



WHITE & CASE

FTC Year in Review White & Case

F. Paul Pittman and Mark Williams

Agenda

1 Overview of FTC's role in privacy and cybersecurity

2 Overview of FTC enforcement trends

A closer look at cases of note

- 3**
- Kochava
 - Epic Games
 - BetterHelp
 - Blackbaud

4 Overview of FTC rulemaking activity

5 Conclusions

Overview of FTC's role

- ❑ Enforces Section 5 of the FTC Act as well as some other privacy-focused laws (e.g., FCRA, GLBA)
- ❑ FTC has issued rules under Section 5
 - COPPA
 - Health Breach Notification Rule
- ❑ No ability to obtain monetary relief unless defendant has (i) violated an applicable FTC order or rule; or (ii) engaged in dishonest or fraudulent conduct
- ❑ FTC can bring a Section 5 action in a U.S. District Court or through an Administrative Law Judge (“ALJ”) working at the FTC



Overview of Section 5

- Section 5 of the FTC Act bans unfair and deceptive acts and practices in or affecting interstate commerce.
- Deceptive practices involve:
 - a material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances.
- An act or practice is unfair if it:
 - causes or is likely to cause substantial injury to consumers which is:
 - not reasonably avoidable by consumers themselves and
 - not outweighed by countervailing benefits to consumers or to competition.

Overview of FTC enforcement trends

- FTC under Lina Khan as taken a more aggressive approach
- FTC's budget has increased recently
- Commission has stated it will take a harm-based approach to enforcement:
 - Sensitive data, including:
 - Data collected from children
 - Health data
 - Precise location data
 - “Commercial surveillance”
 - Cybersecurity and breach reporting

Overview of FTC enforcement trends

- Fifteen consent orders and two unsettled complaints in the last year
- Kochava and Facebook are litigating against the FTC
- Commission obtained \$607 million in monetary relief
 - \$520 million from Epic Games
 - Fines much higher for COPPA violations



FTC Focused on Sensitive Data

- All cases involved data the FTC considers to be sensitive:
 - Bank account/other financial data (Global Tel*Link Corp, Blackbaud)
 - Browsing data (Avast)
 - Precise geolocation data (Kochava, InMarket Media, X-Mode Social/Outlogic)
 - Data collected from Children (Epic Games, Facebook, Edmodo, Amazon, Microsoft)
 - Biometric data (Rite Aid)
 - Criminal record data (TruthFinder)
 - Health data (1Health.io, BetterHelp, Easy Healthcare)
 - Private videos (Ring)

Kochava: Willing to fight

- ❑ Kochava filed pre-emptive complaint against FTC in D. Idaho on August 12, 2022
- ❑ FTC filed complaint against Kochava in D. Idaho on August 29, 2022 alleging:
 - Kochava sold geolocation data that can be used to trace the movements of individuals to and from sensitive locations
 - The device-level data that Kochava shares can be associated with people
 - Kochava doesn't adequately protect sensitive PI from exposure



Kochava: Willing to fight

- Kochava filed MTD arguing:
 - Complaint insufficiently alleged Kochava engaged in unfair conduct
 - FTC Act is unconstitutional
- Court granted MTD in May 2023 holding:
 - FTC did not allege consumers were injured or likely to be injured
 - Privacy harms alleged in complaint did not constitute “substantial injury”
 - Court denied Kochava’s other arguments



Kochava: Willing to fight

- ❑ FTC re-filed complaint in June 2023
- ❑ Kochava again moved to dismiss complaint
- ❑ Judge denied MTD on February 3, holding:
 - Complaint adequately alleged that the targeting of consumers based on geolocation data has and does occur
 - Complaint adequately alleges an invasion of privacy, “which is substantial both in quantity and quality,” that plausibly constitutes a substantial injury to consumers



Epic Games

- ❑ FTC announced complaint, settlement against Avast on February 22
- ❑ FTC alleged:
 - Epic Games violated COPPA by knowingly collecting personal information from U13s
 - Fortnite's text and voice communications features harmed children and teens
 - The company used dark patterns to trick players into making unwanted purchases and let children rack up unauthorized charges without any parental involvement



