October 24, 2024

The FTC's Privacy Program: Where Is It Now and Where Is It Going?

Privacy+ Security Forum

Speakers

D. Reed Freeman, Jr.
Partner
ArentFox Schiff LLP

Tracy Pulito
Global Chief Privacy Counsel
Interpublic Group

Michelle Bowling
Associate
ArentFox Schiff LLP

Background

Privacy+ Security Forum

Background

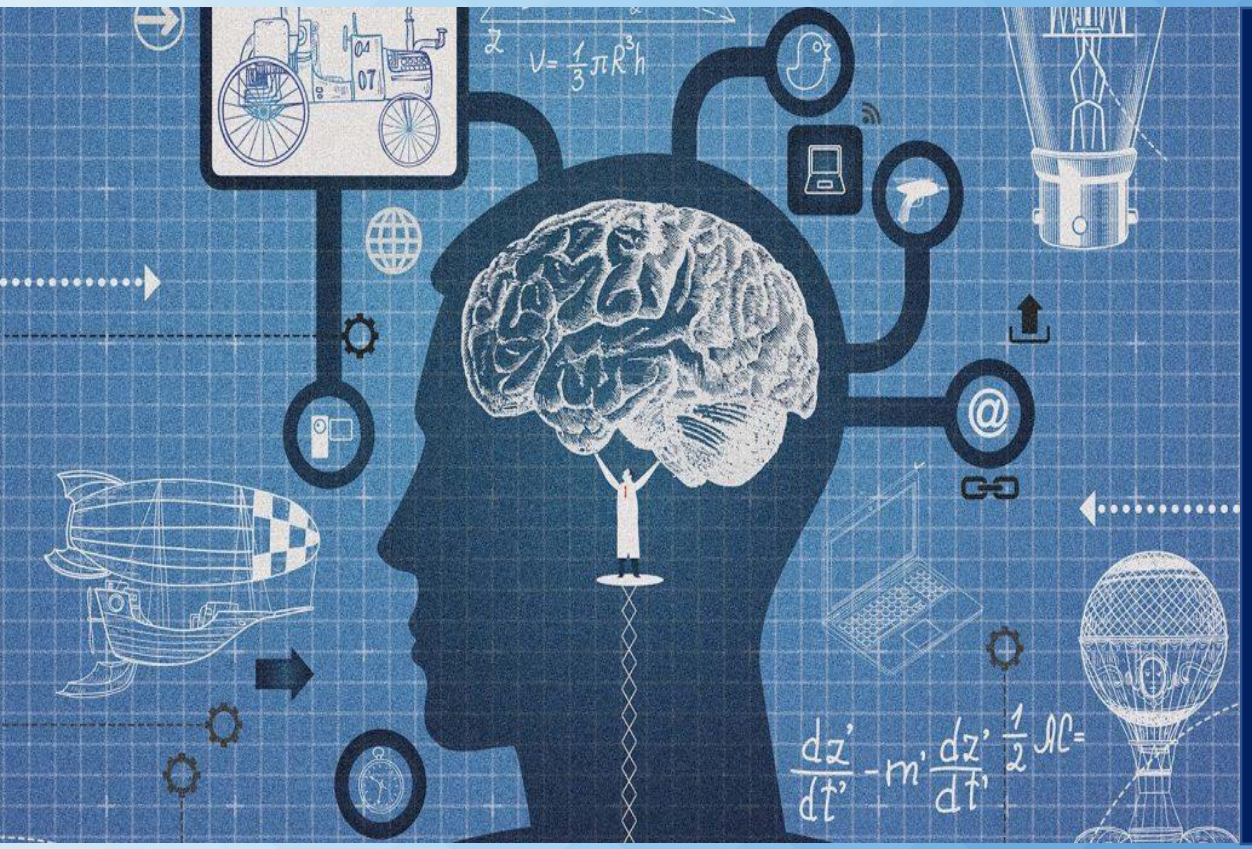
- As businesses focus on compliance with the ever-increasing patchwork of U.S. state comprehensive privacy and data security laws, they must remember that since the 1970's, the Federal Trade Commission ("FTC") has been the primary federal agency tasked with the creating policy on privacy and enforcing federal laws relating to privacy.

