for automated biometric security or surveillance systems in any future system, as well as measures to enhance data security, such as the deletion of any biometric information it collects going forward and the implementation of a robust data security program including independent monitoring, among other things.

8. The perils of data collection are particularly acute in markets involving digital platforms like social networking and e-commerce. Digital platforms often offer a service to a set of users or customers who use the service for little or no monetary cost. Whether or not platform operators charge users a fee, they frequently monetize the service by offering advertising slots to advertisers or collecting fees from transactions that occur between vendors and consumers on the platform. The economics of digital platforms thus provide a strong incentive for firms to collect large volumes of data on their users. Platform operators use this data to offer advertisers products that target very specific groups of users; collecting more information on users allows the platforms to offer more targeted products to advertisers.

9. In addition to monetization, the data that digital platforms collect can be the source of competitive advantage over rival platform operators. Incumbent digital platforms may use data collected from users to monitor potential threats, equipping them to defend and maintain their dominance in a highly targeted manner. These firms can exploit their leverage over dependent users by increasing the demand for valuable personal data or using the extraction of massive amounts of personal data to engage in self-preferencing. Such defensive tactics allow incumbents to protect their dominance by erecting barriers to entry. While it is conceivable that competition could yield some improvements in privacy protections, whether by incumbents or new entrants, today, many incumbents and new entrants continue to pursue the commercial surveillance business model.

10. This mass personal data extraction can entrench firms and exacerbate concentration in already highly concentrated digital markets in several ways. For instance, incumbent firms may use excessive data collection to build moats and insulate themselves from competition. For example, the FTC alleged in its monopolization case against Meta that, unknown to many users, Meta tracked users' activity online to both identify rapidly growing services offered by others that could potentially divert users from Facebook and

surveillance; banning them from entering or making purchases at the Rite Aid stores; publicly and audibly accusing them of past criminal activity in front of friends, family, acquaintances, and strangers; detaining them or subjecting them to searches; and calling the police to report that they had engaged in criminal activity. In many instances, the match alerts that led to these actions were false positives (i.e., instances in which the technology incorrectly identified a person who had entered a store as someone in Rite Aid's database). Among other things, the FTC's complaint alleged that Rite Aid failed to consider or address foreseeable harms to consumers flowing from its use of facial recognition technology, failed to test or assess the technology's accuracy before or after deployment, failed to enforce image quality standards that were necessary for the technology to function accurately, and failed to take reasonable steps to train and oversee the employees charged with operating the technology in Rite Aid stores. The FTC charged that Rite Aid's failures caused and were likely to cause substantial injury to consumers, and especially to Black, Asian, Latino, and women consumers.

identify acquisition targets.[16] In addition, many digital markets are already highly concentrated, and incumbent firms offer apps or services that benefit from network effects (e.g., social media, messaging), which serve as a barrier to competitive entry. These entrenched dominant firms can then exploit their market power by using mass surveillance to extract more data from users or use the data that they collect to identify and thwart emerging threats, some of whom may have sought to offer increased privacy protections. Because many of these apps are necessary for Americans to participate in daily life—as forfeiting connections with family and friends or access to e-commerce are not viable options in the modern era—users have no real choice but to relinquish their data, and, ultimately, their privacy, to these firms.

11. The pervasiveness of entrenched dominant firms that rely on mass data collection results in highly concentrated markets where the barriers to entry can be insurmountable.[17] Whereas incumbent firms have an existing corpus of historical data, as well as the data surveillance infrastructure to continuously update it, new entrants may find it difficult to enter and compete without access to an existing dataset and the infrastructure needed to collect fresh data. As a result, excessive data collection may reinforce barriers to entry, further solidifying many highly concentrated markets.

12. Addressing these privacy and competition concerns does not involve choosing between more privacy and less competition, on one hand, or less privacy and more competition, on the other. Instead, the frameworks of fostering both privacy and competition can be aligned, where competition concerns are addressed once a foundation of baseline privacy protections is established through enforcement and/or legislation. Under such an approach, the goal is to identify a regime that facilitates entry through access to data while, at the same time, reducing the risk that incumbents act as gatekeepers, controlling access to key data needed for entry or expansion.

