May 8, 2025

Update on the FTC's Privacy Program: Recent Developments and Changes Under New Republican Control

Privacy+ Security Forum

Speakers

D. Reed Freeman, Jr.

Partner

ArentFox Schiff LLP

Michelle Bowling

Associate

ArentFox Schiff LLP

Background

Background

- 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.

- Under the Biden Administration, Lina Kahn's FTC used its Business Blog aggressively as a vehicle to push the law. Andrew Ferguson's FTC has pulled back much of this guidance, but it's early, and we'll see where he takes it. It's unlikely they walk away from this tool altogether.

Background, cont'd.

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**, in Section 5 cases brought under Section 13(b). Since then, the Biden FTC 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. Unclear if the Ferguson FTC will follow this policy, but it is a very powerful tool to abandon.

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.

New Administration, New Priorities

- Andrew Ferguson became Chairman of the FTC on January 20, 2025, and on March 18, President Trump removed the two Democratic Commissioners, leaving (now) three Republican Commissioners to advance the Administration's deregulatory agenda.

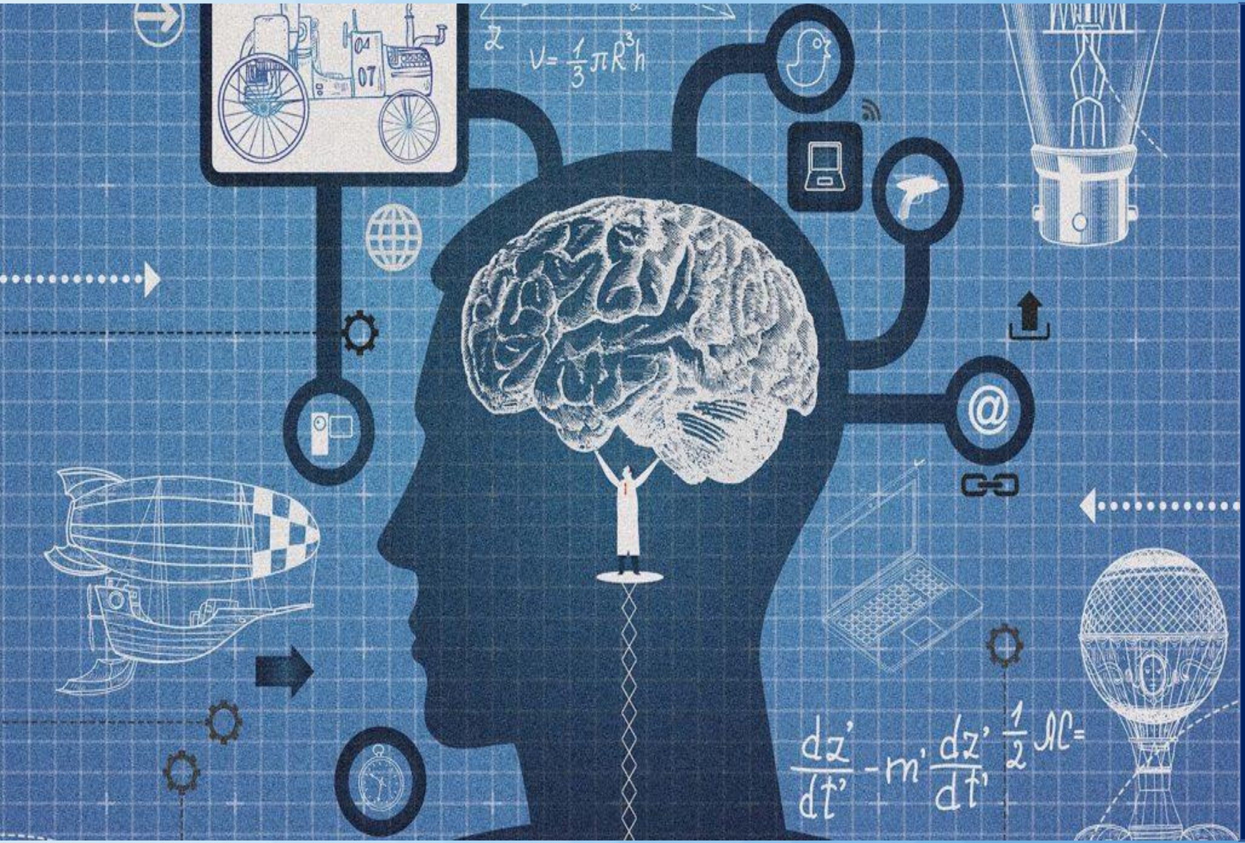
- In a January press release, Chairman Ferguson stated that the FTC will usher in, "**…a New Golden Age for American businesses, workers, and consumers**" but did not elaborate on how that would be accomplished. Sounds like a light-touch, but certainly enforcement actions based on deception are in play. Republicans tend to use unfairness more sparingly.