- The FTC uses law enforcement, policy initiatives, and consumer and business education to ensure the protection of consumers' personal information.

- More recently, the FTC's Business Blog has been used as a vehicle for policy development.

Background, continued

- ***AMG Capital Management v. FTC:*** Supreme Court ruled that the FTC Act does not authorize the FTC to obtain monetary remedies, such as restitution or disgorgement. Since then, the FTC has signaled that it will increasingly rely upon other penalties, such as algorithmic disgorgement, which could result in a greater financial loss to businesses in the long term.
- **Most enforcement actions are brought under Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."**
  - "**Unfairness**": An act or practice that causes or is likely to cause substantial injury to the consumers that is not reasonably avoidable and that is not outweighed by its benefits to consumers or competition.
  - "**Deception**": A representation or omission about a material fact that is likely to mislead consumers acting reasonably under the circumstances and would impact that consumer's choice regarding the product or service.



Artificial Intelligence

Privacy+ Security Forum

Artificial Intelligence: Overview

- The FTC can police the use of AI via its Section 5 authority.

- On June 16, 2022, the FTC published a report to Congress, "Combatting Online Harms Through Innovation" which details the FTC's concerns that AI tools can be **inaccurate, biased, and discriminatory by design**.

- In remarks made to The National Advertising Division Annual Conference in September 2023, the Director of the FTC's Bureau of Consumer Protection asked businesses to consider how generative AI is already leading market participants to **accelerate data collection**, "with firm after firm **changing their privacy policies** to make it easier for them to collect even more data from us and use it in new ways."
  - The Director went on to note that a concerning trend is for businesses to race in lockstep "to supercharge their data collection" providing evidence that a **self-regulatory strategy for AI** is **unlikely to be successful** to establish substantive privacy protections for consumers' personal information.

Artificial Intelligence & Security

Privacy+ Security Forum

The FTC warns that another unintended consequence of the rush to release new AI systems is **“Democratizing” cybersecurity harms** and includes two basic types of issues:

- **Hacking techniques are more accessible**
- **AI “going rogue”** and not following instructions, creating vulnerabilities and chaos.

Artificial Intelligence in the FTC Blogs

Within the past year, the FTC's Business Blog and Technology Blog have provided additional guidance on the use of AI:

- Warning businesses making **unsubstantiated claims** about its AI products and/or making, selling, or using a tool that is effectively **designed to deceive** consumers, ***even if that is not the tool's intended or sole purpose,*** will be considered deceptive practices. (May 1, 2023)

- The design or use of a product can also violate the **unfairness** prong of the FTC Act where their use results in **bias or produce discriminatory results**. (May 1, 2023)

- Businesses that **quietly change privacy policies and terms of service retroactively** could be considered unfair or deceptive acts or practices.

Artificial Intelligence: Notable FTC Enforcement

Privacy+ Security Forum

Rite Aid Corporation, et al. – February 2023

- This is the first FTC action which alleged that **the use of AI resulted in a biased and unfair outcome**.
- The FTC alleged that Ride Aid violated the FTC Act because it failed to take reasonable measures to prevent harm to consumers after AI facial recognition technology used by Rite Aid **erroneously flagged consumers as matching someone who had previously been identified as a shoplifter** or engaging in other wrongdoing.

Artificial Intelligence: Civil Investigative Demands

Privacy+ Security Forum

OpenAI - July 2023

- Ordinarily confidential, this **Civil Investigative Demand ("CID") was leaked** to the Washington Post indicating that the FTC had opened an investigation into OpenAI, the creator of ChatGPT, seeking detailed information about its products, technology, data security and privacy safeguards.

- The key areas of concern with privacy is a focus on both inputs: training data sets and data scraping *and* outputs: accuracy of information regarding individuals.
  - **Demand for "privacy-safe" data sets?**

- The FTC is also trying to determine whether OpenAI engaged in "unfair or deceptive privacy or data security practices" that would harm consumers.