3. The FTC Is Well Positioned to Address Business Practices Raising Privacy and Competition Issues

13. The FTC's dual mission of consumer protection and privacy and competition, and its array of tools and legal authority, make it well positioned to confront the interrelated privacy and competition harms raised by excessive personal data extraction in digital markets.

14. The FTC's dual missions allow the agency to evaluate business practices from both a competition and privacy viewpoint and fashion solutions that advance each mission in a mutually reinforcing manner.[18] As a general matter, the competition mission seeks to promote rivalry by prohibiting unfair methods of competition and undue concentration, thereby encouraging new market entrants, creating incentives for innovation, and motivating sellers to provide more truthful information about their products and driving them to fulfill their promises concerning price, quality, and other terms of sale. The

[16] Substitute Amended Complaint at ¶ 69, FTC v. Facebook, Inc., No. 20-cv-03590-JEB (D.D.C. Sept. 8, 2021).

[17] *See, e.g.*, FTC v. CCC Holdings Inc., 605 F. Supp. 2d 26, (D.D.C. 2009) (finding that developing and maintaining a new database is a "significant" barrier for new entrants).

[18] *Interoperability, Privacy, & Security*, FED. TRADE COMM'N TECH. BLOG (Dec. 21, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/12/interoperability-privacy-security.

consumer protection mission seeks to eliminate practices that harm or deceive consumers so that honest businesses face fair competition. In the context of mass surveillance, the consumer protection mission focuses on unfair or deceptive practices relating to data privacy,[19] including how firms collect, use, retain, and protect enormous volumes of users' personal data, as well as their representations and omissions regarding those practices.[20] In recent years, the FTC has also increasingly used its unfairness authority to address practices that cause privacy injuries and other related harms to consumers.[21] In short, both missions are deeply connected—firms may engage in privacy violations to build or entrench market power, and that aggregation of market power may, in turn, enable firms to further violate consumer privacy and consumer protection laws.

15. The FTC also has a broad assortment of tools to address the complex, interrelated, and pervasive privacy and competition harms caused by excessive data collection. Along with traditional enforcement actions, the FTC may use rulemaking to address unfair or deceptive practices that the Commission has reason to believe are prevalent,[22] as well as conduct broad market studies[23] or in-depth sector-specific inquiries[24] that are not part of a

[19] Section 5 of the Federal Trade Commission Act prohibits "unfair" and "deceptive" acts or practices and is the FTC's primary source of legal authority in the privacy space. To prove a privacy or data security allegation under Section 5, the FTC must show that a company's conduct is "unfair" or "deceptive." An act or practice is unfair if (1) it causes or is likely to cause substantial injury, (2) the injury is not reasonably avoidable by consumers, and (3) the injury is not outweighed by benefits to consumers or competition. 15 U.S.C. § 45(n). A representation, omission, or practice is deceptive if it is likely to mislead consumers acting reasonably under the circumstances and is material to consumers—that is, it would likely affect the consumer's conduct or decisions with regard to a product or service. *See* FTC Policy Statement on Deception (Oct. 23, 1984) (appended to Cliffdale Assocs., Inc., 103 F.T.C. 110, 183 (1984)), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception. The FTC has pursued privacy and data security cases in numerous areas, including against social media companies, mobile app developers, data brokers, ad tech businesses, and companies in the Internet of Things space.

[20] The Children's Online Privacy Protection Act ("COPPA") provides the FTC with additional statutory authority over the online privacy of children. COPPA gives parents control over what information websites can collect from their children and directs the FTC to issue and enforce regulations concerning children's online privacy. In addition to Section 5 and COPPA, the FTC enforces other privacy laws, including the Gramm-Leach-Bliley Act, which protects the privacy of financial information; the CAN-SPAM Act, which allows consumers to opt out of receiving commercial email messages; the Fair Credit Reporting Act ("FCRA"), which protects the privacy of consumer report information; the Fair Debt Collection Practices Act, which protects consumers from harassment by debt collectors; and the Telemarketing and Consumer Fraud and Abuse Prevention Act, under which the FTC implemented the Do Not Call registry. While important, these and other privacy statutes enforced by the FTC only provide privacy protections in specific situations; they do not provide the same coverage a dedicated federal privacy law would.

