RETROSPECTIVE

US POLICY

Top Six Major Privacy Enforcement Trends

FPF U.S. Legislation Retrospective

June 2024

Authored By: **Jordan Francis**, Policy Counsel, U.S. Legislation
Bailey Sanchez, Senior Counsel, U.S. Legislation

FUTURE OF PRIVACY FORUM

Authored By:

Jordan Francis
Policy Counsel for U.S. Legislation, Future of Privacy Forum

Bailey Sanchez
Senior Counsel for U.S. Legislation, Future of Privacy Forum

Acknowledgements:

The authors thank Nick Alereza, Keir Lamont, Tatiana Rice, Felicity Slater, and Jordan Wrigley for their contributions to this report.

Executive Summary

This Retrospective focuses on six major enforcement trends that have recently spoken to key questions or policy issues in the privacy landscape. U.S. commercial privacy rules are rapidly evolving and there have been dozens of enforcement actions at the state and federal levels over the last few years. However, the enforcement actions analyzed below are some of the most significant for understanding important through lines ranging from what constitutes a privacy violation to how expanding regulatory interest in the risks of collecting, inferring, and using sensitive data.

1. **DoorDash: The Right to Cure Under State Law is Not Absolute**: The California Privacy Protection Agency's second enforcement action provides insight into what constitutes a "sale" under state privacy laws, as well as the limitations of businesses' statutory 'right to cure' alleged violations.
2. **GoodRx, BetterHelp, Premom: Unauthorized Disclosures of Health Information as Breaches:** The FTC enforced the Health Breach Notification Rule for the first time since it was finalized in 2009, arguing that unauthorized disclosures of health data can constitute a breach.
3. **Betterhelp and Vitagene: Health Information (and Its Sensitivity) is Contextual and Situational:** When it comes to companies that process health information that is outside the scope of HIPAA, the FTC demonstrated that personal health information may be created based on context and situation.
4. **Epic Games: FTC Focuses on Impact of Design Choices on Teen Privacy:** The FTC is wielding its Section 5 authority to protect the privacy of teenagers as Congress continues to consider amending COPPA to establish federal privacy protections for teens.
5. **Cothron v. White Castle: Multiple Actionable Harms from Single Privacy Violations Spur Legislative Change:** In *Cothron v. White Castle*, the Illinois Supreme Court addressed the critical question of when privacy claims accrue under the Illinois Biometric Information Privacy Act, prompting the Illinois legislature to amend the Act's private right of action.
6. **FTC v. Kochava: How Location Data Sales Impact Privacy Interests:** In *FTC v. Kochava*, the Commission argues that the collection and disclosure of location data can constitute an injury under Section 5 of the FTC Act.

Table of Contents

1. DoorDash: The Right to Cure Under State Law is Not Absolute

Enforcement of the new class of 'comprehensive' state commercial privacy laws is still ramping up, largely because only a handful of the laws have been in effect longer than a few months. Early signs, such as enforcement letters from the Colorado Attorney General and an announcement that the California Privacy Protection Agency (CPPA) is reviewing the connected vehicle space, suggest that more enforcement action is on the horizon. Given that enforcement is not yet in full swing, any state enforcement action will provide important insights for compliance programs. To date, California is the only state with any enforcement actions, and its recent enforcement action with DoorDash provides insights into the limitations of a right to cure as well as what constitutes a "sale" of personal data – two key issues relevant to almost all state privacy laws.

On February 21, 2024, the California Attorney General announced a settlement with food delivery platform DoorDash. The complaint alleged violations of both the California Consumer Privacy Act (CCPA) and the California Online Privacy Protection Act (CalOPPA). According to the settlement, DoorDash was participating in a "marketing co-op" without issuing proper disclosures or offering the required opt-out mechanisms to consumers. The California Attorney General indicated that participation in this marketing co-op constituted a sale under the CCPA. In this marketing co-op, DoorDash shared consumer names, addresses, and transaction histories with a third party in exchange for an opportunity to advertise its services to customers of other companies participating in the co-op. While DoorDash did not exchange consumer data for monetary value, it received the benefit of advertising to potential new customers. The types of data transfers that DoorDash allegedly engaged in as part of the marketing co-op are not as clearly "sales" under the CCPA, such as the activities at issue in the first CCPA enforcement action, which occurred against French beauty retailer Sephora.

