Cooley

Level Up Your Privacy and Cybersecurity Game

May 27, 2025

Enrique Capdevila

Christian Lee

Christopher Suhler

Today's speakers

Enrique Capdevila
Special Counsel
Cyber/data/privacy
Brussels, Belgium

Christian Lee
Special Counsel
Cyber/data/privacy
San Francisco, CA

Christopher Suhler
Associate
Cyber/data/privacy
Denver, CO

Disclaimer

This presentation is provided for general informational purposes only and no attorney-client relationship with the law firm Cooley LLP and Cooley (UK) LLP is created with you when you attend or use it. By attending or using this presentation, you agree that the information in it does not constitute legal or other professional advice. This presentation is not a substitute for obtaining legal advice from a qualified attorney licensed in your state. The information in this presentation may be changed without notice and is not guaranteed to be complete, correct or up-to-date, and may not reflect the most current legal developments. The opinions expressed by the presenters are theirs only and not those of Cooley LLP and Cooley (UK) LLP.

Agenda

1. Why privacy and cybersecurity matter for game companies
2. Legal landscape: U.S.
3. Legal landscape: Europe
4. Other sources of obligations
5. Enforcement actions
6. Key takeaways

Why privacy and cybersecurity matter for gaming companies

Cooley

Introduction

- Why should gaming companies care about privacy and cybersecurity issues?
  - Legal and regulatory obligations
    - Platform requirements
    - Emerging rules
  - Consumer expectations
  - Investor expectations
  - Reduce legal risk
  - Affect product features
- Today: issue spotting key sources of obligations and risks

Why video game companies?

- Fewer geographic barriers
  - Worldwide user populations
  - Localization
  - Advertising campaigns
- Appeal to children
- Volume of personal data processed
- Types of data processed
- Social and other interactive features
- Distribution via digital storefronts
- Monetization strategies

Web of privacy obligations

- U.S. states' general consumer privacy laws
- Subject-matter specific laws
  - Children's data
  - Health data
  - Video viewing
  - Artificial intelligence
  - Wiretapping
  - Social media
- Cross-border data transfer restrictions
  - New DOJ rule on "bulk" sensitive personal data
- App store (platform) rules
- GDPR and other international laws

Legal landscape: U.S.

Cooley

U.S. state comprehensive privacy laws

- 19 U.S. state laws (and counting)
  - Applicability thresholds based on:
    - Total annual revenue
    - Number of data subjects (typically 35k-100k)
    - Data sales
  - Obligations include:
    - Providing a privacy policy, including state law-specific disclosures
    - Honoring data subject rights/requests
    - Providing and honoring other opt-outs (e.g., do not sell/share)
    - Complying with consent/usage restrictions (e.g., for sensitive PI)
    - Implementing contractual privacy protections
    - Obligations for very high-volume processing

Children’s privacy

- Children’s data is subject to additional obligations and scrutiny
- Children's Online Privacy Protection Act (COPPA)
  - Applies to websites or online services “directed to children”
    - Considers factors like subject matter, video/audio content (e.g., cartoony graphics), and marketing activities
  - Compliance obligations include:
    - Privacy notice to parents
    - Parental consent before collecting children’s personal information
  - 2025 amendments require consent for certain third-party disclosures (incl. targeted ads) and limits on data retention
- State comprehensive privacy laws
  - Often have special requirements for children’s personal information (e.g., consent, opt-outs, thresholds for cybersecurity audits)

Kids Online Safety Act (KOSA)

