AN A.S. PRATT PUBLICATION
JANUARY 2023
VOL. 9 NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 1** **January 2023**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2023–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Federal Trade Commission Moves Forward on Privacy Rulemaking

By Christopher B. Leach, Arsen Kourinian, Dominique Shelton Leipzig, Jonathan H. Becker, Howard W. Waltzman, Michael Jaeger and Joshua M. Cohen*

In this article, the authors discuss developments that took place at a virtual public forum relating to consumers' privacy and data security held recently by the Federal Trade Commission.

The Federal Trade Commission (FTC) recently held a virtual public forum on the agency's release of an Advance Notice of Proposed Rulemaking (ANPR)[1] to regulate the protection of consumers' privacy and data security. In addition to allowing the public the opportunity to share feedback about the ANPR, the hearing also included remarks from FTC leaders as well as two panels with consumer advocacy groups and representatives from industry on the perceived harms stemming from what the FTC characterizes as "commercial surveillance" and whether new rules are needed to protect consumers.

Key topics raised by industry representatives and consumer advocates alike included data minimization and the prevention of secondary uses of data, particularly in the context of behavioral advertising. As discussed further below (see "What Can Companies Do?"), the FTC's focus on behavioral advertising and concerns about the widespread collection of consumers' online activities is part of a broader regulatory emphasis on digital marketing across the globe.

We saw this in California in connection with the state attorney general's recent public settlement of an enforcement action for alleged violations of the California Consumer Privacy Act (CCPA) pertaining to cookies; we saw this in Europe, where state regulators such as the French Data Protection Authority (CNIL)[2] have increasingly fined companies for behavioral advertising and cookie practices under the EU General Data Protection Regulation (GDPR); and we saw this when the U.S. Consumer Financial Protection Bureau (CFPB) issued an interpretive rule clarifying that digital marketers are subject to CFPB enforcement as "service providers."

---

* The authors, attorneys with Mayer Brown, may be contacted at cleach@mayerbrown.com, akourinian@mayerbrown.com, dsheltonleipzig@mayerbrown.com, jbecker@mayerbrown.com, hwaltzman@mayerbrown.com, mjaeger@mayerbrown.com and jmcohen@mayerbrown.com, respectively.

[1] https://www.ftc.gov/system/files/ftc_gov/pdf/commercial_surveillance_and_data_security_anpr.pdf.

[2] https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance.

One particular point of tension that came up throughout the FTC forum, and especially during the public comment period, related to the FTC's legal authority to engage in a privacy rulemaking. Some participants warned of the FTC interfering with ongoing congressional negotiations over proposed federal privacy legislation, the American Data Privacy and Protection Act (ADPPA), and others alluded to FTC rulemaking authority struggling to clear the hurdle of Supreme Court scrutiny under the "major questions" doctrine.

Regardless of legal procedural concerns, the rulemaking process is fully underway, with the FTC looking to use public feedback in order to move to the next stage of the Mag-Moss rulemaking process: issuing a Notice of Proposed Rulemaking. The agency took public written comments about the ANPR until October 21, 2022.

COMMISSIONERS' REMARKS

The three Democratic commissioners – Chair Lina Khan and Commissioners Rebecca Slaughter and Alvaro Bedoya – delivered brief remarks highlighting their individual concerns and areas of focus for privacy rulemaking. Notably, neither of the Republican commissioners, Christine Wilson and Noah Phillips, shared their views in this forum, though both publicly dissented from the issuance of the ANPR (Wilson's dissent[3] and Phillips' dissent[4]), airing disputes on policy and the agency's authority to promulgate privacy rules.

Khan highlighted research that asserts that many Americans have limited insight about the information being collected about them and how it is used. Addressing the question of legal authority, Khan noted that the FTC has a long record of using its tools to regulate data privacy and security. But, she added, the goal of this rulemaking process is to determine if business practices today are so "prevalent" that the FTC needs to move beyond case-by-case adjudication and issue market-wide rules. The public forum was an important step to "democratize" this rulemaking process, according to Khan.

Slaughter shared her view that it is important for the FTC to show that the agency is no longer shying away from exercising its rulemaking authority. (Recall that, as the acting chair for the first six months of 2021, she anticipated new rulemakings when she created a rulemaking group within the FTC's Office of General Counsel.) Slaughter also voiced her support for strong federal legislation but noted that, until there is a law on the books, she believes that the FTC must use its tools to regulate the field.

---

[3] https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Wilson%20Dissent%20ANPRM%20FINAL%2008112022.pdf.

[4] https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Phillips%20Dissent%20to%20Commercial%20Surveillance%20ANPR%2008112022.pdf.

Bedoya commented on the breadth of the ANPR, noting his view that the ANPR is intentionally broad, going beyond normal bedrocks of consumer notice and consumer choice/consent. According to Bedoya, privacy rights and harms have gone well beyond the point of initial collection, and the FTC needs to enforce across all of these areas.

RULEMAKING PROCESS

A staff attorney, Josephine Liu, from the FTC's Office of General Counsel gave a brief presentation on the rulemaking process the FTC will employ here. As we have explained previously, the FTC's rulemaking process in this context is governed by the Magnusson-Moss Warranty Act of 1975 (referred to as Mag-Moss) and includes several additional steps beyond normal notice-and-comment rulemaking allowed by the Administrative Procedure Act. The timeline for Mag-Moss rulemaking includes this initial ANPR, followed by the issuance of a proposed rule that also will include the FTC's explanation of why the prohibited practices are sufficiently "prevalent" to warrant rulemaking. After that, interested parties will have an opportunity to cross-examine the FTC's evidence in an investigational hearing. (This part of the process is the least familiar to practitioners and will be subject to new "streamlined" procedures[5] the FTC recently approved.) After this process, if the agency decides that rules are warranted, the FTC would issue final rules, subject to court challenges.

