September 14, 2022

FTC Conducts Public Forum On "Commercial Surveillance" and Data Security

On September 8, 2022, the Federal Trade Commission ("FTC") held a public forum on "commercial surveillance" and data security practices to solicit public comment on potential harms of these practices to consumers and competition. The public forum was conducted to guide the FTC in determining whether to proceed with rulemaking under Section 18 of the FTC Act, otherwise known as Magnusson-Moss ("Mag-Moss") rulemaking, as well as to inform any potential rulemaking. The public forum follows the FTC's issuance of an Advance Notice of Proposed Rulemaking ("ANPR") on data security practices on August 11, 2022.[1]

The public forum included opening comments from FTC Chair Lina Khan and remarks from Commissioners Rebecca Kelly Slaughter and Alvaro Bedoya. FTC staff also solicited comments from industry representatives and consumer advocates during two panel discussions, and fielded dozens of public comments.

In their remarks, the Commissioners discussed using Section 18 rulemaking to expand the definition of what constitutes "unfair" data privacy practices beyond violations of procedural "notice and choice" based privacy protections, and to impose broader "substantive" requirements, such as marketplace-wide limitations on the collection or processing of data in certain contexts. Such an expansion would enable the FTC to use its Section 5 authority to bring enforcement actions related to a wider range of conduct that would constitute unfair data privacy practices under the new rules.

The panels and public comments explored other topics covered by the ANPR, including potential discrimination based on protected categories by automated systems, as well as increasing regulator visibility into online platforms to enable the FTC to identify and address potential violations. The discussion highlights the Commission's ongoing enforcement priorities in the area of data privacy and security.

Key Takeaways

- The FTC is intently focused on potential harms resulting from large-scale data collection through "commercial surveillance" practices, which the FTC defines as the "business of collecting, analyzing, and profiting from information about people."[2] Discussion at the public forum suggests that the FTC is interested in both overt collection of data from consumers, as well as indirect data collection practices for purposes such as cross-platform tracking, advertising targeting and other means of gathering data about consumers.

- The participating Commissioners view the public forum as a key step in the Section 18 rulemaking process, which the FTC may use to expand its authority under Section 5 to address what they view as "unfair" data privacy practices. The Commissioners appear to be contemplating industry-wide standards that, if not adhered to, would permit the FTC to seek monetary relief from targets of enforcement actions.[3]

- Any future rulemaking likely will go beyond existing procedural protections such as notice and choice requirements to address what might be viewed as substantive unfair data privacy practices, including by imposing limitations on the collection and processing of certain consumer data. For example, the Commissioners appear to be contemplating new rules that would limit companies to collecting only the data "reasonably necessary" to providing the product or service specifically requested by the consumer. In his remarks, Commissioner Bedoya observed that existing privacy and data security regimes enforced by the FTC already contain such substantive requirements.

- Companies should consider evaluating their existing data collection and security practices against some of the "best practices" identified during the public forum, such as encrypting data in transit, maintaining incident response policies, conducting risk assessments, implementing access controls such as multi-factor authentication and password requirements, ensuring data backups and resilience, implementation of regular software patching and updates, and utilization of anti-malware software.

Background of the Public Forum

The Section 18 rulemaking and ANPR follow a recommendation in President Biden's July 2021 Executive Order on Promoting Competition in the American Economy, which encouraged the FTC to exercise rulemaking authority in areas such as "unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy."[4]

Many of the principal issues addressed during the public forum were foreshadowed by Chair Khan during her April 11, 2022 keynote address at the 2022 IAPP Global Privacy Summit. During her April speech, Chair Khan raised the possibility of FTC rulemaking that would prohibit certain types of data collection practices entirely, beyond current notice and choice requirements, which Chair Khan described as potentially "outdated and insufficient." This focus on potential substantive limitations on data collection practices was a primary focus of the remarks by the FTC Commissioners at the public forum and of the questions posed to panelists and suggests that such limitations may be a feature of any future proposed rulemaking in this area.