- The CID also asks about OpenAI's data security program and information relating to safety / system cards

Artificial Intelligence: "Operation AI Comply"

Privacy+ Security Forum

In a September 2024 news release, the FTC announced a new enforcement initiative called "Operation AI Comply," detailing actions against five companies for their alleged unfair or deceptive use of AI.

- **Rytr** markets and sells an **AI writing assistant service**, one of its tools being a "Testimonial & Review" generator that can be used to **create false consumer reviews and testimonials** by entering a product name and desired tone within the tool's prompt.
  - The FTC alleged in its complaint that the company engaged in deceptive practices under the FTC Act because the tool could be **used to deceive potential consumers making purchasing decisions**.
  - Additionally, the FTC alleges Rytr engaged in unfair business practices which would "**pollute the marketplace with a glut of fake reviews** that would harm both consumers and honest competitors."

Artificial Intelligence: "Operation AI Comply" cont'd.

- DoNotPay offers an AI-powered "robot lawyer" that it **claimed could "generate legal documents and check small business websites for compliance violations**."
  - In its complaint, the FTC alleged unfair and deceptive practices in violation of Section 5 of the FTC Act because DoNotPay **failed to ensure that the AI chatbot's output was equivalent to a human** lawyer's, its technologies **had not been trained on federal and state laws**, regulations, and judicial decisions or on the application of those laws to fact patterns, and that and that the company itself didn't hire or retain any attorneys.
  - The company agreed to settle for $193,000, to provide notice to subscribers between 2021 and 2023 warning them of the tool's limitations, and to refrain from further claims without being able to substantiate them.

Artificial Intelligence and Privacy: Key Takeaways

Privacy+ Security Forum

- ✓ **Updates to Privacy Policies or Terms of Use** which create more permissive data practices require at least notice to consumers via email or persistent banner on the website. Gateway Learning – Consent
- ✓ **Do not over-represent AI capabilities**
- ✓ **Evaluate data sets** used in training AI algorithms. How collected? Representations made at collection? **Do they include health data, geolocation data, and browsing data?**
- ✓ **Evaluate current and previous privacy policies** to determine if the purposes of processing personal information contemplated its use for training AI.
- ✓ Do not license, sell, or disclose your data sets unless you have determined that **use for AI is consistent with representations at collection**.
- ✓ Audit your AI algorithms to **identify and remediate any foreseeable harms, including privacy, accuracy, and bias**.

Data Brokers

Privacy+ Security Forum

Data Brokers: Overview

Privacy+ Security Forum

- Data brokers are **individuals or companies that specialize in the collection of personal information about consumers** - often through online tracking technologies like cookies – and that personal information is often combined or analyzed and then resold or disclosed to other third parties.

- These mass data collectors engage in what the FTC refers to as, "**commercial surveillance**" which involves "the pervasive and comprehensive tracking of consumers' movements and behaviors across virtually every aspect of [consumers'] daily lives." (See "*Beyond the FTC: The Future of Privacy Enforcement*").

Data Brokers: Notable Enforcement

Privacy+ Security Forum

Avast Limited – February 2024

- FTC Allegations: Avast, which **claimed that its browser extensions and anti-virus software would protect users' privacy by blocking cookies**, was itself tracking consumers' browser information and **sold that information to more than 100 other companies through an affiliate** called Jumpshot, which Avast had acquired and rebranded from an antivirus service to an analytics company.
- The data sold by Avast **included sensitive personal data**, such as student loan application information, heath information, and religious information.
- In most instances, Avast **did not disclose its data sharing practices**, and when it did, the **information was inaccurate and buried within its privacy policy**. The FTC's complaint alleges that the companies violated the FTC Act by unfairly collecting, retaining, and selling consumers' browsing information; **deceptively failing to disclose they were tracking consumers**; and **misrepresenting** that consumers' browsing information would be **shared only in an aggregate and anonymous form** when that wasn't the truth.
- In addition to a **$16.5 million financial remedy for consumer redress**, the **order, finalized in June, bans Avast from selling, licensing, or otherwise disclosing web browsing data from Avast products to third parties for advertising purposes** and requires Avast to obtain **express, informed consent** for uses of personal information, and requires Avast to **delete the web browsing data and any models, algorithms or software developed using that data**.