Epic Games

- Under the consent agreement Epic Games must:
 - Pay \$520 million in monetary relief
 - \$275 for COPPA violations
 - \$245 for refunds to consumers for using dark patterns
 - Only enable Fortnite's text and voice communications for U13s and teens after opt-in consent
 - Delete PI of U13s unless it obtains parental consent
 - Implement a comprehensive privacy program
 - Obtain regular, independent audits
- Epic Games is also prohibited from:
 - Charging consumers through the use of dark patterns or from otherwise charging consumers without obtaining their affirmative consent



BetterHelp

- FTC announced complaint, settlement against BetterHelp on March 2, 2023
- FTC alleged BetterHelp:
 - Promised consumers that it would not use or disclose their personal health data except for limited purposes, such as to provide counseling services
 - Revealed consumers' email addresses, IP addresses, and health questionnaire information to third parties for advertising purposes
 - Did not obtain consumers' consent prior to sharing health information
 - Did not place restrictions on third parties' use of health information



BetterHelp

- Per consent agreement, Better Help must:
 - Pay \$7.8 in monetary relief
 - Obtain affirmative express consent before disclosing personal information to third parties
 - Implement a comprehensive privacy program that includes strong safeguards to protect consumer data
 - Direct third parties to delete the consumer health and other personal data that BetterHelp revealed to them
 - Limit how long it can retain personal and health information according to a data retention schedule



Blackbaud

- ❑ FTC announced complaint, settlement against Blackbaud on February 1
- ❑ FTC alleged Blackbaud:
 - Failed to implement appropriate safeguards to secure and protect the “vast amounts” of personal data it maintains
 - Blackbaud told its customers that it took “appropriate physical, electronic and procedural safeguards to protect [] personal information” but failed to put in place such safeguards
 - Failed to provide timely notice to affected individuals



blackbaud®

Blackbaud

- Per consent agreement, Blackbaud must:
 - Delete data that it no longer needs
 - Develop a comprehensive information security program with detailed requirements, including encryption, intrusion detection, data segmentation, logging and auditing, and MFA
 - Implement a data retention schedule and publish that schedule on its website
 - Notify the FTC if it experiences a future data breach that it is required to report to any other local, state, or federal agency



blackbaud®

FTC's Rulemaking Powers

- FTC can issue rules under Section 5, but the process is lengthy, cumbersome, and subject to pushback
 - Mag-Moss rulemaking process is substantially more burdensome than typical procedure under the Administrative Procedures Act
- In August 2022, FTC released an Advance Notice of Proposed Rulemaking (“ANPR”) on “commercial surveillance” and data security
 - Commission sought input on potential new rules that cover a broad range of activities the FTC considers harmful
 - Comment period closed in November 2022
 - No action by FTC since ANPR

FTC's Rulemaking Powers

Magnuson-Moss

Advanced Notice of Proposed Rulemaking

Public comment

Notice of Proposed Rulemaking

Public comment

Informal hearings

Final Rule

Judicial review – “substantial evidence”

Administrative Procedure Act

Notice of Proposed Rulemaking

Public comment

Final Rule

Concluding thoughts

- ❑ FTC has taken a much more aggressive stance
- ❑ FTC is continuing to focus on sensitive data
 - But powers of the commission are still limited
- ❑ Promulgating rules under Section 5 is difficult
 - But would allow FTC to issue hefty fines (i.e., increase deterrence)
- ❑ When taking a risk-based approach to privacy:
 - Ensure disclosures are detailed and accurate
 - Obtain opt-in consent for unexpected use of sensitive data, new data uses





WHITE & CASE

In this presentation, White & Case means the international legal practice comprising White & Case LLP, a New York State registered limited liability partnership, White & Case LLP, a limited liability partnership incorporated under English law and all other affiliated partnerships, companies and entities.