Prospects for FTC privacy rules

The FTC may begin its own rulemaking process on privacy, but many obstacles remain. **Andrew Smith** and **Christina Higgins** of Covington and Burling report from the US.

On 9 July, President Biden issued an Executive Order "encouraging" the new Chair of the US Federal Trade Commission (FTC), "in her discretion," to make rules regulating "unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy."[1] This call for privacy rulemaking echoes recent comments by the FTC's then-Acting Chair Rebecca Slaughter, who advocated for a privacy rule because of the "consumer-protection implications of widespread collection and dissemination of personal data fuelled by surveillance-based business models and especially by dominant technology firms."[2]

On 1 July 2021, the FTC, on a 3-2 party-line vote, approved a more simplified rule-making process, indicating that it is "clearing the decks" for a more aggressive rulemaking program. As described further below, these changes to the agency's Rules of Practice could enable it to more easily regulate companies' privacy protection practices, including shifting oversight of the rulemaking process from an administrative law judge to the FTC Chair and eliminating a potentially time-consuming staff report on proceedings.

These Rule changes follow the formation of a group within the Office of the General Counsel to centralize FTC rulemaking. In announcing the group, then-Acting Chair Slaughter said that she believes the agency must use rulemaking authority "to deliver effective deterrence for the novel harms of the digital economy" and that she is "excited for this new rulemaking group to explore all the possibilities."[3]

Although the new procedures approved by the Commission streamline the rulemaking path, certain procedural and substantive features of the rulemaking process will likely continue to pose obstacles to the Agency's ability to successfully promulgate rules that address trending privacy concerns.[4]

Procedural obstacles to FTC rulemaking authority

In 1975, Congress granted the FTC the authority to issue industry-wide trade regulations when it passed the Magnuson-Moss Act.[5] This statute authorized the FTC to make rules prohibiting unfair and deceptive practices in commerce generally, and, because of the breadth of this authority, imposed certain procedural safeguards in addition to those already provided by the Administrative Procedure Act. Five years later, in response to public criticism that the FTC was overreaching its rulemaking authority, Congress imposed additional procedural obligations on the Magnuson-Moss rulemaking process through the Federal Trade Commission Improvements Act of 1980.[6]

The procedural requirements imposed by the Magnuson-Moss rulemaking process are significantly greater than what is required under the Administrative Procedure Act for notice-and-comment rulemaking.[7] Magnuson-Moss rulemaking includes elements that are adjudicatory in nature. For example, it requires hearings, cross-examination of witnesses, severe restrictions on communications between Commissioners and FTC staff, and multiple reports and recommendations issued for public comment.

First, the agency must provide an advanced notice of proposed rulemaking to Congress describing the area of inquiry, the objectives to be achieved by rulemaking, and potential regulatory alternatives.[8]

Before actually proposing the rule, the FTC must publish for public comment a Notice of Proposed Rulemaking (NPRM) that describes with particularity the reasons for the proposed rule and potential alternatives, with a cost benefit analysis for each. The Commission may issue such an NPRM only when "it has reason to believe that the unfair or deceptive acts or practices that are the subject of the proposed rulemaking are prevalent," and the finding of prevalence must be premised on prior FTC cease-and-desist orders or "other information" indicating a "widespread pattern of unfair or deceptive acts or practices."[9] This NPRM initiates the formal rulemaking proceeding, including ex parte communication requirements that restrict the FTC staff from communicating directly with individual Commissioners or their staffs except on the public record.

The NPRM must include "disputed issues of material fact" designated by the Commission to be "material and necessary to resolve," and an opportunity for an informal hearing, if an interested person requests to present their position orally. A request to add disputed issues of material fact beyond those identified in the NPRM may be made in the hearing request.

If a hearing has been requested, the Commission must then publish a Notice of Informal Hearing.[10] Interested parties are entitled to present evidence and, if necessary, cross examine witnesses with respect to disputed issues of material fact.[11] Following the hearing, the Presiding Officer makes a recommended decision with a proposed resolution of disputed issues of material fact.