Data Brokers Enforcement Spotlight: Geolocation Data

Privacy+ Security Forum

InMarket Media – January 2024

- FTC allegations: InMarket Media is a digital marketing and data aggregator that the FTC alleged collects location information about consumers from multiple sources, such as its own apps and via third-party apps that incorporate its software development kit ("SDK"), and ultimately combines this location data with other data to target advertisements to consumers.
- The FTC alleged that InMarket **failed to fully inform consumers about how their location information (which included sensitive personal information) would be used** and combined with other personal information **to target advertising** to those consumers.
- Due diligence: InMarket also allegedly **failed to ensure that third party apps using its SDK obtained informed consent from consumers** when collecting personal information.

Data Brokers Enforcement Spotlight: Geolocation Data

Privacy+ Security Forum

InMarket Media – January 2024 (continued)

- On May 1, 2024, the FTC finalized the order against InMarket, in which InMarket:
  - Is **prohibited from selling, sharing, or licensing any precise geolocation information** and providing any product or service that categorizes or targets consumers based on sensitive location information;
  - Must **delete all previously collected location data and any products produced from that data unless it obtains consumer consent or ensures the data has been de-identified**;
  - **Provides a simple and easy-to-find mechanism for consumers to withdraw consent** for the collection and use of location information, both within the app and for previously collected location information; and
  - Must **create a privacy program**, particularly one to manage sensitive location information.

Data Brokers Enforcement Spotlight: Geolocation Data

Privacy+ Security Forum

X-Mode Social, Inc. and Outlogic, LLC – January 2024

- FTC allegations: The FTC filed a complaint against data broker X-Mode Social and its successor, Outlogic, **alleging the companies lacked policies to remove sensitive locations and indirect identifiers** in the form of Mobile Advertiser ID **from raw data it sold**.
- The FTC alleged that X-Mode engaged in:
  - **Deceptive practices when it misled consumers about the purposes for which their location data could be used**; and
  - **Unfair practices** when it: i) sold sensitive data; ii) did not honor a consumer's choice to opt-out of personalized advertising via privacy controls available in the Android operating system; iii) failed to verify consumers provided informed consent for the processing of their data; and iv) inferred characteristics using this sensitive data to create and sell audience segments for marketing.

Data Brokers Enforcement Spotlight: Geolocation Data

Privacy+ Security Forum

X-Mode Social, Inc. and Outlogic, LLC – January 2024 (continued)

- The January 2024 proposed order, which was finalized in April, requires Outlogic to:
  - **Create a program to ensure it develops and maintains a comprehensive list of sensitive locations,** and ensure that it is not sharing, selling, or transferring that sensitive location information;
  - **Delete all previously collected location data and any products produced from that data** unless it obtains consumer consent or ensures the data has been de-identified**;**
  - **Due diligence: Develop a supplier assessment program** to ensure that companies that provide location data to X-Mode/Outlogic are **obtaining informed consent from consumers for the collection, use, and sale of the data** or stop using such information.

Data Brokers: Key Takeaways

Privacy+ Security Forum

- ✓ Clearly and conspicuously disclose all purposes for which a business may use, sell, or share personal information.
- ✓ Evaluate the collection and use of geolocation information.
- ✓ Assess default settings to ensure they align with statements made in the privacy notice and other public representations, such as marketing materials.
- ✓ Avoid unnecessary collection and processing of precise geolocation information.
- ✓ If collecting precise geolocation information, confirm that you are obtaining consent for purposes for which it's used and disclosed.
- ✓ Ensure any third party using your company's SDK is obtaining the appropriate consent prior to collection and disclosure of personal information.

Children's Privacy

Privacy+ Security Forum

Children's Privacy

- Issued in 1999 by the FTC, and updated in 2013, the Children's Online Privacy Protection Act Rule ("COPPA Rule") regulates how websites, apps, and other online operators collect data and personal information from children under 13.

- **Protection of children's data is an enforcement priority** and websites and other online properties that offer children's content, or are known to be used by children, are under increased scrutiny.

