Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

FTC Considers Adopting Commercial Surveillance and Data Security Rules

October 12, 2022

On August 11, 2022, the Federal Trade Commission (FTC) issued an Advanced Notice of Proposed Rulemaking (ANPRM) announcing that the agency is considering enacting new regulations on "commercial surveillance" and data security. The ANPRM is significant because it initiates a process that may result in rules comprehensively regulating companies' data privacy and data security practices. While the FTC has long been active in protecting consumers' data against misuse, its role has primarily been limited to case-by-case enforcement of the Federal Trade Commission Act's (FTC Act's) broad prohibition on "unfair or deceptive acts or practices." Adopting generally applicable regulations that articulate particular data privacy and data security requirements or prohibitions would be a notable change from this case-by-case approach. The ANPRM is also noteworthy because it would be the first time in decades that the FTC has adopted a wholly new "Trade Regulation Rule" (TRR) (i.e., a rule adopted under Section 18 of the FTC Act).

This Sidebar begins by providing a brief background on the FTC's current role as a data privacy and data security enforcer. The Sidebar then explains the FTC's authority under the FTC Act to enact TRRs and the procedures that it must follow. The Sidebar then summarizes the commercial surveillance ANPRM, and closes by discussing some considerations for Congress.

The FTC's Role as a Privacy Enforcer

As discussed in this CRS report, there is no single comprehensive federal law governing how companies gather and use consumer data. Rather, there is a collection of targeted privacy statutes that are generally directed at particular types of entities (e.g., healthcare entities, financial institutions, and communications common carriers) or specific types of data (e.g., children's data). While the FTC enforces some of these statutes, the core of its data privacy and data security enforcement authority comes from Section 5 of the FTC Act. Section 5 prohibits "unfair or deceptive acts or practices" (UDAPs) "in or affecting commerce." The FTC is empowered to enforce this prohibition against all persons, partnerships, or corporations, other than a handful of exempt entities like common carriers and banks.

Section 5's UDAP prohibition is different from typical privacy statutes in that it does not specify certain requirements or prohibitions with which all covered entities must comply. For instance, the FTC Act does

Congressional Research Service
https://crsreports.congress.gov
LSB10839

not impose a bright-line requirement that entities obtain consumers' consent before collecting their data or allow consumers to request, correct, or delete their data. Rather, the UDAP prohibition is a broad standard that the FTC applies to specific factual circumstances. In any UDAP enforcement action, the FTC typically seeks to demonstrate that the defendant's actions, in light of the totality of the circumstances, were either (1) deceptive because they were likely to mislead reasonable consumers about a material fact, or (2) unfair because they unjustifiably and substantially harmed consumers in a way that the consumers could not reasonably avoid.

The FTC has used this broad standard to become, as some commentators have said, the "go-to agency for privacy." The FTC has brought hundreds of enforcement actions alleging that companies' data privacy or data security practices are deceptive or unfair. For instance, the FTC has maintained that companies act deceptively when they handle personal information in a way that contradicts their posted privacy policies or other statements, or when they fail to adequately protect personal information from unauthorized access despite promises that they would do so. The FTC has also alleged that companies' data practices are unfair when, for example, they have default privacy settings that are burdensome to change, retroactively apply a revised privacy policy, or fail to adopt reasonable safeguards to protect personal information. Most of the FTC's data privacy and data security enforcement actions are settled rather than fully litigated, which has resulted in relatively sparse case law on the UDAP prohibition's application. Courts have, however, generally recognized the UDAP provision's flexible nature; at least one court has agreed with the FTC's position that a company's failure to safeguard user data may, in some circumstances, be "unfair" under Section 5.

In Section 5 UDAP enforcement actions, the FTC may obtain a cease-and-desist order through an administrative process or an injunction in federal court. As discussed in another Sidebar, however, it is largely precluded from obtaining monetary relief from first-time violators. The FTC generally may only obtain monetary penalties in Section 5 UDAP actions when a company violates a cease-and-desist order or a consent order. Furthermore, it may only obtain equitable monetary relief, such as restitution or disgorgement, when it firsts obtains an administrative cease-and-desist order and then brings a follow-on action in federal court, where it must show that a reasonable person would have known that the defendant's conduct was dishonest or fraudulent.

The FTC's Trade Regulation Rules

Section 18 of the FTC Act allows the FTC to issue TRRs defining specific acts or practices as unfair or deceptive. In contrast to Section 5 UDAP violations, entities that violate TRRs are subject to civil penalties and a broad range of monetary and other equitable relief. The FTC's process for enacting TRRs under Section 18 of the Act is often referred to as Magnuson-Moss rulemaking, as these procedures were largely added in 1975 by the Magnuson-Moss Warranty-Federal Trade Commission Improvements Act.