Additionally, even though at the title of the action the CCPA provided a right for businesses to "cure" alleged violations which would end an enforcement matter, the Attorney General argued that DoorDash could not cure the alleged violations at issue. Even though DoorDash had stopped the "sales" to the marketing co-op and instructed its customers to delete the data, "personal information and inferences about DoorDash's customers had already been sold downstream to other companies and beyond the marketing co-op's members, including to a data broker that re-sold the data many times over," rendering DoorDash unable to restore its customers to the "same position they would have been if their data had never been sold." In effect, the genie was out of the bottle.

Why It's Important:

- State consumer privacy laws often define "sale" as exchanges of personal data for both monetary value and for "other valuable consideration." However, there is ambiguity as to the types of transfers and business practices that enforcers will consider to be "valuable consideration." The DoorDash enforcement action illustrates a type of other valuable consideration that may be considered a sale—participation in a marketing co-op.
- While the CCPA's right to cure has now sunset, similar statutorily guaranteed opportunities for businesses to resolve alleged violations have been included in every state commercial privacy law enacted since the CCPA. In fact, while some successive states only granted a right to cure "where possible," the CCPA provided for a broader ability to cure any violation within 30 days of a notice of alleged noncompliance. Critics of these provisions often argue that they function as a 'get out of jail free card.' However, this case demonstrates a potential inherent limitation of any right to cure based on the nature of the alleged violation. This action may inform the function of the right to cure in other state privacy laws, and shows that even the broader right to cure allowed under the CCPA was not absolute and has limitations.

2. GoodRx, BetterHelp, and Premom: Unauthorized Disclosures Of Health Information as Breaches

In 2023, the Federal Trade Commission ("FTC") filed complaints against GoodRx, BetterHelp, and Premom, all companies offering health services outside the scope of the Health Insurance Portability and Accountability Act ("HIPAA"). A key theme emerged from these enforcements: unauthorized disclosures of health data where information was passed to third-party providers for the purposes of advertising without adequate notice to individuals constitutes a breach under the FTC's Health Breach Notification Rule ("HBNR"). This pushes the understanding of "breach" beyond the traditionally understood cybersecurity hacking events.

The complaints against GoodRx and Premom represented the first and second time that the agency asserted violations of the HBNR since it was finalized in 2009. The complaints asserted that a breach occurred in violation of the HBNR when the companies disclosed PHI to third parties and ad platforms without individuals' consent and then failed to notify consumers of these "breaches." In both complaints, the FTC alleged "misrepresentation" of disclosures to third parties for advertising purposes in the companies' privacy notices and shared individuals' data without knowledge or consent. In both settlements, the companies were banned from sharing health data for advertising purposes.

In the BetterHelp case (discussed in more detail below), the FTC did not apply the HBNR. BetterHelp collected records directly from consumers and did not pull in information collected from other sources. In her concurring statement, Commissioner Wilson explained that the FTC did not assert that the company's sharing of PHI constituted a breach of the HBNR because "[t]he information BetterHelp collects from consumers and provides to therapists on its platform does not constitute a personal health record of identifiable health information under the Rule because it does not include records that 'can be drawn from multiple sources,' as required by the existing formulation of the Rule."

Why It's Important:

- The FTC's actions evince an intent to revitalize the formerly obscure HBNR and use the rule to hold companies accountable as "vendor[s] of personal health records." The FTC asserts that companies experience security breaches when they share their users' PHI with third parties and advertising platforms without those users' knowledge or consent. The FTC has sought to codify this interpretation in its April 2024 rulemaking.