Children's Privacy: COPPA Key Requirements

Key requirements for operators of commercial websites and online services "directed to children":

- Online privacy notice
- Direct notice to parents
- Must obtain verifiable parental consent
- Data minimization
- Provide parental access
- Set data retention limits
- Reasonable security

Children's Privacy: COPPA 2.0

Privacy+ Security Forum

At the end of July, the Senate passed the Kids Online Safety and Privacy Act (KOSPA), incorporating the Kids Online Safety Act and the Children and Teens' Online Privacy Protection Act (COPPA 2.0), with the following notable changes from the Notice of Proposed Rulemaking:

- **Expands the definition of "operator"** to include an online application or mobile application.
- Expanding the definition of **"personal information" to include biometric data** to account for new methods of identification (such as Face ID and gait analysis) and adding "online contact information" to the definition of personal information to include "an identifier such as a mobile telephone number provided the operator uses it only to send a text message."

- To **codify current guidance for a school's use of educational technology ("EdTech"),** allowing schools to authorize EdTech vendors' use of student personal information without express parental consent, **provided there is a written agreement** and only where the EdTech is **used for a school-authorized education purpose and not for commercial purposes.**

Children's Privacy: COPPA 2.0, continued

The current version of the House mark-up makes the following additional change:

- **General, not actual knowledge, is required** where the operator is a "**Covered High-Impact Social Media Company**," defined as:
  1) an operator that generates more than $3 billion in global annual revenue;
  2) has 300,000,000 or more global monthly active users for not fewer than 3 of the preceding 12 months; and
  3)constitutes an online product or service primarily used to access or share user-generated content.

Children's Privacy: Kids Online Safety Act

- The **Kids Online Safety Act (KOSA) would create a "duty of care"** for covered platforms to prevent and mitigate harms when those online platforms are **likely to be used by minors**.
- Online platforms, such as social media platforms, must also provide minors with options to protect their personal information, disable addictive product features, and opt-out of personalized content based on algorithmic recommendations.
- Online platforms must also **default to the safest settings** where the account may belong to a minor.
- Enforcement would be through the Federal Trade Commission and state attorneys general.

Children's Privacy: Notable Enforcement

Privacy+ Security Forum

Epic Games, Inc. – December 2022

- FTC allegations: FTC alleged that the creator of the video game "Fortnite" violated the COPPA Rule when it **collected personal information from children under 13** who played the game **without notifying the children's parents or obtaining verifiable parental consent.**
- **$275 million penalty for COPPA violations** – the **largest penalty ever obtained** for violating an FTC rule. In addition to a separate large fine for using dark patterns mentioned below, Epic was also ordered to change default privacy settings.
- Additional penalties for "Dark Patterns" discussed below.

Children's Privacy: Notable Enforcement

Privacy+ Security Forum

NGL Labs – July 2024

- NGL offers an app that allows users to receive anonymous messages from friends and social media contacts and was marketed as a **"fun yet safe" place for young people to anonymously share thoughts and feelings.** Users could also create posts using pre-generated prompts like "would you say yes if I asked you out" at which time the FTC alleged users were manipulated into purchasing the NGL Pro version which would reveal the sender of the message, which was a **recurring negative option** - not a one-time fee - that cost $9.99 per week.
- NGL also advertised its "**world class AI content moderation**" which it claimed could filter out harmful language and bullying; however, the FTC alleges NGL received numerous reports of cyberbullying, harassment, and self-harm but did not take action.

Children's Privacy: Notable Enforcement

Privacy+ Security Forum

NGL Labs, continued

- The FTC and Los Angeles District Attorney's Office filed a complaint against NGL and its founders, alleging violations of:
  - Section 5 of the FTC Act, for both unfair and deceptive acts and practices for the apps misrepresentations, especially about the AI filter;
  - the COPPA Rule for failing to provide notice to parents, not obtaining verifiable parental consent, and not allowing a way for parents to stop further use of or delete the data of children under 13;
  - the Restore Online Shoppers' Confidence Act (ROSCA) for the recurring negative option; and
  - the California Business and Professions Code.
- NGL agreed to a $5 million settlement, as well as a **permanent ban** on marketing anonymous messaging apps to kids or teens **under the age of 18**.