Magnuson-Moss rulemaking requires the FTC to comply with several procedures that go beyond the typical notice-and-comment rulemaking procedures under Section 553 of the Administrative Procedure Act, which are the default rulemaking procedures for federal agencies. Under typical notice-and-comment rulemaking, an agency issues a notice of proposed rulemaking (NPRM) and gives interested persons an opportunity to comment on it before issuing a final rule. In Magnuson-Moss rulemaking, the FTC must first issue an ANPRM that contains a brief description of the issue and invites interested persons to submit responses. Following the ANPRM, the FTC may only proceed with the rulemaking if it determines that it has either issued cease-and-desist orders regarding such acts or practices or has any other information indicating a "widespread pattern" of unfair or deceptive acts or practices.

If the FTC decides to proceed with the rulemaking, it must issue an NPRM and give interested persons an opportunity to comment, as well as provide for an informal hearing to resolve any disputed issues of material fact. These informal hearings are overseen by a Chief Presiding Officer and include oral

testimony and, to the extent necessary, opportunities for cross-examination and rebuttals. Following the informal hearing, the Chief Presiding Officer must recommend a decision to the Commission based on the Officer's findings and conclusions of all the material evidence. The FTC's final rule must be accompanied by a statement of basis and purpose, which describes the prevalence of the acts or practices covered by the rule, the manner and context in which the acts or practices are unfair or deceptive, and the economic effect of the rule. There are also several requirements throughout the process that foster increased congressional oversight, such as a requirement that the FTC submit the NPRM to its congressional oversight committees 30 days before publication.

The FTC has infrequently used Magnuson-Moss rulemaking. Most of the FTC's existing TRRs—such as its Unavailability Rule, Prenotification Negative Option Plan Rule, and Franchise Rule—were initiated or finalized before Magnuson-Moss rulemaking procedures took effect. Since 1980, the FTC has used Magnuson-Moss rulemaking to update existing rules rather than to initiate new rulemakings. The FTC has shown a renewed interest in Magnuson-Moss rulemaking, however. In July 2021, the FTC changed its rules of practice to streamline some of the Magnuson-Moss rulemaking requirements, eliminating what it referred to as "self-imposed red tape" that imposed hurdles beyond what Section 18 requires. For instance, the revised rules allow the FTC Chair to designate or serve as the Chief Presiding Officer in informal hearings and allow the Commission to designate disputed issues of material fact for these hearings earlier on in the process.

The Commercial Surveillance ANPRM

On August 22, 2022, the FTC published an ANPRM that asked for public comment on whether it should adopt new TRRs on companies' commercial surveillance and data security practices. The ANPRM observed that there is an "elaborate and lucrative market" for consumer information. Companies collect, aggregate, analyze, and disclose consumer data so they can target services and advertisements toward consumers and better understand consumer behavior. The ANPRM explained that, while these "personalization practices" have the potential to benefit consumers, they reportedly also facilitate consumer harms. The ANPRM specifically noted that commercial surveillance practices may, among other things, make it more likely that "cyberattack[s]" will result in identity theft or fraud, allow bad actors to target fraudulent products to vulnerable consumers, and lead to a greater reliance on algorithms that discriminate against consumers based on protected characteristics (such as race, sex, and age) for things like housing, employment, and healthcare.

The ANPRM also discussed the limitations of the FTC's case-by-case enforcement of companies' data privacy and security practices. The ANPRM emphasized the limited remedies the FTC may obtain for first-time Section 5 UDAP violations and how the FTC's limited resources make it difficult to address the multitude of commercial surveillance and data security practices through case-by-case enforcement.

To build a record for a potential rulemaking, the FTC requested comment on a wide variety of issues related to commercial surveillance and data security. While it did not "delineate a boundary" on the issues that commentators may address, it specifically asked for comments on topics such as:

- the scope of personal data that should be subject to a rule;
- the extent to which commercial surveillance practices or lax security measures harm children and minors;
- whether rules should address companies' data security practices and whether they should be informed by data security requirements in existing laws, such as the Gramm-Leach-Bliley Act and the Children's Online Privacy Protection Act;
- whether rules should address the use of facial recognition or biometric technology;

- whether rules should impose data-minimization requirements or limit data's use based on the purpose for which the consumers provided the data;
- whether rules should require companies to take steps to prevent algorithmic errors;
- the prevalence of algorithmic discrimination and the Commission's authority to address it;
- the effectiveness of consumer consent;
- the extent to which a rule should require companies to disclose their commercial surveillance practices; and
- how the FTC should account for changes in business practices that may render a rulemaking obsolete.