[21] Complaint at ¶¶ 35-38, FTC v. Kochava Inc., No. 22-cv-377 (D. Idaho Aug. 29, 2022); Complaint ¶¶ 140-48, FTC v. Rite Aid Corp., No. 23-cv-5023 (E.D. Pa. Dec. 19, 2023).

[22] 15 U.S.C. § 57a.

[23] *See, e.g.*, FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; FED. TRADE COMM'N, BRINGING DARK PATTERNS TO LIGHT (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

[24] Press Release, Fed. Trade Comm'n, FTC Issues Orders to Social Media and Video Streaming Platforms Regarding Efforts to Address Surge in Advertising for Fraudulent Products and Scams

specific law enforcement matter.[25] The FTC can require businesses to answer questions and provide information about their "business, conduct, practices, management, and relation to other corporations, partnerships, and individuals."[26] This power provides the FTC with an important tool that can be used to develop a deeper understanding of market trends and widespread business practices.[27] The FTC also has authority to issue rules regarding unfair methods of competition.[28]

16. The link between protecting consumers and competition is borne out in the FTC's substantial experience promulgating and enforcing rules designed to stop pervasive unfair or deceptive practices that also promote competition. Two examples include:

17. *Eyeglass and Contact Lens Rules.* The Eyeglass and Contact Lens Rules require prescribers, such as optometrists and ophthalmologists, to provide patients with a copy of their prescription immediately after an eye examination or contact lens fitting.[29] The rules also prohibit prescribers from requiring patients to purchase eyeglasses or contact lenses from the prescriber or charging patients a separate fee to obtain their prescription. These rules were designed to address the unfair practice where prescribers conditioned their examination services on the sale of eyeglasses and contact lenses. These rules thus facilitate consumer choice and promote competition in the purchase of eyeglasses and contact lenses, by allowing consumers to fill their prescription at the eyeglass or contact lens retailer that offers them the best combination of price, quality, service, and convenience.[30]

18. *Right to Repair*. In May 2021, the FTC submitted a report to Congress concluding that manufacturers frequently use strategies that make it harder for consumers to fix and maintain their products, including using adhesives that make it difficult to replace parts, limiting the supply of replacement parts and tools, and making diagnostic software unavailable.[31] By employing strategies that limit repairs, manufacturers may increase costs, limit choice, and impact consumers' rights under the Magnuson-Moss Warranty Act ("MMWA"), raising significant consumer protection and competition issues. The MMWA is a consumer protection law passed in 1975 to clarify how written warranties may be used when marketing products to consumers. It requires warrantors of consumer products to provide consumers with detailed information about warranty coverage and prohibits warrantors from tying warranty coverage to the consumer's use of an article or service identified by brand, trade, or corporate name, unless the warrantor provides that article or

(Mar. 16, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-issues-orders-social-media-video-streaming-platforms-regarding-efforts-address-surge-advertising.

[25] 15 U.S.C. § 46(b).

[26] *Id.*

[27] The market study authority does not, however, include remedial powers.

[28] 15 U.S.C. §§ 45, 46(g).

[29] 16 C.F.R. § 315.3(a)(1) (2024); 16 C.F.R. § 456.2(a) (2024).

[30] Am. Optometric Ass'n v. FTC, 626 F.2d 896, 915 (D.C. Cir. 1980) (upholding the rule requiring automatic release of eyeglass prescriptions because there was ample evidence that withholding them harmed consumers by making comparison shopping harder).

