Privacy + Security Forum

Session:
FTC Privacy Enforcement in 2026 and Beyond

May 8, 2026

Privacy + Security Forum

Speakers: FTC Privacy Enforcement in 2026 and Beyond

D. Reed Freeman
Partner and Chair,
Privacy and Data
Security Group

ArentFox Schiff LLP
Chief Privacy Officer

Reed.Freeman@afslaw.com

Michelle Bowling
Senior Associate
Privacy and Data
Security Group

ArentFox Schiff LLP

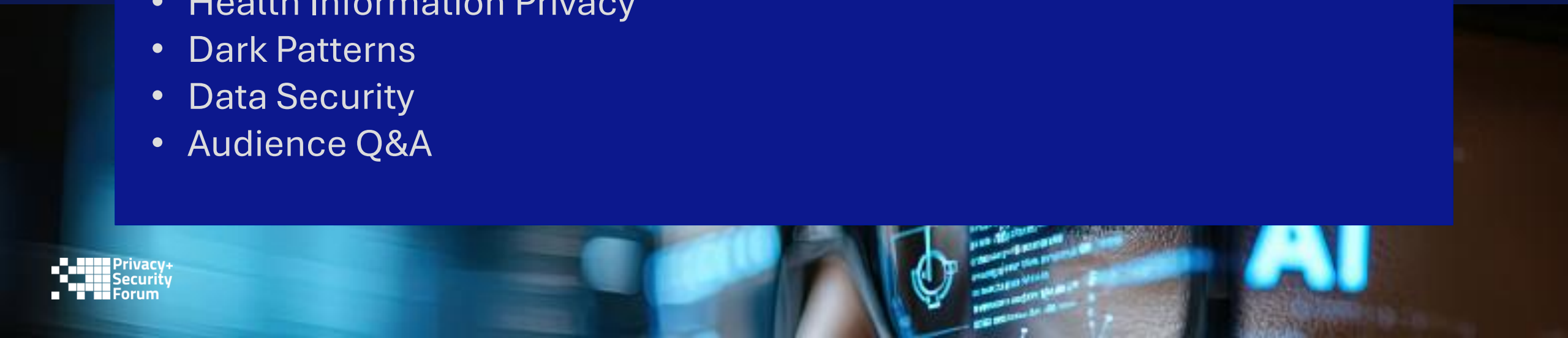
Michelle.Bowling@afslaw.com

Privacy+ Security Forum

Session: FTC Privacy Enforcement in Q2 2026 and Beyond

Agenda

- FTC Background
- Artificial Intelligence
- Data Brokers
- Children's Privacy
- Health Information Privacy
- Dark Patterns
- Data Security
- Audience Q&A



Privacy+ Security Forum

Background

Privacy+ Security Forum

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; under the Trump Administration Chairman Andrew Ferguson's FTC has pulled back much of this guidance.

- The FTC's February 2026 report to Congress notes the agency has brought more than 90 data security enforcement actions, suggesting an effort to strengthen corporate cybersecurity accountability.

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

Privacy+ Security Forum

- Andrew Ferguson became Chairman of the FTC on January 20, 2025, stating in his opening press release that the FTC will usher in, "**…a New Golden Age for American businesses, workers, and consumers**" but did not elaborate how. 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.

- On March 18, 2025, President Trump removed the two Democratic Commissioners and that November, Commissioner Melissa Holyoak (R) resigned to become U.S. Attorney for Utah, with the FTC now operating with only two of its five commissioner seats filled.

- President Trump nominated non-lawyer David MacNeil, the WeatherTech CEO to fill a vacancy; his confirmation is pending.

New Administration, New Priorities

- **New Focus:** **Data brokers** 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. Closely mirrors the DOJ's Bulk Data Transfer Rule, which applies to all entities, not just data brokers. Civil penalties available!