The ANPRM explained that, even if the Commission does not ultimately promulgate regulations, comments on these issues would sharpen its enforcement work and may inform Congress and other policymakers. The ANPRM also announced a public forum, which was held on September 8, 2022, in which panelists and members of the public made remarks on the topics addressed in the ANPRM.

The ANPRM was approved by the Commission by a 3-2 vote. Chairwoman Lina Khan, Commissioner Rebecca Kelly Slaughter, and Commissioner Alvaro Bedoya voted in favor of the ANPRM. Commissioners Noah Phillips and Christine Wilson dissented. The dissenting commissioners reasoned that Congress, rather than the FTC, is the proper body to adopt nationwide consumer data and privacy rules. The dissenting commissioners also criticized the breadth of the ANPRM and its inclusion of topics that have not traditionally been the subject of its UDAP enforcement actions. For instance, Commissioner Phillips expressed concern that the Commission appears to be considering banning targeted advertising, facial recognition technology, and automated decisionmaking technology, although the FTC has never found these practices to be unfair.

Considerations for Congress

Whether the FTC follows through with its commercial surveillance and data security rulemaking may in large part depend on whether Congress enacts comprehensive privacy legislation. As discussed in this Sidebar, on July 20, 2022, the House Energy and Commerce Committee voted to advance the American Data Privacy and Protection Act (ADPPA) to the full House of Representatives. Should the ADPPA be enacted, it would direct the FTC to oversee a comprehensive privacy framework. In the ANPRM, both the majority commissioners and the dissenting commissioners expressed enthusiasm for the ADPPA, although they drew different conclusions about its implications for the FTC's rulemaking process. Commissioner Slaughter maintained that the Commission should not sit "idly by" while Congress deliberates, and that any record developed through the Commission's rulemaking would benefit Congress's efforts. Commissioner Wilson expressed concern that the ANPRM would be used as an "excuse to derail the ADPPA."

Should the FTC complete the rulemaking process and adopt commercial surveillance and data security TRRs, the regulations may be subject to legal challenge. While the issues raised by any litigation would depend on the substance of the final rules, one key issue might be whether, in light of the "major questions doctrine," the regulations exceed the FTC's statutory authority. Under the major questions doctrine, the U.S. Supreme Court has rejected agency claims of regulatory authority when (1) the underlying claim of authority concerns an issue of "vast 'economic and political significance,'" and (2) Congress has not clearly empowered the agency to address that issue. As discussed in this Sidebar, the Supreme Court recently applied this doctrine in *West Virginia v. EPA*, holding that the Environmental Protection Agency (EPA) exceeded its authority under Section 111(d) of the Clean Air Act by promulgating emission guidelines for power plants that were based in part on shifting electricity energy

generation from higher-emitting sources to lower-emitting ones. The Court reasoned, among other things, that Section 111(d) was a "previously little-used backwater" and that it was unlikely that through this provision Congress tasked the EPA with "balancing the many vital considerations of national policy implicated in deciding how Americans will get their energy."

Given the significant economic impact of data privacy and data security requirements, and the FTC's rare use of Magnuson-Moss rulemaking to enact new TRRs, it is possible that a reviewing court would apply the major questions doctrine to invalidate any broad-ranging commercial surveillance and data security TRRs. A reviewing court might conclude that comprehensive data privacy and data security regulation is a "major question" that the FTC Act does not clearly authorize the agency to address. On the other hand, if final rules primarily address the type of conduct that has been subject to past UDAP enforcement actions, a reviewing court may be less likely to determine that they exceed the scope of the FTC's authority. Even if the TRRs go beyond prior enforcement actions, it might be argued that the intentionally flexible nature of the FTC Act makes the major questions doctrine a poor fit. Courts have observed that Congress deliberately drafted the UDAP standard in broad terms because it was "impossible to frame definitions" that encompass all possible prohibited practices. Thus, the FTC Act's silence on whether the FTC may adopt comprehensive data privacy and security rules may be less problematic than in other major questions cases.

To the extent Congress wants to clarify the FTC's authority for commercial surveillance and data security TRRs, it might enact legislation indicating whether it intends for the FTC to have authority to address these issues.

Author Information

Chris D. Linebaugh
Legislative Attorney

Disclaimer