- **Big Tech may be an exception:** In a March 2025 statement at a policy conference in D.C., Chairman Ferguson stated that the "C-Suite deference" to large tech companies is over, but it remains unclear whether that relates to antitrust enforcement or to privacy and security enforcement as well.

New Administration, New Priorities

Commissioner Holyoak at IAPP 2025 (as reported by Bloomberg):

- FTC will focus on enforcement of **existing law and authority** (COPPA – top priority; use every tool, FCRA; GLBA; ROSCA?)
- **Other Privacy:**
  - **In:** *Deception* **--** Deceptive data sharing; data security; data brokers; sensitive data.
  - **Out:** *Unfairness* (except maybe inadequate security); attenuated harm; means and instrumentalities.
- **New Focus:** Selling/transferring/providing access to "personally identifiable sensitive data" to a "foreign adversary" (China, Russia, Iran, North Korea) or "an entity that is controlled by a foreign adversary" under the Protecting Americans' Data from Foreign Adversaries Act – Civil penalties!
- Focus on **responsiveness to CID**s (same as state regulators): **In:** Advocacy; **Out:** Hide the ball.
- **AI:** "promote AI growth and innovation, not hammer it with misguided enforcement actions or excessive regulation."
  - **In:** AI use in fraud and scams; advertising law claims.
  - **Out:** Actions like Rytr – unfairness; service likely to create fake reviews and providing the "means and instrumentalities" to produce deceptive AI-generated content.



Artificial Intelligence

Artificial Intelligence: Overview

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

- During the American Bar Association's 73rd Antitrust Law meeting last month, panelists consisting of former FTC chairs and practitioners predicted that the FTC **may deprioritize enforcement actions alleging that AI systems produce discriminatory outcomes**, instead focusing on "AI washing," which is a term used to describe exaggerated or **unsubstantiated claims** about a company's AI products.

- Focus on AI seems to be advertising law for now, rather than bias or discrimination. Deception is in play for privacy cases. **Must substantiate claims on how AI tools work and on their efficacy.**

Artificial Intelligence in the FTC Blogs

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

- **In:** Businesses that **quietly *and retroactively* change privacy policies and terms of service to address new AI tools** could be considered deceptive acts or practices. (February 13, 2024)

- **Out:** The design or use of a product can also violate the **unfairness** prong of the FTC Act where their use results in **bias or produces discriminatory results**.

Artificial Intelligence: Notable FTC Enforcement

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.
- **How will the Ferguson FTC follow-up?** Maybe same type of facts and focus less on bias and more on claims by a facial recognition system provider.

Artificial Intelligence: "Operation AI Comply"

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. We discuss the DoNotPay action below.

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.
- On February 11, 2025, the FTC finalized an order with the company, which 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: Notable Enforcement

accessiBe Inc. – January 2025

- In January 2025, the FTC announced a complaint and proposed order against accessiBe Inc., alleging the company **misrepresented its AI-powered tool's ability** to ensure its users' websites were Web Content Accessibility Guidelines ("WCAG") compliant.
- The complaint also alleged that the company **deceptively formatted third-party articles and reviews** to appear as though they were objective opinions and allegedly **failed to disclose material connections** to those reviewers.
- On April 22, 2025, the FTC approved a final consent order against the company, in which it **prohibits accessiBe from misrepresenting material facts** about its products and services **absent evidence to support those claims**. The **company must also pay $1M** to the FTC.

Artificial Intelligence: Notable Enforcement, cont'd.

Workado LLC – April 2025

- Workado markets a tool, the Content Detector, that it claims is "98% accurate" in detecting whether online content has been produced using generative AI technology.

- The FTC alleges that Workado violated Section 5 of the FTC Act with its **deceptive claims regarding the tool's accuracy**, which independent testing found to be closer to 53%.

- The FTC's order requires Workado to stop advertising the accuracy of the Content Director absent sufficient evidence and to retain any evidence of such accuracy claims.

- Following the order, the company must submit a compliance report to the FTC one year after it is issued, and then annually for the next three years.

Artificial Intelligence & Security

The FTC also 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.

In a December 2024 Technology Blog post, the FTC warned that companies that rely upon consumer data for product development – especially those relating to AI, targeted advertising, and "surveillance pricing" (a Kahn-FTC term) – may be at greater risk from threat actors through their creation of "valuable pools of information."

Data Brokers

Data Brokers: Overview

- Data brokers are (generally) **individuals or companies that specialize in the collection and sale/disclosure of personal information *about consumers* – *but not directly from consumers.***

- These mass data collectors engage in what the FTC (used to) refer 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

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 allegedly 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 allegedly **included sensitive personal data**, such as student loan application information, heath information, and religious information.