- As of April 2026, the FTC has not yet brought its first enforcement action under this statute, but plaintiff's attorneys are now using the Bulk Data Transfer Rule to allege illegal sales and transfers of consumer data to foreign adversaries (see, *Christy v. Lenovo, Inc.)*

- Focus on **responsiveness to CIDs** (same as state regulators): **In:** Advocacy; **Out:** Hide the ball.

New Administration, New Priorities

In April, the FTC published its FY 2026-2030 Strategic Plan, which will guide the agency over the next five years.

Core Objectives: This articulation of Ferguson-era privacy objectives largely aligns with prior FTC enforcement priorities.

COPPA & Children's Data Protection

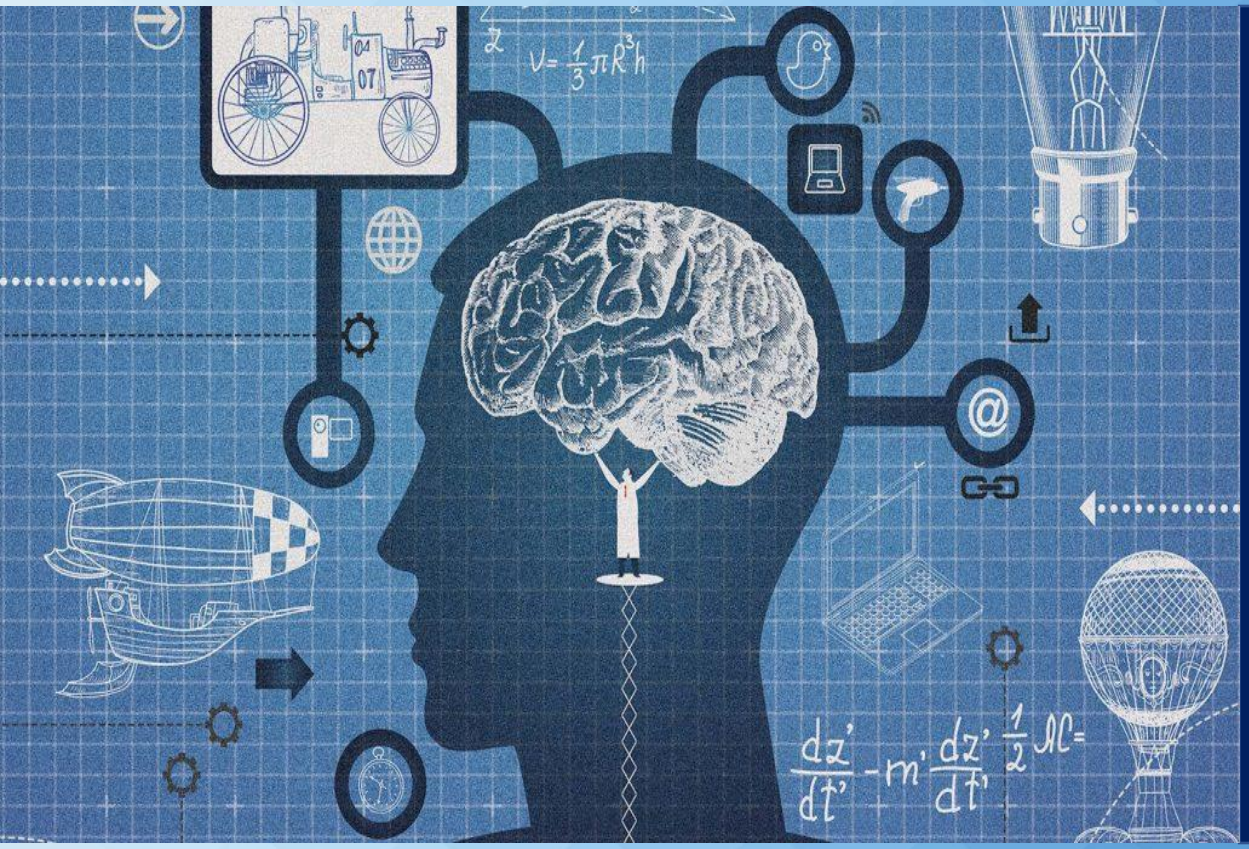
- FTC Chair calls protecting children online "one of the most important consumer protection issues of our time."
- Reinforces COPPA enforcement and new authority under the Take It Down Act.
- Signals heightened scrutiny of cookies, trackers, and age-related data practices for children.