3. BetterHelp and Vitagene: Health Information (and Its Sensitivity) is Contextual and Situational

The FTC's enforcement actions in 2023 and 2024 against BetterHelp and Vitagene, two health companies not covered by HIPAA, highlight the FTC's approach to the protection of health information. These cases illustrate that the meaning of sensitive "personal health information" (PHI) can be context-dependent, based on different technologies and business practices. For example, an email may become health information when input into a health-focused website. In particular, the BetterHelp and Vitagene enforcement actions demonstrated novel understandings of health information at odds with historic data practices.

In *BetterHelp*, the FTC argued that email addresses entered into the website by individuals were health information, given the context. BetterHelp is a teletherapy website and it may be assumed that individuals would input their email addresses with the intention of seeking therapy for themselves or those near to them. Relatedly, the FTC also alleged BetterHelp shared information from "intake surveys" with advertisers without express affirmative consent.

In *Vitagene*, the FTC alleged the company acted unfairly by making significant retroactive changes to its privacy policy that expanded the scope of third-party data sharing without notifying or seeking consent from customers who had given their consent under an earlier version of the

privacy policy. Vitagene develops and sells health-related products such as DNA test kits. Given the enduring quality of genetic data, the FTC argued Vitagene's retroactive changes were particularly risky for individuals. The complaint also explicitly defined information related to an individual's "health *or genetics*" as PHI, bringing within scope any genetic information that may not have previously been considered PHI.

Why It's Important:

- These and similar complaints suggest that the FTC finds the sharing of PHI—defined broadly to include personal information such as email and IP address when the collection of this information reveals that a consumer visited a healthcare website or app—for advertising purposes without consumer consent to be *de facto* unfair. These complaints also indicate that the agency is closely scrutinizing the sharing of health information for advertising purposes in general.

4. *Epic Games*: FTC Focuses on Impact of Design Choices on Teen Privacy

From 2022 through 2024, the Commission settled a series of high-profile enforcement actions focused on youth privacy and commenced rulemaking to update the Children's Online Privacy Protection (COPPA) Rule. While historically the main vehicle for protecting children's privacy online has been through COPPA, the last update to the COPPA Rule was completed in 2013. Some argue that COPPA has not kept pace as technology has evolved, and that COPPA's under-13 applicability is insufficient given the vulnerabilities and harms that teens face online. Perhaps in response to this, the FTC has begun to wield its Section 5 authority under the FTC Act to supplement protections for children online beyond COPPA's protections. One of the most significant examples of this is its enforcement action against Epic Games, which mandated policy changes for Epic Games that covered both children *and* teens.

In December 2022, the FTC announced a settlement with video game company Epic Games, the maker of Fortnite, a popular online game. The FTC alleged violations of both the Children's Online Privacy Protection Act (COPPA) and Section 5 of the FTC Act. On COPPA violations, the FTC alleged insufficient notice of data collection, use, and disclosure; failure to obtain verified parental consent; and failure to delete personal information at the request of parents. The Commission also alleged that the company acted unfairly when it publicly broadcast players' display names and configured default settings so that real-time voice and text chat features were on by default, meaning strangers could easily interact with children and teens playing the game Fortnite.

In addition to curing the COPPA violations, the stipulated order requires the company to implement privacy-by-design features such as obtaining affirmative express consent before enabling a child or teen to converse with another individual using the company's games. What was most notable about this settlement is that it created protections for both children *and teens*. Under COPPA, a child is defined as under 13, and the FTC has no statutory authority to promulgate rules extending COPPA's protections to teens. However, the FTC argued that on-by-default voice and text chat was an unfair practice under Section 5 of the FTC Act. To show that a practice is unfair, there must be an injury. In the complaint, the FTC detailed the harms that children and teens faced on Fortnite as a result of the practices, such as bullying and harassment.

In 2023 the FTC again used its Section 5 authority in a COPPA settlement with education technology provider Edmodo, alleging that Edmodo unfairly required schools and teachers to comply with the COPPA Rule on its behalf, for example by relying on schools to obtain verifiable parental consent without providing sufficient information for them to do so.