Children's Privacy: Key Takeaways

- ✓ Evaluate whether your website or application has children's content and consider marketing plans and other documents to determine if the site is "directed to" children.
- ✓ Honor opt-out and deletion requests. Watch out for advertising.
- ✓ Data retention.
- ✓ Compliant privacy policy, direct notice to parents
- ✓ Collect verifiable parental or legal guardian consent.
- ✓ Consider implementing an age-gate.
- ✓ Note that a check box, such as "I am over 13," is deemed ineffective by the FTC. *Weight Watchers/Kurbo.*
- ✓ Best practice is to use dropdown menu for birthdate with month, date, and year.

Health Information Privacy

Privacy+ Security Forum

Health Information Privacy: Overview

- The FTC has shown increased interest in taking enforcement actions against **companies that use online advertising technologies, such as cookies, pixels, web beacons, and Software Development Kits ("SDKs"),** on websites or in applications which collect sensitive personal data, such as health information.

- In a March 2023 post titled, "Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking" the FTC's Technology Blog warned businesses that third-party tracking pixels enable platforms to collect consumer personal information and track their behavior via these **invisible pixels which consumers cannot avoid**, and when used on digital health platforms, the FTC will seek remedies such as bans on how that personal information may be used or disclosed for advertising.

Health Information Privacy: Recent FTC Activity

Privacy+ Security Forum

Inter-Agency Collaboration between HHS and FTC

- While HIPAA establishes a robust framework to ensure the privacy and security of "protected health information" ("PHI"), with enforcement handled by the U.S. Department of Health and Human Services ("HHS"), only specifically defined "covered entities," including health care providers and health plans, along with their "business associates" ("BAs"), must comply with the HIPAA Privacy Rule's restrictions on uses and disclosures of PHI and other HIPAA requirements, while **a party that obtains PHI but is *not* a covered entity or BA generally falls outside the scope of HIPAA enforcement**.

- A recently updated HHS/FTC joint publication about federal health information laws explains that Section 5 of the FTC Act requires that companies, including HIPAA covered entities and their BAs, "must not mislead consumers about – among other things – what's happening with their health information" and requires companies to "**ensure [their] health data practices aren't causing more harm than good**."

Health Information Privacy: Recent FTC Activity

Privacy+ Security Forum

Updates to the Health Breach Notification Rule ("HBNR")

- Modeled after the HIPAA Breach Notification Rule, the HBNR requires mobile health app developers and other companies that collect, use, or share individuals' health information but are *not* regulated under HIPAA to **notify consumers, the FTC, and, in some cases, the media of the unauthorized acquisition of individually identifiable health information** in an app or other personal health record.

- On April 26, 2024, the FTC announced that it had **finalized changes to the HBNR** designed to strengthen and modernize the rule by clarifying its applicability to **health apps and similar technologies**, while also expanding the information covered entities must provide to consumers when notifying them that a breach has occurred.

Health Information Privacy: Notable Enforcement

Privacy+ Security Forum

BetterHelp, Inc. – March 2023

- BetterHelp **provides an online mental health counseling service**, and marketed its services to the general public, as well as religious groups, teens, and the LGBTQIAP+ community.
- FTC allegations: FTC alleged that during the signup process, BetterHelp **made affirmative representations that it would not use or disclose personal health data except for limited purposes**, such as to provide counseling, but that it **actually used health information for its own advertising purposes** and **disclosed health information to third parties** without limiting those third parties' use of consumers' personal information for advertising or other uses.
- BetterHelp also **allegedly misrepresented its information practices as HIPAA compliant**.
- In July 2023, the FTC finalized its order **requiring BetterHelp to pay $7.8 million** and **prohibited its further sharing of consumer health data with third parties for those third parties' advertising and other purposes**.
- The order also requires BetterHelp to: 1) establish and maintain a comprehensive privacy program which includes safeguards to protect consumer data; 2) obtain express, affirmative consumer consent prior to disclosing personal information (not just health information) to certain third parties for any purpose; 3) **direct third parties to delete the consumer health and other personal data** shared with them; and 4) **limit how long it can retain personal and health information.**