[31] Press Release, Fed. Trade Comm'n, FTC Report to Congress Examines Anti-Competitive Repair Restrictions, Recommends Ways to Expand Consumers' Repair Options (May 6, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/05/ftc-report-congress-examines-anti-competitive-repair-restrictions-recommends-ways-expand-consumers.

service without charge or the warrantor has received a waiver from the Commission.[32] The MMWA, thus, improves consumers' access to warranty information, enabling them to comparison shop for warranties. On the competition side, repair restrictions may violate the antitrust laws. For example, a manufacturer might tie the availability of repair parts to the purchase of the manufacturer's repair services. Such a tie could lessen competition and harm consumers in either the repair services or repair parts markets.[33] Following the report to Congress, the FTC issued a policy statement declaring that it would target repair restrictions that violate the antitrust laws or are unfair or deceptive acts or practices under the FTC Act.[34]

19. In each of these examples, a rule or statute disrupted firms' incentives to engage in unfair or deceptive conduct and instead required that they offer their services or products using the most attractive combination of price, quality, and service. Thus, these experiences show that addressing the root cause of a harm by prohibiting certain unfair or deceptive conduct can be an effective way to promote competition broadly.

20. Building on previous work that involved both missions, in 2022, the FTC issued an Advance Notice of Proposed Rulemaking ("ANPR") to explore whether new rules are needed to protect people from commercial surveillance, including the business of collecting, analyzing, and profiting from personal information.[35] In addition to seeking public input on the nature and prevalence of harmful commercial surveillance practices on people's privacy, the ANPR seeks to understand how a rule on data security or commercial surveillance would affect competition. It also seeks information about how limits on targeted advertising, cookies, and other practices could impact competition and innovation, and similarly how algorithmic discrimination may stifle innovation or competition.[36] The FTC uses the information collected from public comments to determine whether to propose new rules.

4. Disrupting the Incentives of Mass Surveillance through Substantive Privacy Protections

21. It can be challenging to address the significant privacy harms resulting from business models relying on extracting data from users. The notice-and-consent framework that has been popular with businesses fails to provide adequate privacy protections for consumers,[37] especially as businesses are quietly changing their policies using dark patterns

[32] 15 U.S.C. § 2302(c).

[33] Eastman Kodak Co. v. Image Tech. Servs., Inc., 504 U.S. 451 (1992).

[34] Press Release, Fed. Trade Comm'n, FTC to Ramp Up Law Enforcement Against Illegal Repair Restrictions (July 21, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-ramp-law-enforcement-against-illegal-repair-restrictions.

[35] Press Release, Fed. Trade Comm'n, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (Aug. 11, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

[36] *See, e.g.*, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, 51284 (proposed Aug. 22, 2022), https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security ("To what extent, if at all, does algorithmic discrimination stifle innovation or competition?").

[37] Lina M. Khan, Chair, Fed. Trade Comm'n, Remarks of Chair Lina M. Khan As Prepared for Delivery IAPP Global Privacy Summit 2022, at 6 (Apr. 11, 2022), https://www.ftc.gov/news-

and dense legal jargon—jargon that consumers have little ability to parse or avoid. Additionally, enforcement actions involving a few firms may fail to deter others while the rewards from mass data collection remain high.

22. Despite these challenges, the FTC will continue to use its authority, tools, and experience to disrupt the incentives fueling mass surveillance as well as the illegal actions themselves.[38] The FTC's recent enforcement efforts highlight the importance of three substantive privacy principles that support fair competition in the face of mass data collection:

- *Data minimization.* A core data privacy protection is for firms to minimize the amount of data they collect and retain, and the FTC has taken action against firms who fail to protect consumer data once they collect it. Following the exposure of sensitive data about millions of individuals because of careless data practices, in October 2022, the FTC required Chegg, an education technology provider, to allow users to request access to and deletion of their data, limit the data the company can collect and retain, implement a comprehensive information security program, and offer users multifactor authentication to secure their accounts.[39] This principle is especially imperative when data is collected from minors. In another matter, the FTC and DOJ settled charges against Amazon that the company violated the

events/news/speeches/remarks-chair-lina-m-khan-prepared-delivery-iapp-global-privacy-summit-2022.