Data Brokers: Notable Enforcement

Avast Limited – Continued

- In most instances, the FTC alleged that 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.
- The FTC finalized the order in June 2024, and in addition to a **$16.5 million financial remedy for consumer redress**, **Avast is banned from selling, licensing, or otherwise disclosing web browsing data from Avast products to third parties for advertising purposes** and Avast must obtain **express, informed consent** for uses of personal information. Avast must also **delete the web browsing data and any models, algorithms, or software developed using that data**.
- In February 2025, the FTC sent notices to consumers to submit a claim for a refund.

Data Brokers Enforcement Spotlight: Geolocation Data

On December 3, 2024, the FTC announced two separate enforcement actions against data aggregators alleging the companies **unlawfully collected and sold sensitive location data without verifying users had provided informed consent to this sale.**

Gravy Analytics, Inc.

- The FTC alleged that Gravy Analytics, Inc. and its subsidiary, Venntel Inc. **used third-party suppliers to collect geolocation data and then sold "audience segments"** developed using inferences from geolocation data to both commercial and government sector customers **even after the companies learned that consumers did not provide informed consent**.
- Gravy Analytics and Venntel allegedly claimed to collect, process, and curate signals from approximately a billion mobile devices daily.
- The complaint also alleged that the company used **"geofencing"** to identify individuals who attended events relating to medical conditions or visited places of worship.

Data Brokers Enforcement Spotlight: Geolocation Data

Mobilewalla, Inc.

- Mobilewalla is a data broker that **obtains raw consumer data from Real-time bidding ("RTB") exchanges** instead of directly from consumers.
- The FTC alleged that Mobilewalla sold the purchased data without ensuring consumers had provided informed consent.
- Among the FTC's allegations were that Gravy Analytics, Venntel, and Mobilewalla, **engaged in unfair practices** in violation of Section 5 of the FTC Act when the companies:
  - Sold sensitive geolocation data;
  - Inferred characteristics using this sensitive data to create and sell audience segments; and
  - Failed to verify consumers had provided informed consent for the collection, use, and sale of their sensitive geolocation data.

Data Brokers Enforcement Spotlight: Geolocation Data

In January 2025, the FTC issued final orders against all three companies, which:

- Prohibits the companies from selling, disclosing, or using sensitive geolocation data (with limited national security exceptions for Gravy Analytics and Venntel);
- Prohibits any misrepresentation of how the data is collected, used, disclosed, and/or deleted;
- Requires each company to **disclose the extent to which data is de-identified**;
- Requires the companies to **establish a sensitive geolocation data program**; and
- Requires each company to **maintain a supplier assessment program to verify consumers' informed consent** and ensure consumers are able to withdraw consent.
- Notably, the FTC **prohibits Mobilewalla from the collection and retention of consumer data from real-time bidding exchanges**, which is **the first time the FTC has alleged unfairness in connection with this practice**.

Data Brokers Enforcement Spotlight: Geolocation Data

Ferguson Concurrence / Dissent:

- **Unfairness:** First, the Commission alleges that **Gravy Analytics and Mobilewalla sell consumers' precise location data without taking sufficient measures to anonymize the information or filter out sensitive locations**. This type of data— records of a person's **precise physical locations—is inherently intrusive and revealing of people's most private affairs**. The sale of such revealing information that can be linked directly to an individual consumer poses an obvious risk of substantial injury to that consumer. **The theft or accidental dissemination of that data would be catastrophic to the consumer. The consumer cannot avoid the injury…** Finally, given that the anonymized data remain valuable to firms for advertising and analytics, the injury that the consumer suffers is not outweighed by any countervailing benefits for the consumer. **The sale of non-anonymized, precise location data without first obtaining the meaningfully informed consent of the consumer is therefore an unfair act or practice in violation of Section 5**.

Data Brokers Enforcement Spotlight: Geolocation Data

Ferguson Concurrence / Dissent:

- "[S]elling precise location information without sufficiently verifying that the consumers who generated the data consented to the collection of those data by the applications that collected it." **Also unfair**.
- "The Commission accuses Mobilewalla **of sitting on the RTBs, submitting bids, collecting the MAIDs and location data for the bids, retaining those data *even when it did not win the auction*, and combining those data with data acquired from other sources to identify the user represented by the MAID**… Mobilewalla's [actions] exposed consumers to the same substantial risk of injury as collection of their data without consent, was not reasonably avoidable by consumers (as this conduct was far removed from their knowledge and control), and was not outweighed by any countervailing benefits to consumers. **Also unfair.**

But:

- Dissent from the FTC's counts against both firms accusing them of unfairly categorizing consumers based on sensitive characteristics, and of selling those categorizations to third parties. But it does so only because the data were collected **without consent for such use, not because the categories into which it divided the data might be on an indeterminate naughty categories list**.
- Similarly **dissented from allegations that indefinite retention is unfair.** No basis for that.