Privacy & Data Security

- Elevated as a standalone enforcement priority, not just a subset of other programs.
- Plan emphasizes continued, tech-savvy enforcement supported by the FTC's Office of Technology.
- Cross-border data-security enforcement expected to increase.

Unlawful Telemarketing & Robocalls

- Telemarketing remains a top priority, with renewed focus on robocalls and Do Not Call Registry violations.
- Companies expected to tighten TCPA compliance and data-sharing practices.



Artificial Intelligence

Privacy+ Security Forum

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 in April 2025, panelists consisting of former FTC chairs and practitioners accurately predicted that the FTC **would 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.
- **Must substantiate claims on how AI tools work and on their efficacy.** Deception is in play for privacy cases.
- Focus on AI continues to be advertising law, rather than bias or discrimination.
- Deregulatory agenda "does not mean we're not going to break enforcement actions where AI is involved, and we will."

Artificial Intelligence in the FTC Blogs

The FTC's Business Blog and Technology Blog have provided additional guidance on the use of AI:

- In February 2024, businesses were warned that **quietly *and retroactively* changing privacy policies and terms of service to address new AI tools** could be considered deceptive acts or practices.
  - **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**.
  - **Out:** Focus on behavioral advertising. Holyoak: "There is no comprehensive federal privacy law that addresses these issues."

Section 6(b) Resolution on AI Companions

- **Six months after the April 2025 death of Adam Raine,** a 16-year-old who took his life following conversations with a ChatGPT chatbot, **the FTC launched an inquiry into seven large tech companies that provide consumer-facing AI chatbots**.

- The FTC's September 2025 press release announcing the inquiry alleges that AI chatbots, which use generative AI to simulate human interactions, can "**effectively mimic human characteristics, emotions, and intentions**, and generally are designed to communicate like a friend or confidant, which may prompt some users, especially children and teens, to trust and form relationships with chatbots."

- Citing the Trump-Vance FTC's goal of protecting children online, the inquiry's goal is to **determine whether companies are taking sufficient steps to evaluate the safety of their chatbots**, and to limit the use by and potential harms to, children and teens.
  - To date, no enforcement actions have resulted from this inquiry.
  - However, the FTC's January 2026 Age Verification Workshop and February 2026 COPPA Policy Statement on age verification signal the agency's continuing focus on minors' interactions with AI.

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.

Privacy+ Security Forum

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. The final order also requires Workado to create records that include copies of its ad and marketing materials for 10 years following the order and maintain those records for 5 years.

Artificial Intelligence: Notable Enforcement, cont'd.

Privacy+ Security Forum

Ascend Ecom– June 2025 (Pending)

- One of a handful of similar cases. Ascend Ecom advertising content claimed that its **"cutting edge" AI-powered tools could help consumers earn thousands of dollars a month** in passive income by opening online storefronts on large ecommerce platforms.
- The FTC's complaint alleged that Ascend, which operated under multiple different business names, charged consumers tens of thousands of dollars to open storefronts which did not produce the promised income and attempted to stop consumers from filing complaints or posting negative reviews about the company, **allegedly defrauding consumers of $25 million**.
- The proposed order would permanently ban the defendants from 1) selling or marketing similar products as services; 2) making deceptive claims about any unrelated products or services; and 3) including or enforcing contractual provisions restricting a consumer's ability to file complaints or reviews. **Defendants would also have to turn over its assets to compensate affected consumers**.

Artificial Intelligence: Notable Enforcement, cont'd.

Privacy+ Security Forum

Air.AI – August 2025 (Settled March 2026)

- The FTC alleged that Air.AI falsely claimed its "conversational AI" product could replace human representatives and generate significant profits for business owners, but consumers did not earn promised returns.