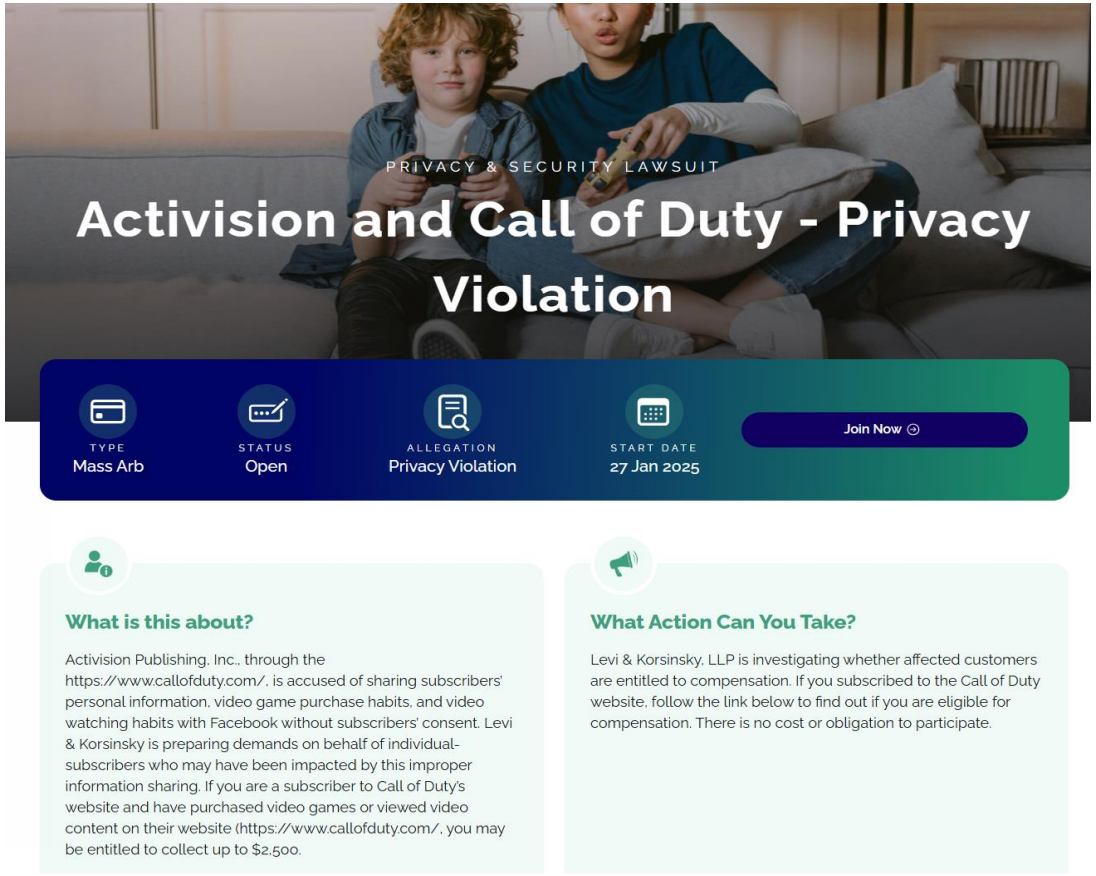
- Bill reintroduced in mid-May 2025
- "Covered platforms" explicitly include "online video games"
  - Games that have creation/uploading of (non-incidental) content, in-game purchases, or user-to-user communication
- Key obligations
  - **Duty of care** that "design features" are implemented so as to prevent and mitigate foreseeable harms to minors, including:
    - Patterns of use that indicate "compulsive usage" ("persistent and repetitive use . . . that significantly impacts one or more major life activities of an individual, including socializing, sleeping, eating, learning, reading, concentrating…")
    - Financial harms caused by unfair or deceptive acts or practices
  - **Safeguards and parental tools** that limit things like communication, time on the platform, personalized recommendations, and features intended to increase frequency/activity on the platform
    - Such safeguards must be set by default to their "most protective" setting for known minors
  - **Reporting, transparency, and disclosure** requirements
- Could require game companies to reassess and fundamentally modify core gameplay, monetization, and other systems of their games (at least for minors)
  - For example: gameplay loops, monetization mechanisms and engagement/progression systems (e.g., battle passes)

Consumer health data privacy laws (WA, NV, CT)

- Broad definitions of “consumer health data”: information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status.
- Obligations include:
  - Stringent consent requirements
  - Standalone consumer health data privacy policy
  - Honoring data subject rights/requests
  - Abiding by sale/sharing restrictions
- Potential applicability to games:
  - In-game accessibility choices could indicate physical health status (e.g., vision or movement conditions)
  - Patterns of gameplay or inputs could indicate physical or mental health status (e.g., obsessively reloading could indicate anxiety/stress)
  - Precise geolocation data could indicate attempts to seek healthcare services

Video Privacy Protection Act (VPPA)

- "Video tape service providers" must get consent to share PII of consumers
  - Subscriber/purchaser?
  - Pre-recorded video content?
  - PII?
- Gaming companies
  - Host video content (e.g., trailers, gameplay, dev videos) on their websites
  - In-game cutscenes
- Activision/COD litigation campaign in early 2025
  - Alleges that Activision "shar[ed] subscribers' personal information, video game purchase habits, and video watching habits with Facebook without subscribers' consent"
  - Currently recruiting plaintiffs, promising that they "may be entitled to collect up to $2,500"