Children's Privacy

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 a top enforcement priority for this FTC,** and websites and other online properties that offer children's content, or are known to be used by children, are under increased scrutiny.
- On April 22, 2025, the FTC published the final amendments to the COPPA Rule, which becomes effective 60 days after this date; however; covered **"operators" have until April 22, 2026, to comply**.

Children's Privacy: COPPA Final Rule

The following are some ***key changes under the COPPA Final Rule***:

- **Expands the definition of "operator"** to include an online application or mobile application.
- Expands the definition of **"personal information" to include biometric data** to account for new methods of identification (such as voiceprints, Face ID, and gait analysis) and adds "**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."
- When determining whether a website or online service is **"directed to children"** the FTC will consider:
  - marketing and promotional materials;
  - representations made to consumers or third parties;
  - user or third-party reviews; and/or
  - **the age of users of similar websites or services**.
- **Defines "mixed audience"** websites or online services as not *primarily* directed to children and allows for certain exceptions for operators to avoid those websites or online services as "directed to children."

Children's Privacy: COPPA Final Rule, cont'd.

Parental notice and consent requirements have been strengthened:

- **Privacy Policy**: In addition to the description of the personal information being collected, used, and processed, **operators must disclose data retention practices, how persistent identifiers are used, the specific identities and categories of third parties that receive children's data, and how audio files are used and retained**.
- **Separate opt-in parental consent is required for any third-party disclosures that are not strictly necessary** to provide the product or service (e.g., AI model training, targeted advertising, and marketing).

Verifiable consent methods now include:

- **Facial recognition**: allows a parent's webcam image to be matched to a government ID (provided the images are deleted immediately after verification).
- **Text messages** to parents to initiate consent (provided children's data is not disclosed to third parties).
- **Knowledge-based authentication**: questions of a significant number and complexity that cannot be reasonably ascertained by a child.

Children’s Privacy: COPPA Final Rule, cont’d.

Increased security obligations:

- **Written Information Security Program (“WISP”):** Operators must implement a written information security program appropriate to its size and the sensitivity of children’s data retained. Detailed requirements in new § 312.8.

- **Data retention**: Children’s data **cannot be retained indefinitely,** so operators must ensure children’s data is only retained as long as reasonably necessary to fulfil the specific purpose(s) for which it was collected.

⚠ **Note for Educational Technology (“EdTech”) providers and Local Educational Agencies (“LEAs”)**: The FTC declined to codify long-standing guidance that permitted schools to authorize the collection of children’s data for EdTech services and not for commercial purposes. For now, the FTC will allow LEAs and EdTech providers to rely on its previous guidance.

Children's Privacy: The "Take It Down" Act

- On April 28, 2025, Congress passed a bipartisan bill known as the "Take it Down" Act that makes it a federal crime to "knowingly publish" (or threaten to publish) real or AI-generated intimate or sexual images without a person's consent.

- While not specific to children, the bill was allegedly inspired by a parent who states that it **took her almost a year** to get a social media company's messaging platform to remove an explicit **AI-generated deepfake of her 14-year-old daughter**.

- Websites and social media companies **must remove such material with 48 hours of the victim's request** and **take steps to delete any duplicate content**.

- Failure to reasonably comply with the notice and takedown obligations is enforceable by the FTC, and civil penalties are available under Section 18(a)(1)(B) of the FTC Act.

- The bill now awaits President Trump's signature.

Children’s Privacy: Notable Enforcement

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

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 app’s misrepresentations, especially about the AI content 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**.

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:** This seems like the kind of enforcement that will carry over to the Ferguson FTC.

- 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

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

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.

(So-Called) "Dark Patterns"

Privacy+
Security
Forum

Dark Patterns: Common Dark Patterns

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**
   - 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)***.

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.

- The **Ferguson FTC is unlikely to continue to use charged phrases like "commercial surveillance" and "dark patterns,"** but much of this discussion is centered on the elements of deception, and to that extent, the current FTC will likely continue to discourage these practices.

Dark Patterns: Notable Enforcement

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.
- In January 2025, the FTC finalized an order requiring H&R Block to pay $7M to be used for consumer compensation, and to make changes to its customer support practices (such as allowing product downgrades via chat versus calling customer support) to be implemented prior to the 2025 and 2026 tax seasons.

Questions & Contacts

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

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

Thank you!