- FTC alleges consumers, many of whom are small business owners, lost as much as $250,000 and were often left in debt after relying on Air.AI's false promises.

- The order settling the Commission's allegations **bans the defendants from marketing business opportunities** and imposes a **monetary judgment of $18 million.**

Artificial Intelligence & Security

Privacy+ Security Forum

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 lowers the skill threshold for carrying out cyberattacks (e.g., phishing, malware, vulnerability scanning)
- Models can generate step-by-step instructions or exploit chains that previously required specialized knowledge; accelerating the spread of ransomware, credential-stuffing, and social-engineering attacks.

AI “going rogue” and not following instructions, creating vulnerabilities and chaos.

- “Rogue” behavior includes bypassing safety filters, generating insecure code, hallucinating system commands, or enabling unauthorized access.
- These failures can create new attack surfaces inside organizations that deploy AI tools.

Artificial Intelligence & Security

Privacy+ Security Forum

Philosophy on AI Enforcement Under Trump Administration:

- In his Senate testimony, Chairman Ferguson disclosed that the FTC's preliminary economic analysis of a Biden administration AI/algorithmic-pricing rulemaking would have created "staggering" compliance costs and criticized the EU AI Act as "a recipe for killing innovation."

- Made clear that the FTC's current AI approach is two-fold: enforcing existing statutes against fraud, misrepresentation, and harms to children, while explicitly disclaiming any role as a "general AI regulator" without congressional authorization.

Data Brokers

Privacy+ Security Forum

Data Brokers: Overview

Privacy+ Security Forum

Data brokers are (generally) **individuals or companies that specialize in the collection and sale/disclosure of personal information *about consumers* – *without having a direct relationship with those consumers* *(i.e., third-party data aggregators)***

In February 2026, the FTC sent letters to 13 data brokers warning them of their responsibility to comply with Protecting Americans' Data from Foreign Adversaries Act, which prohibits data brokers from selling, releasing, disclosing, or providing access to personally identifiable sensitive data about Americans to any foreign adversary, including North Korea, China, Russia, and Iran.

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 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, in which **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**.
- Of the $16.5 million available as a financial remedy for consumer redress, a total of $15.3 million was returned to 103,152 affected consumers who submitted a claim.

Data Brokers Enforcement Spotlight: Geolocation Data

Privacy+ Security Forum

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

Privacy+ Security Forum

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

Privacy+ Security Forum

<u>Ferguson Concurrence / Dissent</u>:

- **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

Privacy+ Security Forum

<u>Ferguson Concurrence / Dissent</u>:

- "[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.**

<u>But</u>:

- 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.

Data Brokers Enforcement Spotlight: Connected Vehicles

Privacy+ Security Forum

General Motors / OnStar

On January 14, 2026, the FTC finalized a sweeping order against General Motors and its subsidiary OnStar, settling allegations that the companies collected, used, and sold drivers' precise geolocation and driving behavior data from millions of vehicles **without adequate notice or consent** — and then sold that data to third parties, including companies that generated risk scores used by insurers.

Key provisions of the 20-year consent order include:

- **A five-year ban** on sharing consumer data with consumer reporting agencies.
- **Strict affirmative express consent** requirements before collecting or sharing geolocation and driving behavior data.
- A prohibition on user interfaces that manipulate or deceive users — for example, by inferring consent from silence or using confusing design elements (i.e., dark patterns by another name).
- Consumer rights to access, delete, and disable location tracking.
- A requirement that all third-party data recipients delete previously received GM/OnStar consumer data.