AI laws

- Laws enacted in Colorado, Utah, California
  - Proposed in many other states
- Applicability depends on how AI is used
  - Developer of AI system
  - Deployer of AI system that is “high-risk” (makes a consequential decision on providing or denying fundamental services)
  - Different requirements based on type of AI system and entity
- Obligations
  - Transparency, such pre-use notice or specific disclosures about specific technologies (e.g., chatbot is being used)
  - Protections for consumers against algorithmic discrimination
  - Organizational-level requirements: risk management policies, risk/impact assessments, consumer rights
- AI in games
  - AI systems in game development tools
  - AI systems in games
  - Chatbot-driven NPCs

DOJ Bulk Sensitive Personal Data Rule

- Covers data transactions of U.S. companies that involve access to bulk U.S. sensitive personal data by persons/entities with ties to countries of concern (including China)
  - Could impact game companies with Chinese investors and/or employees
- "Bulk U.S. sensitive personal data" that game companies may collect includes:
  - Precise geolocation data of >1,000 U.S. devices
  - Personal financial data of >10,000 U.S. persons
  - Personal health data of >10,000 U.S. persons
  - Covered personal identifiers of >100,000 U.S. persons
- Some transactions are prohibited
- Some transactions are restricted – i.e., permitted if company complies with certain privacy and cybersecurity obligations

Other laws

- Wiretapping laws
  - Applied to technologies like chatbots, analytics, and advertising cookies/pixels, as well as SDKs for mobile games
  - Common basis for demands by plaintiffs' firms
- Age verification and social media laws
  - Passed in a number of states, but most have been enjoined
  - Impose requirements such as age verification/parental consent to access social media platforms
    - Also restrictions on certain features such as algorithmic feeds
  - Some laws exclude games, but some laws and some requirements would also explicitly apply to online games (e.g., Ohio) and/or could apply to certain games depending on their social features
  - Also "age-appropriate design codes" (e.g., California)

Legal landscape: EU

Cooley

Comprehensive legal framework (non-exhaustive list)

- **General Data Protection Regulation (GDPR):** Core privacy law regulating how game developers and publishers collect, use, and store personal data—relevant for player profiling, analytics, marketing, and age verification.
- **ePrivacy Directive:** Governs the use of cookies, tracking technologies, and direct marketing—especially relevant for in-game advertising, web-based games, and mobile apps.
- **Digital Services Act (DSA):** Applies to gaming platforms that host user-generated content or enable interaction (e.g., chat, mods, virtual marketplaces); imposes obligations around content moderation, transparency, and platform accountability.
- **Digital Markets Act (DMA):** Targets gatekeeper platforms—implications for distribution platforms and app stores (e.g., Apple App Store, Google Play) that may control access to users or developers.
- **Cyber Resilience Act (CRA):** Introduces mandatory cybersecurity requirements for hardware and software products, including video games and connected gaming devices (e.g., consoles, VR headsets).
- **Artificial Intelligence Act (AI Act)**: May apply where AI systems are embedded in games (e.g., adaptive gameplay, moderation tools, behavioral analytics); rules depend on risk classification and purpose of use.
- **Consumer protection legislation:** prohibition of dark patterns, transparency on pricing, in-game purchases and in-game currencies.

Privacy

- EU/UK GDPR
  - Applicability can extend to non-European companies, for example if they:
    - Target goods/services to the EU/UK
    - Monitor the behavior of EU/UK individuals
  - Obligations include:
    - Satisfying transparency obligations
    - Honoring data subject rights/requests
    - Abiding by stringent consent requirements
    - Appointing local data representatives
    - Contractual terms
    - Complying with cross-border data transfer restrictions
- ePrivacy

Digital Services Act

- Scope: e.g.: developers, providers of online games, app stores, communities of players and other online platforms with user-generated content may qualify as intermediary services under the DSA.
- No duty to monitor, but a duty to act upon awareness.
- User-generated content & moderation: Games that allow players to upload, share or communicate content (e.g., chat, custom skins, photos, etc.) must implement:
  - clear terms of use
  - notice and action mechanisms,
  - statement of reasons for content removal.
- Trusted flagger mechanism: online platforms may be required to cooperate with trusted flaggers who report illegal content—this affects moderation workflows and response times.
- Transparency reporting: obligation to publish periodic transparency reports detailing content moderation actions, notice handling, use of automated tools, and appeals statistics.
- Minors and default settings: Platforms likely to be accessed by minors must adopt appropriate protections by design and by default, including safer moderation, privacy settings.
- Fines: Up to 6% of the provider’s total worldwide annual turnover for serious breaches of the DSA.
- Enforcement: on-site inspections, restrictions, also criminal sanctions.