The Commission then reviews the recommendation and rulemaking record and may take additional testimony, before promulgating a Final Rule.

The most recent Magnuson-Moss rulemaking was an amendment to the Business Opportunity Rule, which took almost 15 years from its ANPR in February 1997,[12] to the Final Rule in December 2011.[13] One commentator noted that the FTC has made just seven Magnuson-Moss rules since the 1975 law was passed, and the average time to complete those efforts was 2,035 days, or nearly six years.[14] The slow and cumbersome nature of this rulemaking process presents unique concerns for a data privacy rule, as the rapid pace of technological advances could potentially render any data security rule outdated once it is finally implemented. In

addition, Commissioners' terms run only seven years, and are usually much shorter than that. The extraordinary length of the rulemaking proceedings means that the Commissioners who authorize the rule in the first instance are not likely to still be serving when decisions about the rulemaking – including approval of the Final Rule – are required to be made.[15]

The recent changes to the agency's Rules of Practice will allow the Chair to exercise greater control over the rulemaking process by designating the Chair to serve as the Chief Presiding Officer, or designate an alternative Chief Presiding Officer (previously, it was the Chief Administrative Law Judge who had this privilege). The rule changes also eliminate the requirement for a staff report on the rulemaking record and eliminate the opportunity for public comment on the Chief Presiding Officer's recommendation. The key elements of the Magnuson Moss rulemaking process – the ANPR, the Initial and Final NPRM, the evidentiary hearing on the record, and the recommendation of the Chief Presiding Officer – remain unchanged.

Substantive Obstacles to FTC Rulemaking Authority

In addition to the procedural hurdles presented by the Magnuson-Moss process, the substantive criteria that the FTC must demonstrate during the rulemaking process also present challenges to rulemaking in an area such as data privacy where consumer harms may not be concrete,[16] and the effectiveness of the solutions are open to debate.[17] To justify a Final Rule under the Magnuson-Moss trade regulation rulemaking procedures, the FTC must state with particularity:

1. the need for the Rule;
2. the objectives of the Rule;
3. the unfair or deceptive acts or practices which are the subject of the proposed rulemaking are "prevalent," based on prior FTC's cease-and-desist orders or "other information" indicating a "widespread pattern of unfair or deceptive acts or practices";
4. the manner and context in which such acts or practices are unfair and/or deceptive;
5. the economic effect of the proposed rule, taking into account the effect on small businesses and consumers;
6. the reasons for the determination of the Commission that the rule will attain its objectives;
7. alternatives to the rule;
8. the costs and benefits of each of the alternatives;
9. the effectiveness of the proposal and each alternative in meeting the stated objectives of the proposed rule;
10. the reasons why the Commission chose a particular alternative; and
11. a summary of any significant issues raised by the public comments and the assessment by the Commission of those issues.[18]

The need to demonstrate that certain practices to be prohibited are prevalent and per se unfair or deceptive is not trivial. In the privacy context, most of the FTC enforcement actions have alleged that the defendant engaged in deception – defined as a practice that is likely to mislead consumers acting reasonably under the circumstances to their detriment.[19] FTC challenges brought under the "deception" concept involve claims of misleading disclosures that appear in companies' privacy policies regarding how the company handles consumer data, including what information it collects, how it uses the information, how long it keeps the information, who it shares the information with, the ability of consumers to exercise choices with respect to the information, and the level of security provided for the information.[20] These harms are typically remedied by either refraining from the misleading statement, or providing an adequate disclaimer to set the record straight.

Privacy laws, such as those that have been enacted in several states and the European Union, typically impose substantive requirements on companies, such as requiring companies to provide consumers with access to data about them and an opportunity to correct or delete those data.[21] The affirmative obligations created under these laws go well beyond the prohibition of misleading statements with respect to privacy. As a result, it seems more likely that any privacy rule that imposes substantive requirements and restrictions on companies handling personal data would be premised on the FTC's authority to prohibit "unfair" practices.