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 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' were required to comply by April 22, 2026 — a deadline that has now passed.**

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 May 19, 2025, the "TAKE IT DOWN" Act was signed into law, making it a federal crime to "knowingly publish" (or threaten to publish) real or AI-generated intimate or sexual images without a person's consent. Protecting children continues to be an enforcement priority.
- 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 FTC's civil enforcement authority over the Act's notice-and-takedown provisions **takes effect on May 19, 2026.**

Children's Privacy: Notable Enforcement

Large Entertainment Company – September 2025

- The FTC filed a complaint against a Large Entertainment Company, alleging that **the company collected personal data from children viewing child-directed videos on YouTube** without parental notification or consent in **violation of the COPPA Rule**.
- The FTC alleges that Large Entertainment Company failed to designate child-directed videos as "Made for Kids" prior to making them available on YouTube, instead making the designation at the channel level. The child-directed videos were then published to channels designated as "Not Made For Kids" and unlike the "Made for Kids" channels, **the "Not Made for Kids" channels do not automatically disable targeted advertising, auto-play, and comments**.
- On December 31, 2025, a federal judge approved the final order **requiring Large Entertainment Company to pay a $10 million civil penalty**, provide notice to parents, **'Audience Designation Program'** obtain COPPA-compliant verifiable parental consent, and ensure that each video is appropriately labeled.

Children's Privacy: Notable Enforcement

Apitor Technology Co. – September 2025

- Apitor is a China-based company that **sells robot toys targeted to children ages 6 to 14**. The toys include a **free companion mobile app that allows the toys to be controlled and programmed**.
- The FTC's complaint alleges that Apitor's mobile app required Android device users to enable the location permissions, **allowing the collection of precise geolocation information without verifiable parental consent** in violation of COPPA.
- Additionally, the FTC alleged that Apitor's integration of a third-party software development kit ("SDK") into is app and agreements with that third party allowed broad usage of data collected from the app, including for advertising purposes.
- Apitor has agreed to a **$500,000 civil penalty** and to injunctive provisions requiring it to provide notice to parents, **obtain verifiable parental consent, to retain children's personal information only as long as reasonably necessary to satisfy the purpose for which it was collected, and to honor deletion requests from parents**.

COPPA Age Verification Policy Statement

Privacy+ Security Forum

On February 25, 2026, the FTC issued a policy statement announcing that it **will not bring COPPA enforcement actions against operators that collect personal information solely for the purpose of age verification**, provided they meet the following conditions:

- *Purpose Limitation*: Data collected for age verification is used only for that purpose.
- *Prompt Deletion*: Age verification data is deleted promptly after verification is complete.
- *Vendor Oversight*: Operators that use third-party age verification services exercise appropriate oversight.
- *Transparency*: Privacy policies clearly disclose the age verification process.
- *Reasonable Accuracy*: Age verification methods are reasonably accurate.