[38] On April 7, 2024, Representative Cathy McMorris Rodgers (R-WA), Chair of the House Committee on Energy and Commerce, and Senator Maria Cantwell (D-WA), Chair of the Senate Committee on Commerce, Science and Transportation, released the *American Privacy Rights Act*. The draft legislation would establish national data privacy rights and protections for Americans and authorize the FTC to enforce the law against violations. The proposal would, among other things, minimize the data that companies can collect and retain, require companies to obtain express consent before transferring sensitive data to a third party, give individuals the ability to prevent the transfer or sale of their data, and require companies to let individuals access, correct, delete, and export their data. Press Release, Committee Chairs Rodgers, Cantwell Unveil Historic Draft Comprehensive Data Privacy Legislation (Apr. 7, 2024), https://energycommerce.house.gov/posts/committee-chairs-rodgers-cantwell-unveil-historic-draft-comprehensive-data-privacy-legislation.

Over the years, the FTC and its leadership have consistently supported federal privacy and data security legislation. *See, e.g.*, FED. TRADE COMM'N, FTC REPORT TO CONGRESS ON PRIVACY AND SECURITY 10 (Sept. 13, 2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf ("[T]he Commission continues to urge Congress to enact privacy and data security legislation, enforceable by the FTC."); FED. TRADE COMM'N, 2019 PRIVACY AND DATA SECURITY UPDATE 12 (2019), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf ("[T]he Commission called for privacy and data security legislation in testimony before the House and Senate Appropriations Committees and the House Energy and Commerce Committee."); Jon Leibowitz, Chair, Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 1-2 (Mar. 26, 2012), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-chairman-jon-leibowitz-prepared-delivery/120326privacyreport.pdf ("We call on Congress to enact legislation addressing data security, which we have long supported, and data brokers – the companies that, without the consent or even knowledge of most consumers, collect and traffic in the data we leave behind as we travel through virtual and brick-and-mortar worlds. We also ask Congress to consider baseline privacy legislation.").

[39] Press Release, Fed. Trade Comm'n, FTC Finalizes Order with Ed Tech Provider Chegg for Lax Security that Exposed Student Data (Jan. 27, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/01/ftc-finalizes-order-ed-tech-provider-chegg-lax-security-exposed-student-data.

Children's Online Privacy Protection Act Rule and deceived parents and users of the Alexa voice assistant about its data deletion practices.[40] Under the settlement, Amazon will have to delete inactive child accounts and certain voice recordings and geolocation information, and will be prohibited from using such data to train its algorithms. In the last several years, the FTC has secured data minimization requirements in more than a dozen cases, a remedy that the FTC had not previously obtained.

- *Restrictions on data use.* A second principle of data privacy is that firms should not collect data for one purpose and then use it for another. Many consumers use Ring's video doorbell and security cameras to protect their homes, but a recent FTC action alleged that Ring provided its employees with unfettered access to customers' videos, where employees used those videos to train image recognition algorithms and even harass and threaten the people whose homes were monitored by Ring cameras.[41]

- *Prohibitions on sharing sensitive data.* Finally, because some data is particularly sensitive, firms should not share sensitive data about users. Data broker X-Mode and its successor company settled charges with the FTC that they sold precise geolocation data that could be used to track people's location, including potentially sensitive places like medical and health clinics, places of worship, and domestic abuse shelters.[42] Under the settlement, X-Mode and its successor will be prohibited from sharing or selling any sensitive location data. As with restrictions on data use, there may be instances where a firm must share sensitive data to provide a service.

23. In addition to enforcement, the FTC is also undertaking other initiatives that could provide the foundation for establishing substantive privacy protections on a much broader scale. In an ongoing study, the FTC is examining how the companies that operate Facebook, Instagram, Messenger, Discord, Reddit, Snapchat, Twitch, TikTok, Twitter, WhatsApp, and YouTube collect and use personal data. In particular, the FTC is seeking to examine how these companies collect, estimate, and derive personal and demographic information, how they determine which content and advertisements to show to users, and how they measure and promote user engagement.[43] These types of in-depth studies can help inform the FTC's policy and enforcement approaches.

[40] Press Release, Fed. Trade Comm'n, FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever.

[41] Press Release, Fed. Trade Comm'n, FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users.