Health Information Privacy: Notable Enforcement

Privacy+ Security Forum

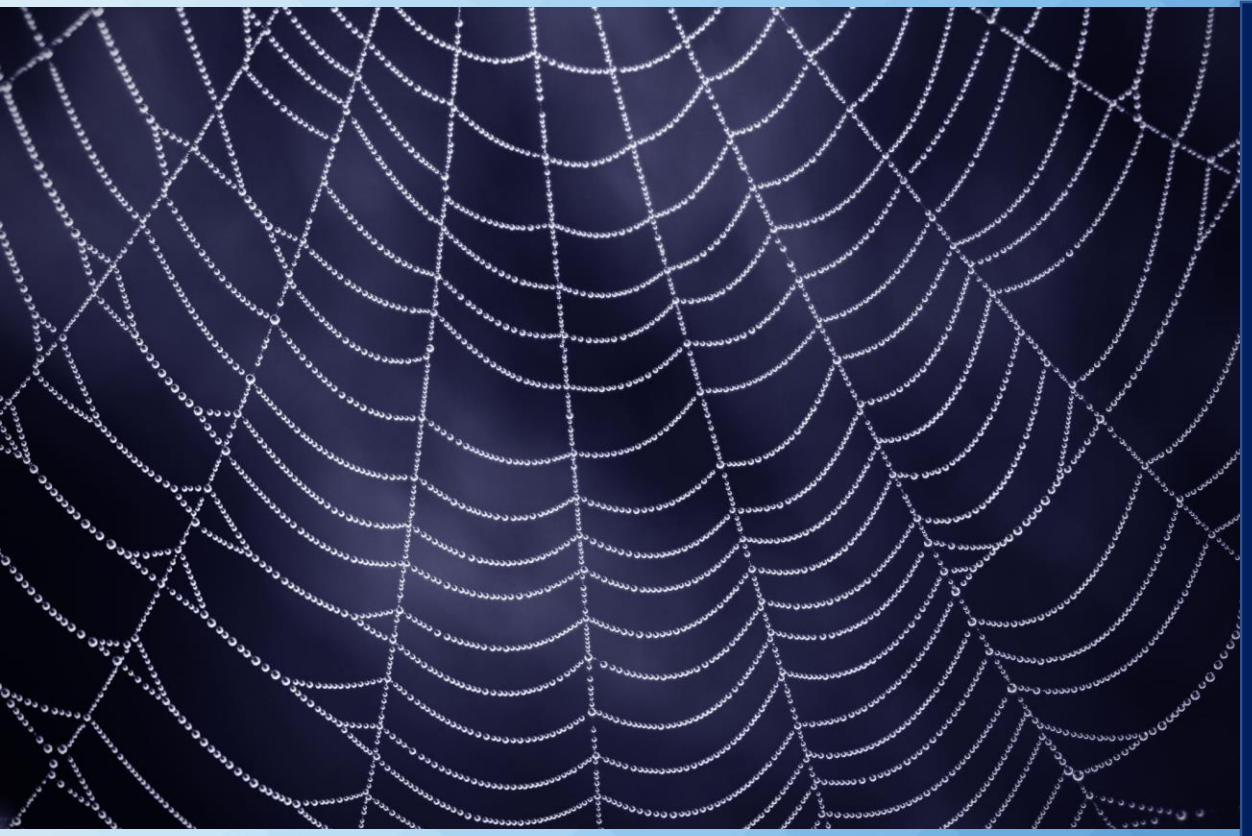
Monument, Inc. – May 2024

- Monument provides online alcohol addiction treatment services, including support groups, community forums, online therapy, and physicians.
- FTC allegations: Although Monument's website, marketing materials, and customer service representatives indicated that information shared with Monument would remain confidential and that Monument was HIPAA compliant, Monument's **"voluminous, densely worded privacy policy" hid** the fact that Monument **disclosed personal information to third parties via its use of tracking technologies**.
- The FTC alleged that Monument violated Section 5 of the FTC Act by failing to:
  - Implement reasonable measures to prevent disclosure of consumers' health information via tracking technologies;
  - **Obtain affirmative, express consent prior to disclosing consumers' health information to third parties and for Monument's advertising purposes**;
  - Accurately represent its disclosure of consumers' health information; and
  - Comply with HIPPA, despite its representations to the contrary.