In calling for the public forum, Chair Khan cited the "growing digitization of our economy" purportedly characterized by companies that "collect personal data on a massive scale and in a stunning array of contexts" and "business models that can incentivize endless hoovering up of sensitive user data and a vast expansion of how this data is used."[5] Chair Khan asserted that "case-by-case enforcement" to date has "fail[ed] to adequately deter lawbreaking or remedy the resulting harms" of potentially unlawful use and collection of sensitive user data.[6] In other public statements leading up to the public forum, Commissioners emphasized that rulemaking focused on data privacy that "establish[es] clear privacy and data security requirements across the board and provide[s] the Commission the authority to seek financial penalties for first-time violations could incentivize all companies to invest more consistently in compliant practices."[7]

The ANPR defines "commercial surveillance" as the "business of collecting, analyzing, and profiting from information about people."[8] The ANPR posed 95 questions across the following four broad categories for public comment and discussion, including 1) the extent to which "Commercial Surveillance Practices" or lax data security measures harm consumers; 2) the extent of harm to children and teenagers from "Commercial Surveillance" and lax data security; 3) how to balance the costs and countervailing benefits of additional rulemaking; and 4) how and whether the FTC should regulate harmful "Commercial Surveillance" or data security practices.[9]

The Commissioners' Remarks

During her introductory remarks, Chair Khan emphasized the "need for urgency and rigor" in determining whether the FTC would proceed with proposed rulemaking, and what form the proposed rules should take. To proceed with Section 18 rulemaking the FTC must have "reason to believe" that "unfair or deceptive practices are prevalent," which may be shown by the issuance of "cease and desist orders regarding such acts or practices" or other information indicating "a widespread pattern of unfair or deceptive acts or practices."[10] Chair Khan stated that the discussion and comments at the public forum would be

"critical" for determining whether the Commission has an "evidentiary basis for proceeding with the rulemaking and whether we meet the legal requirements for creating any particular type of rule." [11]

Commissioner Slaughter noted that while she "support[s] strong federal privacy legislation," presumably referring to the American Data Privacy and Protection Act ("ADPPA"), which stands poised for a vote in Congress, "until there's a law on the books, the Commission has a duty to use all the tools we have to investigate and address unlawful behavior in the market." [12] She characterized the initiation of the rulemaking process as "a bookend to the long era of not appropriately exercising our rulemaking authorities." She also, however, encouraged active engagement by industry in the rulemaking process to "ensure that any possible rules are effective and not just a burdensome compliance exercise." [13]

Commissioner Bedoya's remarks focused in part on attempting to demonstrate that American privacy law historically has not been limited to "notice and choice" requirements, stating that, "from the very beginning of American commercial privacy law, privacy harms and privacy rights to protect against those harms have gone well beyond that initial point of collection. They've extended to use, purpose, specification, commercialization, security, sharing, fair access, correction, etc." By way of example, Commissioner Bedoya pointed to the Fair Credit Reporting Act, the Children's Online Privacy Protection Act ("COPPA") and the Safeguards Rule of the Gramm-Leach-Bliley Act, which he said in "sum total . . . go far beyond that initial question of notice and choice." [14]

Other Topics Addressed

Although the FTC also solicited input on other topics such as the administrability of certain rules and regimes, including decisions between self-regulation and binding rules, participants in the forum focused primarily on substantive issues that may be addressed in future proposed rulemaking. Participants in the public forum addressed, among other topics:

- **Expansion of FTC's authority to enforce unfair data practices.** Comments included proposals for rules that would: 1) limit broad scale, "non-contextual data collection and tracking" by parties with whom consumers do not expressly interact; and 2) implement data minimization requirements that would limit the collection of data to align with consumer "expectations" and permit collection only of data that is "reasonably necessary" for the product or service provided.

- **Notice and consent.** Certain participants, including Commissioner Bedoya, expressed the view that notice and choice-based privacy protections were insufficient to address potential harm from "commercial surveillance" practices and data security lapses. Representatives from consumer advocate organizations similarly characterized measures designed to ensure adequate disclosures and effective consent as inadequate "individual interventions." [15]

- **Establishing uniform definitions and interpretations.** Comments during the public forum discussed establishing uniform definitions for commonly used data privacy terms and concepts such as "de-identification" and "anonymization" of data, as well as what categories of data should be considered sensitive personal data.