[42] Press Release, Fed. Trade Comm'n, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data (Jan. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

[43] Press Release, Fed. Trade Comm'n, FTC Issues Orders to Nine Social Media and Video Streaming Services Seeking Data About How They Collect, Use, and Present Information (Dec. 14, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/12/ftc-issues-orders-nine-social-media-video-streaming-services-seeking-data-about-how-they-collect-use.

24. Even with enforcement actions, industry studies, and the development of rules, the FTC may encounter obstacles in its work to protect consumers from excessive data collection. The business of mass surveillance is complex and subject to rapid technological change. Additionally, the firms engaged in commercial surveillance include many well-resourced businesses who could lose their dominant market positions and significant profits if stronger privacy protections went into place. Thus, they may seek to challenge any legislation or rules establishing substantive privacy protections.

5. Changing the Incentives for Business Models Premised on Mass Surveillance May Promote Competition

25. The FTC and the U.S. Department of Justice have long recognized and recently emphasized the importance of non-price competition in their enforcement of the antitrust laws, and that privacy can be a key form of non-price competition.[44] Conversely, in less competitive markets, we often see dominant firms exploiting their market power to mass collect user data and minimize privacy protections for consumers. In addition, by reducing businesses' incentives to engage in excessive data collection, protecting consumer privacy could spur the development of new business models that do not rely on invading users' privacy. In particular, rules limiting the amount and types of data that firms can collect, as well as prohibiting how firms can use and share those data, could enhance the competitive process in several ways:

- *Lower entry barriers.* If firms are no longer able to collect certain types of data, new entrants may have an easier time competing on a level playing field because they will no longer need as much data or the data collection and surveillance infrastructure they would have otherwise needed.
- *Greater symmetry of information.* Data minimization and limits on how data can be used could facilitate greater information symmetry between consumers and businesses. With such rules, privacy policies should be shorter and more understandable, as firms may not need lengthy and incomprehensible lists of all the data they collect and the myriad ways in which they can be used. Short, understandable policies then should facilitate meaningful comparison shopping by consumers, where they can compare firms' data practices and consider them alongside other important price and non-price terms. This should provide users greater control over how their personal information is used.
- *Hamper moat building.* Restrictions on the amount of data that firms can collect and how they can use it could also make it more difficult for dominant firms to track the other apps and services that their users use, or the products that users buy.

[44] *See, e.g.*, Complaint at ¶¶ 10, 85, 143-47, United States v. Apple Inc., 24-cv-04055 (D.N.J. Mar. 21, 2024); Substitute Amended Complaint at ¶¶ 105, 221-22, FTC v. Facebook, Inc., No. 20-cv-03590-JEB (D.D.C. Sept. 8, 2021) (alleging that greater competition would "enable[] users to select a personal social networking provider that more closely suits their preferences, including, but not limited to, preferences regarding the amount and nature of advertising, as well as the availability, quality, and variety of data protection privacy options for users, including, but not limited to, options regarding data gathering and data usage practices." "Without meaningful competition, Facebook has been able to provide lower levels of service quality on privacy and data protection than it would have provided in a competitive market."). The recently released Merger Guidelines allow the FTC and DOJ to use the "SSNIPT" test to evaluate worsened non-price terms, an especially useful tool in zero-price markets. U.S. Dep't of Just. & Fed. Trade Comm'n, Merger Guidelines, 41-42 (2023), https://www.justice.gov/d9/2023-12/2023%20Merger%20Guidelines.pdf.

Without comprehensive insights into the apps users use, how much they use them, and the features they use, dominant firms may have less ability to build moats and exclude nascent competitors.

- *Level playing field.* Rules limiting firms' data practices could level the competitive playing field. Today, first-time violations of the FTC Act, such as unfair or deceptive privacy practices, do not result in civil penalties. Under duly promulgated rules, for example, all violators, including first-time violators, would be subject to civil penalties if they acted 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.[45] If all firms are subject to civil penalties, a given firm will not be able to gain a competitive advantage through an initial privacy violation.

