Preparing for Increased Regulatory Enforcement in Privacy, Cybersecurity and AI

Jennifer C. Everett and Dorian W. Simmons

In 2024, the Federal Trade Commission (FTC) has continued its public data privacy and security enforcement actions. Many of these actions have addressed alleged violations relating to health, location, and biometric data practices. Below is a summary of several FTC enforcement actions and potential considerations for mitigating risks arising from FTC enforcement.

Health Privacy

- On April 26, 2024, the FTC announced that it finalized changes to its Health Breach Notification Rule (the "HBNR"). The changes clarify that the HBNR applies to online services, including mobile applications and inter-connected devices, that track health-related data or provide other health related services. Specifically, "vendors of personal health records" and related entities not covered by HIPAA are required to notify individuals, the FTC and the media of certain security breaches involving unsecured personally identifiable health data. The FTC brought its first enforcement actions under the HBNR against a digital healthcare platform and an online counseling service in 2023 and has continued its enforcement efforts related to health data in 2024.

- On April 15, 2024, the FTC issued a consent order against an online telehealth company in connection with allegations that the company disclosed health information using cookies and other online tracking technologies to advertising platforms in violation of the company's privacy policy, promotions and other public assurances. The order requires the company to pay over $20 million in civil penalties and implement a comprehensive privacy and information security program subject to ongoing FTC monitoring for 20 years.

- On June 7, 2024, the FTC obtained an order against an online alcohol addiction treatment service that allegedly disclosed personal health data using cookies and other online tracking technologies to advertising platforms without consumer consent in violation of the company's privacy statements. The order bans the company from disclosing health information for advertising purposes and requires the company to pay a $2.5 million civil penalty and implement a comprehensive privacy program with ongoing FTC monitoring for 20 years.

Location Privacy

- On April 11, 2024, the FTC finalized an order prohibiting a data broker and its successor from sharing or selling sensitive location data. The FTC alleged that the data broker sold mobile device location data to third parties that were able to use such data for their own business purposes. The order requires the data broker to, inter alia, implement a supplier assessment program to require third parties to provide consent for the collection and use of location data.

- On April 29, 2024, the FTC finalized a settlement with a digital marketing and data aggregator that allegedly unlawfully collected and used consumer location data for advertising and marketing purposes. The order prohibits the company from selling or licensing location data and providing products or services that target consumers based on such data. It also requires the company to implement a supplier assessment program and maintain a comprehensive privacy program subject to ongoing FTC monitoring for 20 years.

Biometric Privacy

- On February 23, 2024, the FTC and a retail pharmaceutical company agreed to a stipulated order regarding the company's use of a facial recognition technology system to identify consumers that were previously deemed likely to engage in shoplifting or other criminal behavior. The FTC alleged that the company failed to assess and address foreseeable harms, test the accuracy of the facial

recognition technology system, take reasonable steps to train employees on the use of the system, and monitor the system. The order bans the company from using certain facial recognition technology for five years. It also requires the company to delete any data, models or algorithms it previously derived from the system, and implement a biometric security or surveillance system monitoring program with ongoing FTC monitoring for 20 years.

Takeaways

Given recent FTC enforcement activity, companies and other stakeholders should take protective steps to address compliance concerns. FTC enforcement could lead to the imposition of civil penalties and other fees, disgorgement of profits and data, and the required implementation of comprehensive privacy and security programs subject to decades of FTC monitoring.

Potential Steps for Consideration:

- Identify data that the company processes, including health, location and biometric data, and evaluate potential exposure under FTC Rules, including the HBNR.

- Regularly review and confirm the accuracy and completeness of privacy-related representations, including those that are made in privacy policies, promotions and advertisements, inquiries to consumers and any other publicly available materials or documents.

- Clearly communicate to consumers how the business uses and discloses their personal information, including in connection with cookies and other online tracking technologies for targeted advertising.

- Monitor third parties that collect, share or use company data. Contractual terms that limit the purposes for which such third parties are able to process personal information, without appropriate audit controls, may not be sufficient to regulate data sharing with third parties.