Under the FTC Act, however, a practice is unfair only if: (1) it "causes or is likely to cause substantial injury to consumers;" (2) the injury "is not reasonably avoidable by consumers themselves;" and (3) the injury is "not outweighed by countervailing benefits to consumers or to competition.[22] The FTC's Policy Statement on Unfairness further provides that a "substantial injury" usually involves a monetary harm and that emotional impact and other more subjective types of harm will not render a practice unfair.[23]

From an enforcement perspective, unfairness has been much less frequently alleged than that in deception in privacy cases. Over the last two years, since July 2019, the FTC has brought more than 40 cases alleging violations of the FTC Act relating to privacy or data security.[24] Twenty-two of these cases allege misrepresentations or deceptive practices with respect to privacy or data security, and eight allege unfair practices.[25] Of these eight unfairness cases, six allege unreasonable data security as an unfair practice, and only two address violations involving the collection, use, or disclosure of personal information.[26] One is a case alleging that the provision of "stalkerware" sold to third parties to surreptitiously track others is an unfair practice,[27] and the other alleged that the posting online of sensitive personal information in retaliation for bad product reviews is an unfair practice.[28]

This dearth of enforcement actions alleging unfair practices with respect to the privacy of personal information does not bode well for an FTC privacy rulemaking premised on unfairness. If, over the past two years the FTC has found only two cases where it believed that the collection, use, or disclosure of information was unfair, how does it expect to discover widespread privacy practices that are similarly unfair – that is, practices that present a risk of substantial injury that is unavoidable by consumers and that is do not provide any offsetting benefits? At the very least, this poses a challenge for the FTC to demonstrate through its prior enforcement actions that a particular privacy practice is "prevalent," as required by the Magnuson Moss

procedures.

Where there are no prior enforcement actions addressing a particular practice, and very few enforcement actions alleging unfairness with respect to privacy in any context, it seems as though it will be difficult for the FTC to argue that the particular practices that it aims to prohibit are "prevalent," as well as unfair.

Conclusion

As technology continues to advance, protecting privacy will remain a concern for the government, consumers, and companies. Should the substantive and procedural regulatory obstacles we explored in this article limit the FTC's ability to promulgate rules that address pressing privacy issues, Congress might be better positioned to enact comprehensive data security and privacy legislation. Although the outlook for passage of comprehensive federal legislation remains uncertain, the FTC continues to emphasize to Congress the importance of federal data security rules.[29] "I fervently hope that Congress passes a national privacy law …. But Congress has not yet acted," Slaughter commented last year.[30] "The worst outcome, in my view, is not that we get started but Congress passes a law; it's that we never get started and Congress never passes a law."[31]

AUTHORS

Andrew Smith is a Partner at Covington & Burling (Washington DC). Prior to rejoining the firm, Andrew served as Director of the Bureau of Consumer Protection at the Federal Trade Commission. Christina Higgins is an Associate at Covington & Burling.

The authors also acknowledge the assistance of Jaina Patel, a summer associate at Covington & Burling, in the preparation of this article.