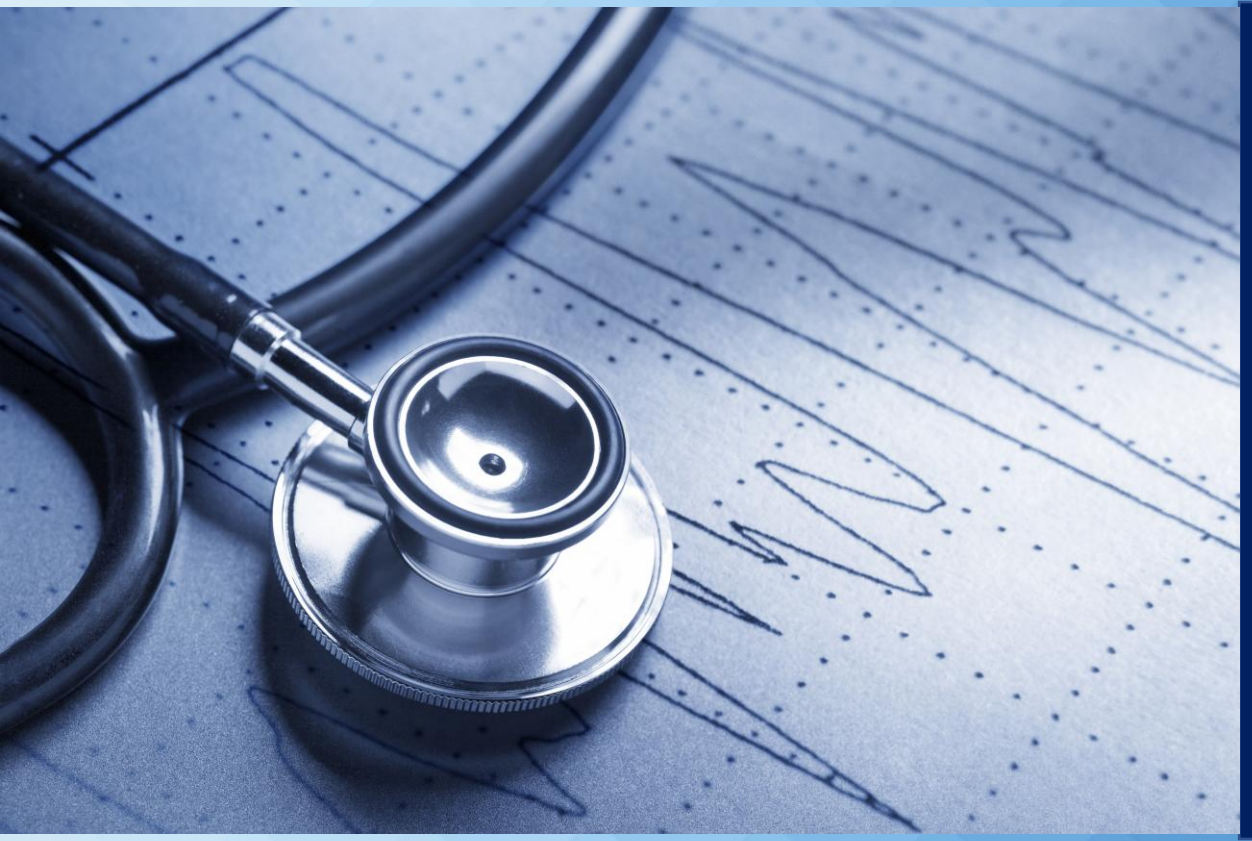
This policy statement was preceded by a January 28, 2026, Age Verification Workshop at which Chairman Ferguson signaled possible future COPPA Rule amendments to promote age verification technologies.

The statement is designed to remove a compliance barrier that had discouraged platforms from implementing age gates by assuring operators they will not face COPPA liability for verification-related data collection.

Children's Privacy: Key Takeaways

Privacy+ Security Forum

- ✓ 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. See *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:** 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.

- While the FTC continues to enforce the **Health Breach Notification Rule in 2025,** it has shifted its enforcement focus to health care employment noncompete agreements and antitrust enforcement.