Why It's Important:

- COPPA has been on the books since 1998, but the FTC is limited to enforcing COPPA under COPPA's definition of children as those under 13. Epic Games marks the first time that the FTC recognizes teen privacy as a distinct class of individuals who need heightened protections. Until Congress amends COPPA or passes additional federal privacy laws, the Epic Games settlement may provide the clearest example of what types of harmful privacy practices the FTC will enforce, such as ensuring default settings for interacting with other users are tailored to the level of potential risk.
- This case also marks the first time that privacy by design is ordered in an FTC settlement, COPPA or not. Although the requirement here to adopt strong default privacy settings in a video game may not be broadly applicable to all organizations, it gives color to privacy by design principle. While this principle is incorporated into the GDPR, it has not yet taken hold in the same way in the United States and this provides an early example of what privacy by design means to a U.S. enforcer.

5. *Cothron v. White Castle*: Multiple Actionable Harms from Single Privacy Violations Spur Legislative Change

In February 2023, the Illinois Supreme Court ruled 4-3 in *Cothron v. White Castle* that a separate claim for a statutory damages accrues under the Illinois Biometric Information Privacy Act (BIPA) each time a private entity scans or transmits an individual's biometric identifier or information without prior informed consent. The ruling raises a critical issue that must be considered by any jurisdiction in drafting and enforcing privacy laws: when does actionable privacy harm occur? The ruling also provided an impetus for the Illinois legislature to pass legislation narrowing the accrual of damages under BIPA's private right of action.

Under the Illinois Biometric Information Act (BIPA), a private entity may not collect or disclose biometric information without prior informed consent. In *Cothron v. White Castle*, the company implemented an employee biometric authentication system in 2008 (the same year BIPA became effective) to secure employee pay stubs and computers, but did not seek employees' consent until 2018. The key question before the Illinois Supreme Court was when Plaintiff's BIPA claim accrued or when the clock started for statute of limitations—if her claim accrued in 2008 when White Castle first obtained her fingerprint, her claim would be untimely, but if it accrued every time her fingerprint was scanned, her claim would survive. White Castle estimated their damages could exceed $17 billion, given that the case was a class action lawsuit on behalf of 9,500 employees over ten years.

The Illinois Supreme Court found that her claim was timely and a violation occurred per scan. The court emphasized "[e]ach time an employee scans her fingerprint to access the system, the system must capture her biometric information and compare that newly captured information to the original scan." The Court also rejected White Castle's argument that a claim accrues when an individual loses their "right to control" biometric information, noting that their decision in *Rosenbach v. Six Flags* recognized that a person is "aggrieved" when there is a statutory violation, and BIPA is not predicated on an "injury" or loss of control of privacy. In fact, the Court was sympathetic to concerns regarding damages and the potential for multiple statutory violations to occur and explicitly stated, "We respectfully suggest that the legislature review these policy concerns and make clear its intent regarding the assessment of damages under the Act. "

In contrast, three dissenting justices argued that subsequent authentication scans did not constitute additional collections or disclosures. These justices reasoned that with subsequent scans, the fingerprint is not being obtained, but rather being compared to the fingerprint that the employer already has. The dissenters also disagreed with the majority's legislative analysis, explaining that the "precise harm" the legislature was addressing was an individual's loss of the right to maintain biometric privacy, which in this case was lost upon initial enrollment. The

dissenting opinion stated, "Once that entity has the fingerprint, there is no additional loss of control, loss of privacy, or loss of secrecy from subsequent scans of the same finger. This is true whether the same finger is scanned a few times or one million times. The individual loses control over it only once."