Cyber Resilience Act (CRA)

- Scope: The CRA applies to products with digital elements, including software and hardware—video games, game consoles, apps, and connected devices (e.g. VR headsets) may fall within scope.
- Standalone software covered: Most video games distributed as standalone software or through digital platforms (PC, console, mobile) are considered “products with digital elements” and must meet CRA cybersecurity requirements.
- Security-by-design obligations: Game developers and publishers must ensure that cybersecurity is embedded throughout the lifecycle of the game—design, development, distribution and patching.
- Mandatory vulnerability handling: Companies must establish vulnerability reporting processes and address security flaws through timely updates (including security patches).
- Risk categorization: If the game includes features like online multiplayer, voice chat, payment functionalities, or interacts with critical infrastructure, it could be classified as a “critical product”, triggering stricter obligations.
- Supply chain responsibility: Studios using third-party engines, plug-ins, or assets (e.g. Unity, Unreal) must assess their cybersecurity posture and ensure CRA compliance for components integrated into their games.
- Conformity assessments: Most games will need to undergo a self-assessment, but those with high-risk features (e.g. games controlling hardware or integrating AI/IoT elements) may require third-party certification.
- Post-market obligations: Even after launch, developers must monitor security risks and maintain technical documentation.
- Fines and enforcement: Non-compliance with the CRA can lead to significant fines (up to €15M or 2.5% of global annual turnover).

AI Act

- Use cases:
  - Adaptive gameplay: AI-driven systems that tailor game difficulty or narrative based on player behavior.
  - NPC behavior: Sophisticated AI used for non-playable characters' decision-making and realism.
  - In-game moderation: AI tools for detecting toxic behavior, cheating, or illegal content in chats or user-generated content.
  - Personalization and recommendation systems: Suggesting games or content based on player profiles—may trigger transparency requirements.
  - AI in matchmaking: Used in multiplayer games to match players based on skill level or behavior.
- Risk categorization:
  - Most gaming-related AI systems will likely fall under minimal or limited risk
  - However, AI systems used for content moderation, profiling of minors, or biometric-based emotion recognition (e.g., in VR) may fall under high-risk, triggering stricter obligations.
- Obligations (depending on the level of risk):
  - Perform a conformity assessment
  - Implement risk management systems
  - Maintain technical documentation
  - Enable human oversight
  - Ensure robust data governance
  - Transparency
- Maximum administrative fines: up to €35 million or 7% of global annual turnover

Consumer Protection Legislation

- Multiple current and future regulations (like the Digital Fairness Act)
- There is a specific framework regulating contracts for supplying digital content or digital services, including video games.
- Transparency obligations:
  - Not only applicable to pricing or ranking criteria
  - Players must be informed if they are interacting with a trader or another consumer (especially relevant in user marketplaces or trading features).
- In-game purchases & dark patterns:
  - The use of manipulative design (e.g., hiding costs, pressure tactics) is under scrutiny.
  - Obligation to inform users of real-money purchases
  - Loot boxes are heavily regulated.
  - Geo-blocking rules prevent unjustified restrictions on cross-border access to games, platform stores and subscription services.
  - Age and vulnerability considerations: Games targeted at minors must ensure age-appropriate content, age verification requirements
- BEUC (the European Consumer Organization) complaint
  - In 2024, BEUC filed a coordinated complaint with the European Commission and national consumer protection authorities, targeting major video game publishers for the use of manipulative in-game design practices, such as loot boxes, aggressive monetization and dark patterns.
  - The complaint argues that these practices exploit consumer vulnerabilities, particularly among children and adolescents, and likely infringe different consumer protection laws.
  - If the complaint is upheld, it could lead to enforcement actions, including fines, mandatory design changes and the ban of certain monetization mechanics across the EU. It also increases regulatory pressure on the gaming industry to adopt more transparent, age-appropriate and ethically compliant business models.