Health Information Privacy: Key Takeaways

Privacy+ Security Forum

- ✓ The FTC considers health data, including sensitive details about medical conditions and treatments, to be highly susceptible to exploitation.
- ✓ Digital health companies and mobile apps should avoid the use of third party advertising technology on websites, consumer interfaces, or webforms where patients search for or submit health information unless prior express, affirmative consumer consent is obtained.
- ✓ Limit data retention to only what is necessary and adhere to any established data retention schedule.
- ✓ Disclose all purposes for which your service or third-party affiliates collect, maintain, use, or disclose data.
- ✓ Limit retention of health data.



Dark Patterns

Privacy+ Security Forum

Dark Patterns: Common Dark Patterns

Privacy+ Security Forum

In September 2022, the **FTC issued a report** called **"Bringing Dark Patterns to Light"** in which it highlighted **four of the most common dark pattern tactics** employed by companies, including**:**

1. **Difficulty in canceling subscriptions or charges**

    - The FTC has filed actions against companies that **required users to navigate multiple screens** in order to cancel subscriptions (***Cerebral* - May 2024**).

2. **Misleading consumers and disguising advertisements**

    - FTC alleged that the creator of the video game "Fortnite" **employed dark patterns** to trick millions of players into making unintentional purchases, resulting in children authorizing charges without any parental involvement. This resulted in Epic Games having to pay **$245 million in refunds** to affected users. The FTC also **alleged separate COPPA violations** which were discussed earlier in this presentation. (***Epic Games, Inc. – December 2022)***.

    - A company which claimed that its browser extensions and anti-virus software would protect users' privacy by blocking cookies, was itself allegedly tracking consumers' browser information and sold that information to more than 100 other companies through an affiliate called Jumpshot, which the company had acquired and rebranded from an antivirus service to an analytics company. (***Avast Limited – February 2024)***.

Dark Patterns: Common Dark Patterns, continued

3. Hiding key terms

- The FTC alleged that an internet phone service provider **subjected its customers to dark patterns** and junk fees when trying to cancel the services. It was required to revise its T&Cs and simplify the cancellation process. (***Vonage* – November 2023).**

4. Tricking consumers into sharing unnecessary data

- This tactic, which is also the **highest enforcement priority** for the FTC, employs dark patterns which appear to provide consumers with a choice but intentionally steer them towards an option that provides the most personal information.

Dark Patterns: Notable Enforcement

Privacy+ Security Forum

H&R Block – February 2024

- The FTC alleged that H&R Block **unfairly deleted consumers' tax data** and required consumers to contact customer service when downgrading to more affordable online tax preparation products, while product upgrades were performed "seamlessly."
- The FTC also alleged that products were deceptively marketed as "free" even though they were not free for all consumers.
- Samuel Levine, Director of the FTC's Bureau of Consumer protection, likened H&R Block's practices to "**an obstacle course of tedious challenges to consumers**…" and warning that "companies using coercive techniques that harm consumers can expect to hear from the FTC."
- In August, H&R Block lost its lawsuit to stop the FTC's enforcement action, and a hearing for the FTC's administrative case is set for late October 2024.

Dark Patterns: Key Takeaways

Privacy+ Security Forum

To avoid being considered a dark pattern when obtaining consumer consent, **choices must meet the following requirements**:

- ✓ Easy to understand.
- ✓ Provide symmetry of choice.
- ✓ Avoid language that is confusing to the consumer.
- ✓ Avoid encouraging a choice that results in the sharing of more personal information.
- ✓ Opt-outs of data sharing or sales should be easy to execute.

Questions & Contacts

D. Reed Freeman, Jr.
Partner
ArentFox Schiff LLP
Reed.Freeman@afslaw.com

Tracy Pulito
Global Chief Privacy Counsel
Interpublic Group
Tracy.Pulito@interpublic.com

Michelle Bowling
Associate
ArentFox Schiff LLP
Michelle.Bowling@afslaw.com

Thank you!