Articles + Publications | April 4, 2024

FTC Releases 2023 Privacy and Data Security Update

WRITTEN BY

Ronald Raether, Jr. | Kim Phan

On March 28, the Federal Trade Commission (FTC) released a Privacy and Data Security Update, highlighting the FTC's activities in recent years through December 2023. The FTC underscored its work on issues related to artificial intelligence (AI), health data, geolocation tracking, children and teens' data, data security, credit reporting and financial privacy, as well as spam calls and emails. In the update, the FTC noted its consistent call on Congress to restore its ability under Section 13(b) of the FTC Act to seek monetary relief, including consumer refunds, in federal court, and to pass comprehensive privacy legislation.

- Artificial Intelligence.
    - The FTC has brought several enforcement actions, alleging that companies violated the FTC Act or other laws in connection with their collection, retention, or use of consumers' personal information to develop or deploy machine learning or similar algorithms.
    - The FTC has also sought to ensure that unlawfully obtained or retained data cannot be used to develop algorithms or for machine learning.
    - As discussed here, the FTC recently announced that it is proposing changes to the Impersonation Rule to address the production of AI "deepfakes" that can impersonate individuals' voices through voice cloning, which could be used in communications and marketing efforts to misrepresent products or services that could be harmful to consumers.
    - **Steps to Minimize Regulatory Impact.** How do you begin to implement a responsible AI approach to minimize regulatory scrutiny?
        - Utilize AI to help map data to the right use case. Develop methods and tools that enable analysis of use cases in order to understand feasibility, complexity, suitability, and risk. Leverage cross-functional teams that have technology, business, and risk experience.
        - Ensure that governance mechanisms have the right speed, scale, and enterprise reach so that there is a common enterprisewide view of AI and its risks. Governance needs to cover third-party risk management, privacy, data, compliance, as well as other functions where it might come into play.
        - Develop an AI risk taxonomy that covers (i) AI models, (ii) data collection, processing, storage, management, and use of systems, (iii) systems and infrastructure, taking into account potential privacy and cybersecurity risks, (iv) risks posed by users, *e.g.*, misuse, malicious actions, and cyberattacks, (v)

applicable laws, rules, and regulations, and (vi) the impact on existing workflows.

    - Emphasize governance from the start as consideration is given to AI initiatives.

    - Establish clear roles and responsibilities and develop training for better understanding of AI. This may also include developing or updating codes of conduct and acceptable use policies.

- Health Data.

    - According to the update, recent FTC orders have imposed strong injunctive relief, requiring health-related businesses to: (a) stop sharing health information with third parties for advertising purposes, (b) obtain affirmative express consent for other disclosures of health data, (c) instruct third parties to delete improperly disclosed data, (d) provide notice to consumers about illegal third-party disclosures, and (e) establish privacy or data security programs without independent assessments.

    - In addition, recent FTC orders have included civil penalties under the Health Breach Notification Rule. Last year, the FTC brought an action against a telehealth and drug discount provider for sharing users' information with third-party advertising platforms contrary to its privacy promises and focused on the company's third-party tracking capabilities.

    - **Steps to Minimize Regulatory Impact.** Increase focus on advertising practices.

        - Enhance third-party service provider contracts and data processing agreements to prohibit the sharing of health information for advertising purposes without the user's express written consent.

        - Establish processes and procedures to analyze the information that might be shared with third parties through pixels, cookies, and software development kids (SDK).

        - Incorporate protections against sharing of health information for advertising purposes in privacy and safeguards security policies.

- Geolocation Tracking.

    - Over the past few years, the FTC has focused on preventing harm to consumers that can result from exposure of highly sensitive information about an individual's location, such as their visits to cancer treatment or reproductive clinics, places of worship, or domestic violence shelters.

    - **Steps to Address Tracking Issues.** The following steps can be taken to help address tracking issues:

        - Develop and keep an updated inventory of cookies and tracking technologies.

        - Determine how the data will be used internally and in what form it will be retained (aggregated or de-identified) as well as who will have access.