26. The FTC may face challenges achieving these competition goals even with a privacy regime that discourages mass data collection. In particular, established dominant firms may attempt to insulate themselves from competition because they have already amassed massive troves of user data and the corresponding insights from the data that new entrants will be unable to replicate. To be sure, traditional enforcement actions may be able to curtail at least some unlawful conduct by such firms, including depriving parties the benefits from their past illegal actions, as broad remedies are available in antitrust cases.[46] However, any such actions could be time-consuming and resource intensive. Nevertheless, substantive privacy rules could play a role in preventing certain markets from tipping.

6. Conclusion and Horizon Scanning

27. Through its work, the FTC is attempting to use its tools to establish substantive restrictions on the amount of data that firms can collect on consumers, as well as limits on how they can use such data. For example, the FTC is considering whether to propose rules regarding commercial surveillance and data security practices that harm consumers. If adopted, such rules would provide general privacy protections to all Americans. These rules may lessen the incentives for businesses to engage in excessive data collection and

[45] Press Release, Fed. Trade Comm'n, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (Aug. 11, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

[46] The availability of broad remedies in antitrust cases may be a way to restore some competition lost because of anticompetitive data collection practices. *See* United States v. United Shoe Mach. Corp., 391 U.S. 244, 250 (1968) ("[I]t is the duty of the court to prescribe relief which will terminate the illegal monopoly, deny to the defendant the fruits of its statutory violation, and ensure that there remain no practices likely to result in monopolization in the future."). For instance, a firm that maintained its monopoly by engaging in exclusionary data collection practices could potentially be required to delete that data, as well as any associated algorithms. In fact, in recent privacy cases, the FTC has secured orders requiring defendants to delete data obtained in violation of Section 5 of the FTC Act. *See supra* ¶ 19(a). In certain cases, requiring firms to delete algorithms trained on unlawfully collected data may also be appropriate, as firms may consider monetary penalties as a "cost of doing business." Interview by Guy Rolnik with Jonathan Kanter, Assistant Atty. Gen., Antitrust Div., U.S. Dep't of Just., and Lina Khan, Chair, Fed. Trade Comm'n, in Chicago, Ill. (Apr. 18, 2024), https://www.promarket.org/2024/05/22/dinner-keynote-with-jonathan-kanter-and-lina-khan-transcript/ (Lina Khan: "[A] core part of the remedy has to be not just deletion of the data but also deletion of any algorithms or models that were trained on that unlawfully gotten data. Because if you're just focused on things like fines, you can see how illegally collecting data could just be a cost of doing business[.]").

encourage them to compete in a race to the top on privacy, resulting in more protections for consumers, not less. With privacy-degrading business models less viable, firms would be pushed to develop new business models and products that do not depend on constant and extensive surveillance of all aspects of people's lives, including when they are not even actively using their devices. In this way, general privacy protections could also encourage competition.

28. The FTC is closely monitoring advancements in technology to identify markets that may involve excessive data collection and the role that could play in leading those markets to becoming dominated by a handful of firms. In particular, the FTC is considering whether markets involving artificial intelligence may be at risk because AI models, especially generative AI models, have a nearly endless appetite for data. Left unchecked, AI firms may be training their models on data that raise substantial privacy concerns, such as personal emails and location data, without consumers' knowledge or consent. Additionally, it appears that only a few firms currently control the substantial computing resources required to train AI models.[47] The FTC already recognizes that firms developing AI products may try to renege on their existing privacy commitments to collect even more training data, potentially helping them to buttress their market position.[48] Rapid changes in AI technology and market dynamics, along with recognition that past missteps may have contributed to tipping in other digital markets, impel the FTC to, at a minimum, closely scrutinize AI firms' practices to ensure that they do not run afoul of privacy and competition laws.

[47] *Generative AI Raises Competition Concerns*, FED. TRADE COMM'N TECH. BLOG (June 29, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns.

[48] *AI Companies: Uphold Your Privacy and Confidentiality Commitments*, FED. TRADE COMM'N TECH. BLOG (Jan. 9, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/01/ai-companies-uphold-your-privacy-confidentiality-commitments.