KIRKLAND & ELLIS

Kirkland Alert

FTC Issues Report and Related Statements on the Use of Consumer Data by Tech Industry

01 October 2024

Last week, the Federal Trade Commission ("FTC") Staff published a report expressing concern over certain aspects of the data practices of nine Social Media and Video Streaming Services ("SMVSS"). The publication marked the conclusion of a study begun in 2019 through which the FTC Staff sought and obtained internal documents and data from these SMVSS.

Below we summarize several key take-aways from the FTC's findings in the report:

- **Carefully evaluate company policies and practice relating to the deletion or de-identification of consumer data.** The report details circumstances in which companies responded to consumer requests to delete data by de-identifying the data, rather than deleting it, and even the dissenting commissioners raised concerns with this practice. The report indicates that the FTC does not consider de-identification of user data an adequate substitution for outright deletion, at least in certain circumstances. As such, companies should consider reviewing their policies regarding whether they delete or merely de-identify user data, including in response to consumer requests. The FTC also encourages organizations to adopt data deletion policies that mandate deletion of consumer data when no longer necessary to fulfill a legitimate "business purpose." (Note that this is statutorily required for online operators that collect personal information from children under 13 and are subject to the Children's Online Privacy Protection Act ("COPPA").)
- **Use "consumer-friendly privacy policies" to explain the types of personal information collected from consumers, how it is used and with whom it is shared — whether or not these mechanisms are visible to users.** The report takes issue with the fact that many companies use "privacy-invasive tracking technologies" such as pixels to collect and transmit consumer data, which goes

largely undetected by users, as well as the fact that certain types of data may be generated, collected or used in unexpected ways (*e.g.*, using an IP address or device data for targeted advertising purposes; inferring a user's age through algorithmic data analysis or AI; importing household income or location data from data brokers). It also indicates companies are expected not just to disclose their data practices in clear and easy to understand language, but also implement *formal written policies* around data collection, use and sharing.

- **Consider allowing users to opt out of certain types of sharing and/or use of their data.** The report suggests companies should allow users to opt out of having their data used for purposes of targeted advertising, in particular.
- **Ensure compliance with COPPA as needed and consider implementing additional safeguards to protect the data of teens (who are not subject to the statutory protections of COPPA).** As mentioned above, COPPA requires certain online operators to provide heightened protections and consent mechanisms for collecting personal information online from children under 13. The report found that while some SMVSS do make efforts to provide protections for children, others have taken the position that they are not aware of children using their sites — sometimes despite evidence to the contrary. Not only should companies collecting personal information from children ensure they are complying with COPPA as needed — including if they have "actual knowledge" that they are collecting such information from children under 13 — the report also suggests they should consider treating data collected from teens aged 13–17 (who are not protected by COPPA) differently than data collected from adults, including, for example, by limiting the use of AI to drive user engagement (given the risk of highlighting certain forms of harmful content in doing so), imposing stricter privacy settings by default, and allowing parents or legal guardians to review or access their child's data and request deletion thereof.
- **Evaluate company policies and practices relating to collecting, using, and/or sharing consumers' "sensitive" personal information, especially for purposes of targeted advertising.** The report took issue with companies' ad targeting practices based on "sensitive categories" of personal data — including political affiliation, race, religion, health or sexual orientation — as raising "serious privacy concerns." Specifically, the FTC alleges such practices can cause injuries including "unlawful discrimination, emotional distress, stigma, reputational harm, embarrassment, and invasion of privacy." And even when targeted advertisements are not based explicitly on sensitive categories, the report notes that different categories of data that are not facially considered sensitive can sometimes be used as proxies for sensitive data (*e.g.*, using zip code as a proxy for race).
- **Review data used in algorithmic and AI-based processes and evaluate whether to allow consumers to opt out of having their personal information used for such purposes.** With respect to AI (used here to refer collectively to algorithmic

processes and/or machine learning), the report called out consumers' lack of ability to "review the information used by these systems or their outcomes, to correct incorrect data or determinations, or to understand how decision were made" as particularly problematic, claiming that the applying AI to consumer data increases "risks to consumers' privacy and civil rights."

The report and its findings were not without disagreement. The FTC's Democratic majority asserted that "the tech industry's monetization of personal data has created a market for commercial surveillance" with "inadequate guardrails" in place to protect the privacy of consumers, particularly children and teens. Meanwhile, Republican commissioners Andrew Ferguson and Melissa Holyoak each penned a partial concurrence/partial dissent that largely agreed with the concerns related to child/teen privacy but criticized the report for failing to consider the potential for FTC action to stifle free speech. Commissioner Holyoak expressed concern that the report's recommendations amounted to informal regulatory directives that should go through the standard rulemaking process, rather than through the issuance of non-binding policy statements.

Celanire Flagg also contributed to this Kirkland Alert.

Authors

Olivia Adendorff, P.C.

Partner / Dallas / Washington, D.C.

Richard H. Cunningham, P.C.

Partner / Washington, D.C.

Lucie H. Duvall

Partner / Washington, D.C.

Christopher B. Leach

Partner / Washington, D.C.

Related Services

Practices

- Cybersecurity & Data Privacy
- Litigation
- Antitrust & Competition

Suggested Reading

- 29 October 2024 Speaking Engagement GCR Live: Antitrust in Pharmaceuticals 2024
- 15 October 2024 - 16 October 2024 Speaking Engagement Hatch-Waxman Practitioners Think Tank on Paragraph IV Disputes
- 01 October 2024 Press Release Kirkland & Ellis Announces New Partners