- **Potential vulnerable groups.** Participants in the public forum identified several particular groups of consumers who may face potential risk of harm from certain data security practices, such as automated decision-making and large-scale data collection. Identified groups included children and teens who have aged out of protections under COPPA, minorities and underrepresented groups, students, and users of large internet platforms. Consumer advocates argued that automated decision-making based on large-scale data collection may subject certain communities to discrimination when seeking credit, housing, employment or when voting.

- **Data security best practices.** Several commentators offered their view on "best practices" to address potential lapses in data security, including: encrypting data in transit, maintaining incident response policies, conducting risk assessments, implementing access controls such as multi-factor authentication and password requirements, ensuring data backups and resilience, regular software patching and updates and the use of anti-malware software. Both industry representatives and

consumer advocates also highlighted developments such as the Global Privacy Control, which allows internet users to notify businesses of their privacy preferences through a browser's setting or a browser extension.[16]

If, through the notice and comment period, the Commission determines, before the October 21, 2022 deadline, that it has established an adequate evidentiary record that there is "reason to believe" that existing data security and "surveillance" practices likely to be targeted by the proposed rulemaking are "prevalent," the Commission will likely move on to crafting proposed rules to be released in a Notice of Proposed Rulemaking ("NPR"), followed by an opportunity for industry, consumers, and others to provide further input during hearings on the NPR.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Yahonnes Cleary
+1-212-373-3462
ycleary@paulweiss.com

Meredith R. Dearborn
+1-650-208-2788
mdearborn@paulweiss.com

Harris Fischman
+1-212-373-3306
hfischman@paulweiss.com

Michael E. Gertzman
+1-212-373-3281
mgertzman@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Richard C. Tarlowe
+1-212-373-3035
rtarlowe@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

Associates Cole A. Rabinowitz and Carter Greenbaum contributed to this Client Memorandum.

---

1 *See* FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices, (August 11, 2022), *available at* https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

2 *See* Commercial Surveillance and Data Security Rulemaking, (August 11, 2021), *available at* https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking.

3 16 C.F.R. §§ 0.16, 0.17 (2021). The Supreme Court decision in *AMG Capital Management LLC* v. *FTC*, 593 U.S. ___ (2021) does not prevent the FTC from obtaining monetary relief through enforcement of a rule.

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

5 *See* FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices, (August 11, 2022), *available at* https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

6 *See* Statement of Chair Lina M. Khan Regarding the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking, (August 11, 2022), *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-chair-khan-regarding-commercial-surveillance-data-security-advance-notice-proposed.

7 *See* FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices, (August 11, 2022), *available at* https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

[8] *See* Commercial Surveillance and Data Security Rulemaking, (August 11, 2021), *available at* https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking.

[9] *See* Trade Regulation Rule on Commercial Surveillance and Data Security, 87 FR 51273 (Aug. 22, 2022) (to be codified at 16 CFR__), *available at* https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security.

[10] *See* 15 U.S.C. § 57a(b)(3).

[11] *See* Remarks of FTC Chair Lina Khan, FTC Commercial Surveillance and Data Security Public Forum, (September 8, 2022), *available at* https://kvgo.com/ftc/commercial-surveillance-sep-8.

[12] *See* Dissenting Statement of Commissioner Christine S. Wilson, Trade Regulation Rule on Commercial Surveillance and Data Security, (August 11, 2022), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Wilson%20Dissent%20ANPRM%20FINAL%2008112022.pdf.

[13] *See* Remarks of Commissioner Rebecca Kelly Slaughter, FTC Commercial Surveillance and Data Security Public Forum, (September 8, 2022), *available at* https://kvgo.com/ftc/commercial-surveillance-sep-8.

[14] *See* Remarks of Commissioner Alvaro Bedoya, FTC Commercial Surveillance and Data Security Public Forum, (September 8, 2022), *available at* https://kvgo.com/ftc/commercial-surveillance-sep-8; 16 C.F.R. §312.7; 16 C.F.R. § 314.3(a).

[15] *See* Panel 2: Consumer Advocate Perspectives on Commercial Surveillance and Data Security, Comments of Harlan Yu, FTC Commercial Surveillance and Data Security Public Forum, (September 8, 2022), *available at* https://kvgo.com/ftc/commercial-surveillance-sep-8.

[16] *See* Frequently Asked Questions, Global Privacy Control, *available at* https://globalprivacycontrol.org/.