Emails: asmith@cov.com
chiggins@cov.com

REFERENCES

1 See White House, Executive Order on Promoting Competition in the American Economy (July 9, 2021), www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/
2 See Federal Trade Commission, Keynote Remarks of Acting Chairwoman Rebecca Kelly Slaughter, Consumer Federation of America's Virtual Consumer Assembly (May 4, 2021), www.ftc.gov/system/files/documents/public_statements/1589607/keynote-remarks-acting-chairwoman-rebecca-kelly-slaughte-cfa-virtual-consumer-assembly.pdf
3 Federal Trade Commission, FTC Acting Chairwoman Slaughter Announces New Rulemaking Group (Mar. 25, 2021), www.ftc.gov/news-events/press-releases/2021/03/ftc-acting-chairwoman-slaughter-announces-new-rulemaking-group
4 Notably, if the Commission were to successfully promulgate a data privacy rule, anyone who violates the 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" could be liable for civil penalties. See 15 U.S.C. Sec. 45(m)(1)(A).
5 Magnuson-Moss Warranty Act, Pub. L. No. 93-637, 88 Stat. 2183 (YEAR).
6 Federal Trade Commission Improvements Act of 1980, Pub. L. No. 96-252, 94 Stat. 374 (YEAR).
7 See 5 U.S.C. § 553(b)–(e) (2012) (prescribing the procedural requirements of notice-and-comment rulemaking).
8 See 16 CFR § 1.10.
9 See id at § 18(b)(3)(B).
10 Notably, during proceedings to promulgate the Business Opportunity Rule in 2009, the Commission conducted a public workshop rather than a hearing. Although three commenters requested a hearing, these commenters agreed to participate in a public workshop instead. See Business Opportunity Rule, 76 Fed. Reg. 76816, 76,818 n.12, 76840 n.287 (Dec. 8, 2011), www.ftc.gov/sites/default/files/documents/federal_register_notices/16-c.f.r.part-437-disclosure-requirements-and-prohibitions-concerning-business-opportunities-final-rule/111122bizoppfrn.pdf
11 See 16 CFR § 1.10.
12 62 Fed. Reg. 9115 (February 28, 1997).
13 See Business Opportunity Rule, 76 Fed. Reg. 76816 (Dec. 8, 2011), www.ftc.gov/sites/default/files/documents/federal_register_notices/16-c.f.r.part-437-disclosure-requirements-and-prohibitions-concerning-business-opportunities-final-rule/111122bizoppfrn.pdf
14 Jeffrey S. Lubbers, It's Time to Remove the "Mossified" Procedures for FTC Rulemaking, 83 Geo. Wash. L. Rev. 1979, 1997 (2015).
15 Although some Commissioners serve their full seven-year term or longer, the great majority of Commissioners serve considerably less than seven years. For a timeline of Commissioner Terms, see Federal Trade Commission, Commissioners, Chairwomen and Chairmen of the Federal Trade Commission (Nov. 2018), www.ftc.gov/system/files/attachments/commissioners/commissioner_chart_november_2018_0.pdf
16 See generally TransUnion LLC v. Ramirez, 141 S. Ct. 972, 208 L. Ed. 2d 504 (2020) (holding that only a plaintiff concretely harmed by a defendant's violation of the Fair Credit Reporting Act has Article III standing to seek damages against that private defendant in federal court).
17 Commissioner Noah Phillips of the FTC has testified that the types of value judgments that would be required to make a privacy rule are more appropriate for a legislature than an unelected administrative agency: "Legislation should be based on harms that Congress agrees warrant a remedy, and tools like penalties and rulemaking should be calibrated carefully to address those harms. …Congress should also give appropriate consideration to the trade-offs involved in new regulation, and, with regard to rulemaking, reserve to itself fundamental value judgments appropriately made by the legislature." See Prepared Statement of the Federal Trade Commission: Oversight of the Federal Trade Commission Before the Committee on Energy and Commerce Subcommittee on Consumer Protection (May 8, 2012), at 6, n.12, www.ftc.gov/system/files/documents/public_statements/1519212/p180101_house_ec_oversight_testimony_may_8_2019.pdf
18 See 16 CFR § 1.14(a)(1).
19 See Letter from James C. Miller III, Fed. Trade Comm'n Chairman, to John D. Dingell, Chairman, House Comm. on Energy and Commerce (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.
20 See Federal Trade Commission, FTC's Use of Its Authorities to Protect Consumer Privacy and Security (2020), https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf
21 See California Privacy Rights Act, § 1798.105(a) & §1798.106(a) (2020);