Beyond the U.S. and Europe

- Numerous other jurisdictions have privacy regimes
  - Including large markets such as China (PIPL) and Brazil (LGPD)
- Compliance with U.S. and (especially) European privacy laws can often provide a good starting point for a global privacy compliance program
  - May require work with local counsel to assist with additional, jurisdiction-specific compliance requirements

Other sources of privacy obligations

Cooley

Platform rules

- Mobile app / gaming platforms may have privacy requirements. For example:
  - Apple App Store App Review Guidelines
  - Google Play Developer Program Policies
- Obligations go beyond those in privacy laws
  - Unique privacy policy disclosures
  - Restricting how game companies can use or share data of platform users
  - Requiring companies to offer account and/or content deletion features
  - Requiring consent to access/collect certain data
- Failure to comply with these obligations will delay or prevent access to a platform

Agreements

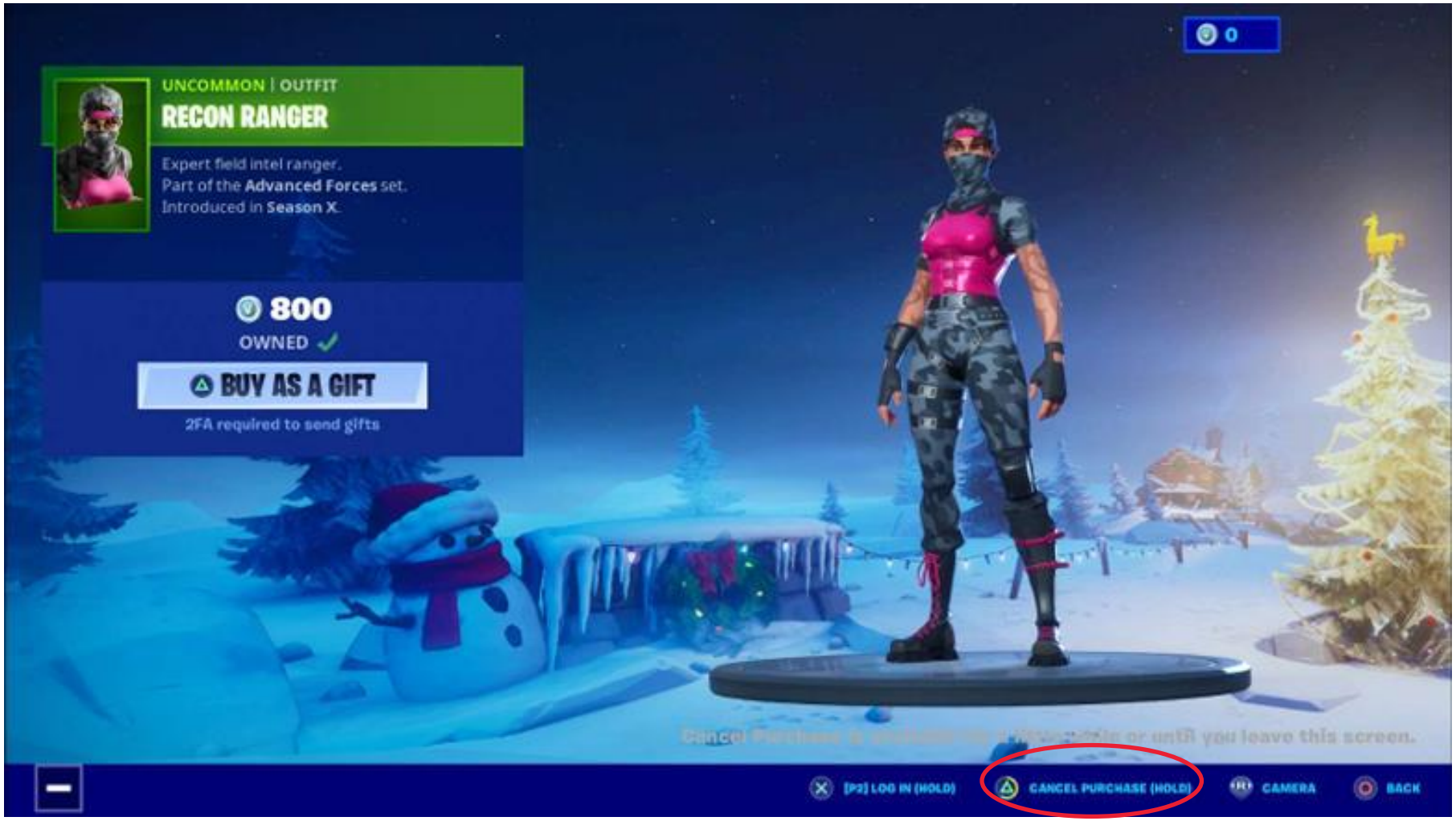
NVCA IRA:

5.13 [Cybersecurity. The Company shall, within 180 days following the date of this Agreement, use commercially reasonable efforts to: (a) identify the Company's confidential business information, trade secrets, and any information about identified or identifiable natural persons maintained, disclosed, or otherwise processed by or on behalf of the Company (collectively, "Protected Data") and the Company's servers, laptops, desktops, cloud computing, containers, virtual environments, data centers, and/or other Company or vendor systems and applications that process Protected Data, or are used to provide, host or enable the Company's operations or services (collectively, "Systems"); (b) restrict access to Protected Data and Systems to those individuals or entities who have a need to access such Protected Data and Systems; (c) conduct a commercially reasonable risk assessment to evaluate the potential risks, vulnerabilities, and threats to Protected Data and Systems; (d) implement and maintain commercially reasonable physical, technical and administrative safeguards designed to protect the security, confidentiality, integrity and availability of all Protected Data and Systems, and (e) provide its applicable employees, agents, and contractors with privacy and security training as determined reasonably necessary by the Company.]

Enforcement Actions

Cooley

In the Matter of Epic Games (FTC)



In the Matter of Epic Games (FTC)

- Enforcement alleged COPPA violations and dark patterns
- Settlements with Epic (maker of Fortnite) totaling $520 million
  - $275 million for COPPA violations
    - Collection of children's PI without notice to or verifiable consent from parents
    - Largest-ever penalty for violation of an FTC rule
    - Settlement requires Epic to adopt stronger default privacy settings, including text/voice off by default
  - $245 million for UDAP violations related to in-game monetization
    - Dark patterns to trick users into making unintended in-game purchases (e.g., inconsistent, confusing button configurations on payment screens)
      - FTC received over 1 million consumer complaints
    - Lack of consent from cardholder/parent; banning users who dispute charges
    - Settlement prohibits Epic from use of dark patterns, charging without consent and banning users who dispute unauthorized charges

Enforcement actions: U.S.

In the Matter of Cognosphere (FTC)

- Enforcement alleged COPPA and UDAP violations
  - Settlement with Cognosphere (maker of Genshin Impact): $20 million fine
- COPPA violations: Collection of children's PI without notice to or verifiable consent from parents
  - FTC cited Genshin Impact's graphics, animation, characters and promotion through influencers popular with children as grounds that the game is directed to children
- UDAP violations: Dark patterns to obscure true costs/odds of obtaining in-game assets and entice players to open loot boxes
- Also requires Cognosphere to change the violative practices, including by:
  - Offering an option to directly purchase loot boxes with real money (not just virtual currency)
  - Disclose loot box odds and virtual currency exchange rates
  - Not allowing under-16s to purchase loot boxes without a parent's affirmative express consent

California v. Tilting Point Media (CA AG)

- Enforcement alleged CCPA and COPPA violations by maker of a SpongeBob mobile game
  - Settlement with Tilting Point Media: $500,000 civil penalty
- Lack of parental consent to collect children's data, as well as inadequate age gating
  - Including misconfigured third-party SDKs that resulted in collection and sale of children's data
- Injunctive relief includes: use of neutral age gating screens, enhanced SDK governance and providing just-in-time notice for sales/sharing of children's PI

Enforcement actions: Europe

EU Consumer Protection Cooperation Network (CPC): Alleged children's privacy and consumer protection violations by maker of Star Stable Online

- Test case for EU's new legal principles on virtual currencies
- Among other effects, these principles give virtual purchases protections similar to those for physical goods

Key takeaways

Cooley

Get out ahead of the game

- Spot potential issues early on
- Understand contractual obligations
- Understand data flows (“data mapping”)
- Assess areas with higher risk or more burdensome compliance requirements
  - Types of activities
  - Types of data handled or data subjects
- Assess exposure to different jurisdictions
- Determine organization’s risk tolerance
- Determine approach – one sized fits all?
- Gap assessment
- Implement mitigation strategies

Questions?

Cooley