In addition to describing the Mag-Moss rulemaking process and timeline, Liu highlighted three key questions with which the FTC is grappling among the 95 questions raised in the ANPR:

- Which of these measures or practices are prevalent? Are some practices more prevalent in some sectors than in others?
- How should the Commission identify and evaluate these commercial surveillance harms or potential harms? On which evidence or measures should the Commission rely to substantiate its claims of harm or risk of harm?
- Which areas or kinds of harm, if any, has the Commission failed to address through its enforcement actions?

INDUSTRY PERSPECTIVES

After the staff presentation, the forum turned to perspectives from industry. The four panelists included Jason Kint (chief executive officer, Digital Content Next), Marshall Erwin (chief security officer, Mozilla), Paul Martino (vice president and senior policy

[5] https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-votes-update-rulemaking-procedures-sets-stage-stronger-deterrence-corporate-misconduct.

counsel, National Retail Foundation), and Rebecca Finlay (chief executive officer, Partnership on AI). Each panelist discussed issues from their own organization's perspective.

Below are some highlights from each panelist's statement:

- Kint: Collecting data in one context and using it in another (for behavioral advertising) tends to violate consumer expectations. Behavioral advertising fueled by commercial surveillance primarily benefits the dominant market players.
- Erwin: Web platforms and browsers play a role in protecting privacy (e.g., features in Firefox), but technical solutions are not enough. He would like to see regulation in the following areas: dark patterns, harmful uses of data after it is collected, and more transparency about systematic harm on the main platforms.
- Martino: Martino would like the FTC to follow three key "customer is always right" principles: (1) the customer should be free to make informed choices, (2) businesses can use data to serve customers as they choose to be served, and (3) regulations should be customer-centric and risk-based.
- Finlay: Algorithmic decision-making is growing exponentially (cites the Stanford AI index, showing private sector investment in AI as more than double than that of the previous year).

The panelists also discussed "best practices" from their perspectives. Finlay explained that, when AI is deployed – especially in high-risk settings such as healthcare and hiring – companies need well-functioning internal organizational processes from design to deployment. Erwin stated that there are consensus best practices in data security – consistent with FTC's safeguards rule – that are universally accepted but not universally adopted. Kint pointed to best practices coming out of specific companies, naming specific examples such as Apple (app tracking transparency), Firefox, Brave, and Global Privacy Control. And Martino focused on retailers, explaining that certain concepts, such as Global Privacy Control, could frustrate consumers' choices if they previously elected to receive communications or other services from businesses.

CONSUMER ADVOCATE PERSPECTIVES

Next, the forum invited the opinions of five panelists from the consumer protection space: Caitriona Fitzgerald (deputy director, Electronic Privacy Information Center (EPIC)), Harlan Yu (executive director, Upturn), Ambassador Karen Kornbluh (ret.) (director, Digital Innovation and Democracy Initiative, German Marshall Fund of the U.S.), Spencer Overton (president, Joint Center for Political and Economic Studies), and Stacey Gray (senior director for U.S. Policy, Future of Privacy Forum (FPF)). These

panelists focused on the perceived harms of commercial surveillance and the need for the FTC to use the tools at its disposal.

Below are some highlights from each panelist's statement:

- Fitzgerald: The United States is facing a crisis because powerful companies have employed commercial surveillance systems to build profiles of individuals, far beyond what individuals expect. The FTC should thus create a strong data minimization rule.
- Yu: The FTC needs to use all available tools to tackle the disparate adverse impacts that leave certain consumers systematically behind and perpetuate discrimination.
- Kornbluh: The Supreme Court's *Dobbs* decision revealed the dangers of data collection in our current environment, including sales of personal information about vulnerable people.
- Overton: Companies collect data on users and develop algorithms to promote content. These processes can facilitate discrimination, e.g., ads for employment opportunities and housing.
- Gray: Rapid development of wearable tech, connected technology, etc. makes this time ripe for the FTC to adopt federal rules.

The panelists also suggested ways for the FTC to implement data minimization and transparency in practice as well as debated whether notice and consent remains an appropriate framework. Fitzgerald and Overton stressed that the burden should move away from individual users, with structural rules assigning compliance obligations to companies. Yu highlighted that the FTC should require companies to make good faith efforts to stop discrimination in their data processing and to "show their work." Gray encouraged the FTC to codify past enforcement actions related to inadequate disclosures being an unfair practice. All five panelists disapproved of the notice and consent framework, highlighting the need to consider power imbalances.

WHAT CAN COMPANIES DO?

The FTC rulemaking process will take time, with several additional opportunities for companies and industry groups to share their thoughts and concerns and to describe beneficial uses of data that may be negatively impacted by a rulemaking. Crafting any rule will be difficult for the FTC given the hurdles of showing that the practices are prevalent, not negatively impacting data collection and use practices that benefit consumers, and developing a rule sufficiently narrow to avoid vacatur under the major questions doctrine.

But the FTC is not the only regulator looking at these issues. If, as a company, you are actively using digital marketing or cookies to track users online across websites and apps, then you should consider yourself formally on notice that you are engaging in the kind of so-called "commercial surveillance" that is generating regulatory and public angst around the globe.

The first step for companies involved in this space is to understand how you are using digital marketing. Of course, digital marketing is not in itself anti-consumer – many companies rely on this advertising to find and cultivate their business and to provide meaningful choices and opportunities to consumers. But it is important to recognize when you are gathering behavioral data about users interacting with your website and then tracking those users across different websites and apps. This latter type of third-party tracking and profile building is the kind of activity that is concerning to regulators and, to a certain degree, consumers.