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

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: Notable Enforcement

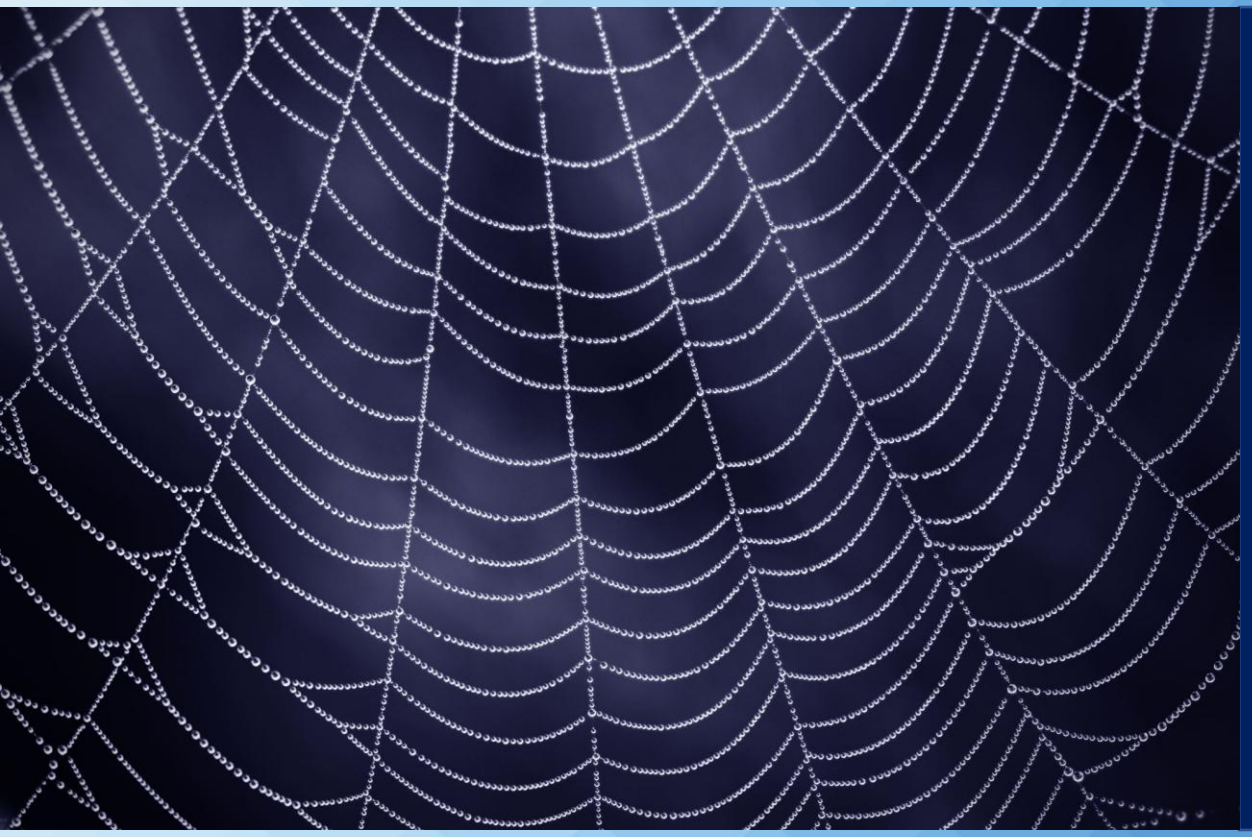
Privacy+ Security Forum

Assurance IQ and MediaAlpha, Inc. – August 2025

- MediaAlpha and Assurance used advertisements and websites claiming to provide health insurance quotes and to **collect personal information from consumers seeking to purchase health insurance**.

- The FTC alleges that Assurance and MediaAlpha did not sell any health insurance to consumers, and instead **used the information collected via its advertisements and websites to sell personal information to telemarketers**, which the FTC alleges amounted to **119 million consumer leads in 2024 alone**. Consumers that interacted with Assurance and MediaAlpha ads or websites were "bombarded" with telemarketing and robocalls, even those consumers listed in the Do Not Call Registry.

- On August 7, 2025, the FTC announced that **both companies agreed to pay a combined total of $145 million** to settle the FTC's complaint that it engaged in unfair and deceptive acts and practices by engaging in **unlawful lead generation**.



(So-Called) “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**). **This is still an enforcement priority.**
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)***. **This is still an enforcement priority.**

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).** **This is still an enforcement priority.**

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. **Maybe not such an enforcement priority now.**

Dark Patterns: Notable Enforcement

Privacy+ Security Forum

Chegg, Inc. – September 2025

- Chegg is an educational technology provider whose subscription-based services include homework assistance, textbook rentals, and writing tools.

- In September 2025, the FTC alleged that Chegg's deceptive billing and cancellation practices made it **"nearly impossible" for students and parents using its services to cancel auto-renewal subscription** services and **continued to charge consumers even after cancellations**.

- The FTC had also taken action against Chegg in 2022, following allegations that the company lacked security, allowing the exposure of sensitive personal information about millions of customers and its employees. Under the FTC's settlement, Chegg was **ordered to bolster its security practices to prevent data breaches and to delete unnecessary data**.

- Under the current proposed order, **Chegg will pay $7.5 million to provide refunds to affected consumers** and Chegg must maintain simple cancellation mechanisms.