        - Make sure that data that is shared with third parties is being used only for permitted purposes and that any secondary uses are limited.
        - Update contracts and agreements to deal with data use restrictions.
        - Develop checkpoints to be certain that tracking technology is being properly used.

- Children and Teen's Data.
    - According to the update, the FTC has brought 42 Children's Online Privacy Protection Act (COPPA) cases and collected more than $532 million in civil penalties since 2000.
    - The FTC is continuing in its efforts to update the COPPA Rule to address the evolving methods of collecting, using, and disclosing personal information from children, including those in their teenage years. It recently denied an application, without prejudice, for the use of "Privacy — Protective Facial Age Estimation" technology, which utilizes the geometry of a user's face to confirm that they are an adult. The FTC took no position on the merits of the application, indicating that more information is needed to better understand age verification technologies and their application.
    - **Tips to Minimize Regulatory Impact.** While this area is in state of regulatory flux, there are areas that can be addressed to minimize drawing regulator attention:
        - Aside from requiring verifiable consent from parents for using or disclosing children's data, ensure that internal operations and/or AI are not used in a way to encourage or prompt use of website or online services without sufficient notice to parents so that they can provide informed consent.
        - Tailor security safeguards to take into account the sensitivity of children's information.
        - Minimize the use of children's information to that which is only reasonably necessary, *e.g.*, participating in a game.
        - Consider developing age gating processes that incorporate knowledge based authentication and facial recognition technologies.

- Data Security.
    - Since 2000, the FTC has brought 89 enforcement actions against companies alleging inadequate protection of consumers' personal data.
    - The FTC noted that it is imposing stronger terms in its data security cases. For example, the update listed new terms in settlements such as requiring the company to implement a comprehensive security program, to obtain robust third-party biennial assessments of the program, and to submit annual certifications by a senior officer about the company's compliance with the order.

- **Steps to Minimize Regulatory Impact.** Consider the following suggested steps:
  - Perform a comprehensive review of your privacy and information security policies and procedures to ensure that they address FTC safeguards.
  - Implement assessment and testing processes to make certain that control processes are working effectively.
  - Develop external sources of information to keep the organization aware of potential threats.
  - Develop and test incident response plans to be certain they are working effectively and that employees understand their responsibilities in the event of an incident or security breach involving data. Performing tabletop exercises to reinforce responsibilities and responses required in the event of an incident is highly recommended.
  - Enhance training and communication related to privacy and information security to increase awareness.

- Credit Reporting and Financial Privacy.
  - The FTC has brought 117 cases against companies for violating the Fair Credit Reporting Act (FCRA) and has obtained more than $137 million in civil penalties. According to the FTC, these cases have helped ensure that consumer reporting agencies follow reasonable procedures to assure the maximum possible accuracy of consumer report information.
  - Since 2005, the FTC has brought about 35 cases alleging violations of the Gramm-Leach-Bliley Act (GLB). The GLB requires financial institutions to send customers initial and annual privacy notices and allow them to opt out of sharing their information with unaffiliated third parties.

- Spam Calls and Email.
  - In 2003, the FTC amended the Telemarketing Sales Rule to create a national Do Not Call Registry. Since that time, the FTC has brought 167 cases enforcing Do Not Call provisions against telemarketers.
  - The Telemarketing Sales Rule was recently amended to cover misrepresentations made in business-to-business calls, and made it clear that prerecorded messages created by AI are covered by the Rule. In an effort to stem the surge of “tech support scams,” the FTC is proposing further amendments to the Rule to cover tech support services.
  - The FTC reported that it shut down more than a billion robocalls through “Operation Stop Scam Calls.” Many of the cases alleged that the defendants tricked consumers into providing personal information and “consent” to receive robocalls.
  - The FTC brought two cases under the CAN-SPAM Act, which protects consumers from receiving commercial email spam.

The update also summarizes the FTC's rulemaking efforts, including proposed rules to clarify the applicability of the Health Breach Notification Rule and an advanced notice of proposed rulemaking that sought public comment on the harms stemming from "commercial surveillance."

Marc Loewenthal, Senior Senior Privacy & Security Advisor, also contributed to this article.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber