VENABLE LLP

Amid Pushback, the FTC Issues Anticipated Report on Data Practices of Social Media and Video Streaming Services

September 25, 2024

Stuart P. Ingis, Kelly DeMarchis Bastide, The Honorable Thomas M. Boyd, Emilio W. Cividanes, Rob Hartwell, Tara Sugiyama Potashnik, Michael A. Signorelli, Julia Tama and Dana Holmstrand

On September 19, 2024, the Federal Trade Commission (FTC or Commission) released a long-awaited staff report, *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services* (the Report), the culmination of an investigation, started in December 2020, into the data practices of nine social media and video streaming services (SMVSS). In addition to outlining the Staff's findings related to these companies' data practices, the Report identifies alleged harms created by these practices, including advertising, automated systems, and practices relating to children and teens. These findings shed light on possible topics the FTC could address in its potential Commercial Surveillance and Data Security Rulemaking. The Report includes several recommendations related to SMVSS to "inform" both company and policy decisions. Many of these recommendations ask companies to take steps that go beyond what is required by existing law. Below, we summarize takeaways from the findings and recommendations in the Report.

Critical Reactions

While all five FTC commissioners voted to issue the Report, both Republican commissioners also issued separate statements expressing concerns about specific aspects of the Report. In a separately released Concurring and Dissenting Statement, Commissioner Andrew Ferguson dissented from the Report's sections on targeted advertising and artificial intelligence. Commissioner Ferguson said, "I do not share the Report's apparent view that the display of targeted advertising to adults is, on balance, harmful" and stated that targeted advertising can benefit consumers and producers. Commissioner Melissa Holyoak also issued a separate Concurring and Dissenting Statement, in which she stated the Report's recommendations "seek to regulate private conduct through a sub-regulatory guidance document" and that such recommendations "at times, incorporate mischaracterizations of what current law requires."

Industry also offered comments on the Report. In response to the Report, both the Association of National Advertisers (ANA) and the Digital Advertising Alliance (DAA) released statements. The ANA noted that the report failed to account for the value that targeted advertising brings to consumers and competition. The DAA pointed out that its self-regulatory program provides the type of transparency

and tools that the Report asks industry to provide.

The Report Called on Congress to Pass a Comprehensive Privacy Law

The FTC recommended that Congress pass a comprehensive privacy law, noting that the FTC would like to see such legislation restrict data collection and the ability to monetize data, and would like legislation to include stricter consent requirements for some data collection activities and stringent deletion and retention requirements. The FTC also opined that legislation is necessary to address "responsible use" of automated systems and to protect teen users of online services.

The Report Recommended That SMVSS Collect, Use, and Share Information Only as "Necessary"

The FTC suggested specific actions that SMVSS could take regarding data collection, processing, and sharing.

- **The FTC Recommended SMVSS Limit Data Collection to What Is "Necessary" to Provide the Service.** Of note, the Report appears to differentiate the use of data for advertising(for either third-party products or the SMVSS's own products) from what is "necessary" to deliver an SMVSS's service.
- **The Commission Suggested SMVSS Limit Data Sharing with Affiliates, Company-Branded Entities, and Third Parties to What Is "Necessary" to Provide the Service the Consumer Is Seeking**. The focus on affiliate sharing is notable, as such sharing is not generally restricted under current privacy laws. The FTC further recommended that SMVSS that are part of multinational organizations develop processes to oversee sharing between affiliates and company-branded entities and develop contractual language to govern such exchanges to avoid access to data about U.S. individuals by foreign countries.
- **The FTC Stated SMVSS Should Implement Data Minimization and Retention Policies.** The FTC took the position that SMVSS should develop concrete data minimization and retention policies to limit the collection, use, and disclosure of information to what is "necessary" to provide the service the consumer is seeking, and should develop "clear-cut" retention periods tied to those purposes.
- **The FTC Recommended That SMVSS Delete Data When No Longer Needed.** The FTC alleged that some SMVSS de-identified data in response to user requests and did not delete or only partially deleted data, notably practices that may explicitly be allowed under state privacy laws. The FTC suggested that SMVSS "properly delete" data when it is no longer needed.
- **The Commission Stated SMVSS Should Simplify Privacy Policies.** The FTC recommended that SMVSS publish "consumer-friendly" privacy policies in "clear, simple, and plain language" that describe the information collected, the purposes for this collection, retention

periods, and any third parties to which information will be disclosed.

The FTC Signaled Continued Focus on Targeted Advertising Using "Sensitive" Information

Expressing concern that use of ad targeting could create "inaccuracies or biases" that could harm consumers in the receipt of advertising, the FTC offered the following recommendations to SMVSS regarding advertising practices.

- **The FTC Recommended That SMVSS Clarify and Standardize Ad Targeting Restrictions.** The FTC continued to voice concern about the use of what the Commission considers to be "sensitive" categories, including political affiliation, race, and sexual orientation, for ad targeting. The FTC recommended that SMVSS review their own policies and practices for ad targeting based on sensitive categories and to "broadly" interpret sensitive categories, opining that the definitions in current state privacy laws are a floor and not a ceiling. The FTC did not discuss the benefits that targeting advertising on certain demographic data can provide, such as to government programs or cause-based organizations.
- **The FTC Stated SMVSS Should Use "Caution" When Collecting Sensitive Information Using AdTech.** The FTC recommended that advertisers "exercise caution" when using certain technologies, such as pixels, for advertising because these technologies can transmit many types of information, including what the FTC considered sensitive information, to advertising services. The FTC characterized pixels and other common advertising technologies as "privacy-intrusive."

The Report Suggested SMVSS That Use Automated Systems Provide Consumers "Control" Over Personal Information and Develop Testing Standards

The FTC offered the following suggestions for SMVSS using automated systems, such as algorithms, data analytics, and artificial intelligence (AI).

- **The Commission Recommended That SMVSS Enhance Access, Control, and Transparency of Automated Systems.** Citing a perceived lack of transparency and consumer control over the use of personal information in SMVSS automated systems, the FTC encouraged SMVSS to create notices and controls for consumers.
- **The FTC Suggested SMVSS Should Adopt More Stringent Testing and Monitoring Standards.** The FTC recommended that SMVSS develop more rigorous, comprehensive, and consistent testing and monitoring of automated systems. The FTC stated that SMVSS had disparate policies and offered limited information.

The FTC Recommended That SMVSS Adopt Data Practices Regarding Children and

Teens That Go Beyond COPPA's Requirements

The FTC alleged that SMVSS were not adequately protecting children and teens online and recommended that SMVSS adopt the following practices beyond what is required by the Children's Online Privacy Protection Act (COPPA).

- **The FTC Recommended That SMVSS Adopt Additional Protections for Children.** The FTC suggested that COPPA is the "floor, not the ceiling" and opined that SMVSS should provide additional safety measures for children under 13 when appropriate.
- **The Commission Suggested That SMVSS Should Adopt Policies to Address Child Users Found on Services.** The FTC expressed concern that certain SMVSS had allegedly stated there were no child users on their platforms because children were not permitted to create accounts. For SMVSS that do not permit child users, the FTC recommended that such companies develop more definitive policies and procedures to determine whether a user is a child and address any identified child users.
- **The Commission Recommended That SMVSS Provide Parents Control over Personal Information about Children**. The Commission suggested SMVSS should develop a "uniform" process for parents and legal guardians to request access to or deletion of information collected from their child. For operators subject to COPPA, such access and deletion opportunities are required.
- **The FTC Stated SMVSS Should Adopt New Protections for Teen Users**. The Commission stated some SMVSS placed "no restrictions" on teen accounts and did not distinguish between teen and adult users, a finding that is consistent with the fact that COPPA does not apply to users aged 13 and above. The FTC recommended that SMVSS consider additional protections for teen users, including, at a minimum, (1) designing age-appropriate experiences; (2) giving teen users privacy-protective settings by default; (3) limiting the collection, use, and sharing of teen user data; and (4) retaining teen user data only as long as necessary to fulfill the purpose of collection.

What Can You Do?

While the Report's recommendations are directed to SMVSS and go beyond what the law requires, the Report may illuminate areas of regulator focus. As voluntary measures to reduce risk, companies can consider the following steps:

- **Data Map.** Companies can learn what data they have, where it came from, who has access, and why the data was collected in the first place through a data mapping exercise. This work could include a review of sharing with advertising service providers to confirm appropriate agreements are in place.
- **Assess Minimization and Retention.** Companies can use the information learned from a data map to assess their data collection and use practices and enhance data retention and deletion policies.

- **Review Consumer-Facing Policies and Controls.** Companies can review their privacy policies and other consumer disclosures for accuracy and understandability. Additionally, they can review how consumer requests are made and acted on to ensure those tools are designed to be easy to use and are effective.
- **Develop and Implement Policies for AI tools.** As new automated tools come into the marketplace, companies can consider creating new review, oversight, and testing policies to help prevent unlawful bias and discrimination in the use of those tools.
- **Assess Children and Teen Policies.** If a company may interact with children and teen users, it could assess its handling of such data in light of new state laws and regulatory guidance.

About Venable: Venable's Privacy and Data Security Practice Group offers a suite of managed privacy services that can help companies of all sizes build data governance programs. Whether you are seeking full assessments to help create a new program or looking for custom-built assessments addressing any aspect of the data life cycle, Venable's Privacy and Data Security team can help. Please feel free to contact us with any questions about how Venable can help your organization.