Why It's Important:

- Jurisdictions enforcing privacy laws will need to determine when and how damages accrue in cases involving ongoing collection, use, or disclosure of personal information of multiple individuals that may be in violation of a law. In response to *Cothron v. White Castle,* in 2024, the Illinois legislature amended BIPA to clarify that a private entity that more than once collects or discloses a person's biometric identifier or biometric information from the same person in violation of the Act has committed a single violation for which the aggrieved person is entitled to, at most, one recovery.
- BIPA is one of the few privacy laws to contain a private right of action. Given the potential for repeat statutory violations adding up to millions of dollars in damages, it is often pointed to as an example of why privacy laws should not have any privacy enforcement. However, the Illinois legislature's clarification on when a violation occurs and what type of recovery is available may increase awareness that a private right of action is not an all-or-nothing proposition, and encourage policymakers to consider different ways that such an enforcement mechanism can be crafted.

6. *Kochava*: How Location Data Sales Impact Privacy Interests

The Federal Trade Commission's (FTC) ongoing lawsuit against Kochava provides insight into how courts and regulators are grappling with the privacy harms raised by collecting and disclosing sensitive location data. The lawsuit alleges that Kochava's sale of precise geolocation data that is linked or linkable with particular individuals and from which inferences about individuals' visits to sensitive locations can be drawn is an unfair trade practice in violation of Section 5 of the FTC Act. This case also addresses when location data collection and disclosure constitutes an injury under Section 5 of the FTC Act. Depending on the outcome of the case, it may determine whether an invasion of privacy is itself an "injury" under Section 5, rather than needing to prove the privacy violation led to harm, setting a significant precedent and influencing how other policymakers and courts consider the issue.

In August 2022, the FTC filed its initial complaint against data broker Kochava, seeking to permanently enjoin Kochava from selling precise location data without implementing privacy safeguards. The timing of this lawsuit reflects the FTC's concern about reproductive health

privacy. Reproductive health privacy has been an enforcement priority for the FTC, partly because of the Biden Administration's urging after the decision in *Dobbs v. Jackson Women's Health Organization*.

In May 2023, the United States District for the District of Idaho ("the District Court") dismissed the FTC's complaint with leave to amend. The District Court rejected Kochava's arguments that an act or practice must violate some other existing law or public policy or be "immoral, unethical, oppressive, or unscrupulous" to be unfair under Section 5(a) but found that the FTC had not adequately alleged a likelihood of substantial consumer injury, rejecting both the FTC's theories:

- **Secondary Harms:** First, the FTC alleged that by selling location data, Kochava could enable third parties to generate inferences based on individuals' movements to and from sensitive locations and then "inflict secondary harms including 'stigma, discrimination, physical violation, [and] emotional distress.'" The District Court found this theory plausible, but ultimately found that the FTC did not adequately allege that consumers *are* suffering or *are likely to suffer* such secondary harms. According to the court, such secondary harms must be more than "theoretically possible" to establish substantial injury under Section 5—the FTC must allege that there is a "'significant risk' that third parties will identify and harm consumers."

- **Invasion of Privacy:** Second, the District Court found that invasion of privacy alone can constitute substantial injury, but that the alleged privacy harm in this case (disclosure of location data) was not severe enough to do so. Although "[d]isclosing where a person has been every fifteen-minutes over a seven-day period could undoubtedly reveal information that the person would consider private," the District Court held that location data becomes sensitive only when individuals make inferences based upon it, and that these inferences are often unreliable. The Court also noted that the FTC did not "even generally indicate[ ]" how many individuals were affected by this, which impacts the substantiality of the injury.

The FTC attempted to overcome both of these objections in a June 2023 amended complaint by arguing that beyond there being a mere risk that third parties might link location data sold by Kochava to particular individuals, Kochava actively markets its ability to match the data it sells, including location data, with particular individuals. Likewise, the FTC attempted to rebut the suggestion that data buyers must take any additional steps to glean sensitive information about individuals from the data they purchase from Kochava, noting that Kochava groups the data it sells into "audience segments," including segments organized by sensitive characteristics.