Data Security

Privacy+ Security Forum

Data Security: FTC Priorities

Priorities from FTC's Official Senate Testimony

- **Section 5 as the Primary Data Security Tool:** Reaffirmed that Section 5 continues to be the primary tool in data security and deception cases but called it "not the ideally suited tool" for the modern data economy; the FTC must bend modern data economy problems — algorithmic pricing, mass surveillance, cross-platform tracking, AI-driven data processing — into legal standards originally crafted for traditional consumer fraud and deception.

- **Push for a National Privacy & Data Security Framework:** Chairman Ferguson explicitly urged Congress to advance a comprehensive federal privacy law, noting that current tools are insufficient for modern data risks.

- **Constraints & Need for Stronger Enforcement Tools:** limits on the FTC's ability to secure monetary redress after the Supreme Court's decision restricting Section 13(b) in *AMG Capital Management v. FTC*, but "Congress can fix that problem [by] enact[ing] legislation authorizing the FTC to obtain equitable monetary redress for consumers."

Data Security: Notable Enforcement

Educational Technology Provider— December 2025

- The FTC required Education Technology Provider to implement a comprehensive data security program after a breach exposed personal data of more than 10 million students.
- A hacker used the credentials of a former employee — who had departed three and a half years earlier — to access cloud databases for 13 days, exfiltrating names, addresses, dates of birth, student records, and health-related information.
- The FTC imposed no monetary penalty but required data deletion, a public retention schedule, and a comprehensive information security program.
- Notably, state attorneys general (California, Connecticut, New York) extracted $5.1 million in penalties for the same incident — illustrating the growing state/federal enforcement divergence.

Data Security: Notable Enforcement

Privacy+ Security Forum

Illusory Systems / Nomad — December 2025

- The FTC brought a complaint against Illusory Systems (d/b/a Nomad), a cross-chain crypto asset bridging protocol, for security vulnerabilities that allowed hackers to steal more than $186 million from consumers.

- The FTC alleged that Illusory touted its security in its advertising, claiming that it offered "security-first" services, when in fact, the company failed to live up to these promises by failing to use secure coding practices or implement processes for addressing vulnerability reports or security incidents.

- The settlement requires a comprehensive security program and biennial assessments.

Looking Ahead: Key Dates and Developments

I. **FTC Background:** The Ferguson FTC's FY 2026–2030 Strategic Plan elevates privacy and data security as a standalone enforcement priority, with deception-based Section 5 actions remaining the primary tool.

II. **Artificial Intelligence:** The FTC has deprioritized AI bias and discrimination cases in favor of enforcement against "AI washing" or unsubstantiated claims about AI product capabilities, while also launching an inquiry into AI chatbot safety for children.

III. **Data Brokers:** Enforcement actions under the Protecting Americans' Data from Foreign Adversaries Act signal that selling or sharing precise geolocation and other sensitive data without consent will draw significant FTC scrutiny.

IV. **Children's Privacy:** The amended COPPA Rule's April 22, 2026 compliance deadline has passed, requiring operators to meet expanded parental consent, data retention, and written information security program obligations — while new enforcement tools under the TAKE IT DOWN Act take effect May 19, 2026.

V. **Health Information Privacy:** The FTC continues to target companies that use tracking pixels, cookies, and SDKs on health-related platforms to collect and disclose sensitive health information without consumer consent.

VI. **Dark Patterns:** Difficult cancellation flows, misleading purchase interfaces, hidden terms, and design tricks that steer consumers into sharing unnecessary data remain high-priority enforcement targets.

VII. **Data Security:** The FTC requiring comprehensive security programs for basic failures, while state attorneys general are stepping up to impose monetary penalties the that the FTC cannot impose post-*AMG Capital Management*.

Questions & Contacts

D. Reed Freeman, Jr.
Partner and Chair, Privacy
and Data Security Group

ArentFox Schiff LLP
Reed.Freeman@afslaw.com

Michelle Bowling
Senior Associate, Privacy and
Data Security Group

ArentFox Schiff LLP
Michelle.Bowling@afslaw.com

Thank you!