REFERENCES

Virginia Consumer Data Protection Act, § 59.1-573(A)(2)&(3) (2021); Colorado Privacy Act § 6-1-1304 (1)(b)&(c) (2021).
22 15 U.S.C. § 45(n).
23 Federal Trade Commission, FTC Policy Statement on Unfairness (Dec. 17, 1980), www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.
24 FTC, Cases Tagged with Privacy and Security, www.ftc.gov/enforcement/cases-proceedings/terms/245 (last visited July 16, 2021).
25 Id. The remainder of the cases allege violations of specific statutes enforced by the FTC, such as the Children's Online Privacy Protection Act or the Fair Credit Reporting Act.
26 Id.
27 In Re Retina-x Studios, LLC, 2020 WL 1549674 (F.T.C. Mar. 26, 2020), www.ftc.gov/enforcement/cases-proceedings/172-3118/retina-x-studios-llc-matter.
28 United States. v. Mortgage Solutions FCS, Inc., No. 4:20-cv-110 (N.D. Cal. Filed Jan. 6, 2020), www.ftc.gov/enforcement/cases-proceedings/182-3199/mortgage-solutions-fcs-inc.
29 See Federal Trade Commission, FTC's Use of Its Authorities to Protect Consumer Privacy and Security (2020), www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf.
30 See Federal Trade Commission, Keynote Remarks of Acting Chairwoman Rebecca Kelly Slaughter, Consumer Federation of America's Virtual Consumer Assembly (May 4, 2021), www.ftc.gov/system/files/documents/public_statements/1589607/keynote-remarks-acting-chairwoman-rebecca-kelly-slaughte-cfa-virtual-consumer-assembly.pdf.
31 See footnote 30.

EU recognises the UK's DP Act as adequate

The EU formally announced on 28 June that it has recognised the United Kingdom's data protection law as adequate to enable the free flow of personal data from the European Economic Area to the UK's.

This 93-page document gives a very thorough assessment which starts by describing the framework of democracy and law in the UK, even referring to the Magna Carta and the Bill of Rights 1689, and more recently the UK's ratification in 1987 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

As expected, this EU document states: "As the UK GDPR is based on EU legislation, the data protection rules in the United Kingdom in many aspects closely mirror the corresponding rules applicable within the European Union" and is therefore, "essentially equivalent."

The UK government's response was enthusiastic "The UK government welcomes the move, which rightly recognises the country's high data protection standards." However, at the same time it gives an indication of the development of the UK's data protection policy in the future. "The government plans to promote the free flow of personal data globally and across borders, including through ambitious new trade deals and through new data adequacy agreements with some of the fastest growing economies, while ensuring people's data continues to be protected to a high standard."

It sets a clear independent path stating "All future decisions will be based on what maximises innovation and keeps up with evolving tech. As such, the government's approach will seek to minimise burdens on organisations seeking to use data to tackle some of the most pressing global issues, including climate change and the prevention of disease."

Věra Jourová, Vice-President for Values and Transparency, said: " … we have listened very carefully to the concerns expressed by the Parliament, the Members States and the European Data Protection Board, in particular on the possibility of future divergence from our standards in the UK's privacy framework. We are talking here about a fundamental right of EU citizens that we have a duty to protect. This is why we have significant safeguards and if anything changes on the UK side, we will intervene."

The decision includes a sunset clause saying it will automatically expire four years after its entry into force. After that period, the adequacy findings might be renewed, however, only if the UK continues to ensure an adequate level of data protection. During these four years, the Commission will continue to monitor the legal situation in the UK and could intervene at any point, if the UK deviates from the level of protection currently in place. Should the Commission decide to renew the adequacy finding, the adoption process would start again.

• *See: www.privacylaws.com/news/eu-recognises-the-uk-s-data-protection-act-as-adequate/*
and PL&B UK Report, July 2021, p.1

Italy develops privacy icons

Italy's DPA, the *Garante*, has held a contest for solutions that can make information notices simpler, clearer and immediately understandable through icons, symbols or other graphic elements. The *Garante* was seeking submissions by the end of May by calling upon software developers, tech professionals, experts, lawyers, designers, university students, and anyone interested in this topic, to send a set of symbols or icons that can represent all the items that must be contained in an information notice under Articles 13 and 14 of the GDPR.

The *Garante* is in the process of selecting three datasets of symbols and icons that are considered especially effective and will make them available on its website for use by all stakeholders.

• *See edpb.europa.eu/news/national-news/2021/easy-privacy-information-icons-yes-you-can-italian-dpa-launches-contest_en*