Kochava moved to dismiss the amended complaint, but, in February 2024, the Court denied the motion, finding that the FTC's theories of increased risk of secondary harms and invasion of privacy alleged facts sufficient to proceed. Key to this was the inclusion of additional detail regarding Kochava's products and business practices. Regarding secondary harms, the FTC alleged that "Kochava's customers can target consumers who have visited sensitive locations," and that the risk of such targeting was exacerbated by a lack of control regarding who can access that data, how they can use it, and that Kochava makes it easy to identify individuals by linking MAIDs and geolocation data. The Court found persuasive the FTC's real-world examples of secondary harms to individuals resulting from the disclosure of location data and app-use data. With respect to invasion of privacy, the Court found that selling "comprehensive, aggregated collections of raw and synthesized data" is a violation of privacy "substantial both in quantity and quality," plausibly constituting substantial injury. Looking at the products Kochava offers, including an "App Graph" that shows an individual's activities within a particular app, the Court found that these inferences are more reliable than those drawn solely from geolocation data. As of June 2024, this litigation is ongoing, though it was reported that the parties might be open to settling.

Why It's Important:

- The District Court's response to this amended pleading, and, in particular, the Court's receptivity to the FTC's characterization of the privacy risks posed by Kochava's data collection practices, will have important implications both for individual privacy rights as well as for businesses that collect, buy, sell, or use individual location data. In particular, this could provide a basis for litigation where the collection, use, or disclosure of individual location data facilitates secondary harms or the initial collection and use of data is so voluminous and granular as to be a violation of privacy itself.
- It is a widely embraced privacy principle that data about people's precise geolocation, especially when combined into datasets that track individuals' movements over time, is particularly sensitive. Such data is so sensitive both because it can reveal details about an individual's visits to sensitive locations, including health facilities, places of worship, and public demonstrations, as well as because it can paint a very detailed picture of an individual's activities over time, indicating where individuals live, work, and habitually spend their leisure time.
- While *Kochava* faces ongoing litigation, the FTC has advanced this theory of unfair sensitive data collection and sharing in other enforcement actions, reaching settlements with X-Mode and InMarket in January 2024 regarding the companies' collection and sale of sensitive location data.

Appendix: Case Materials

1. DoorDash: The Right to Cure is Not Absolute

DoorDash

- Complaint: People v. DoorDash, Inc., No. CGC-24-612520 (Super. Ct. Cal. Feb. 21, 2024), https://oag.ca.gov/system/files/attachments/press-docs/DoorDash%20Complaint.pdf.
- Settlement: People v. DoorDash, Inc., No. CGC-24-612520 (Super. Ct. Cal. Feb. 22, 2024), https://oag.ca.gov/system/files/attachments/press-docs/DoorDash%20Stip%20Judgment%20.pdf.

Sephora

- Complaint: People v. Sephora USA, Inc., No. CGC-22-601380 (Super. Ct. Cal. Aug. 23, 2022), https://oag.ca.gov/system/files/attachments/press-docs/Complaint%20%288-23-22%20FINAL%29.pdf.
- Settlement: People v. Sephora USA, Inc., No. CGC-22-601380 (Super. Ct. Cal. Aug. 24, 2022), https://oag.ca.gov/system/files/attachments/press-docs/Filed%20Judgment.pdf.pdf

2. GoodRx, BetterHelp, Premom: Unauthorized Disclosures of Health Information as Breaches

GoodRX

- Complaint: United States v. GoodRX Holdings, Inc., No. 3:23-cv-460 (N.D. Cal. Feb. 1, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/goodrx_complaint_for_permanent_injunction_civil_penalties_and_other_relief.pdf.
- Stipulated order: United States v. GoodRX Holdings, Inc., No. 3:23-cv-460 (N.D. Cal. Feb. 1, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/goodrx_stipulated_order_for_permanent_injunction_civil_penalty_judgment_and_other_relief.pdf.

Premom

- Complaint: United States v. Easy Healthcare Corp., No. 1:23-cv-3107 (N.D. Ill. May 17, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2023186easyhealthcarecomplaint.pdf.
- Stipulated order: United States v. Easy Healthcare Corp., No. 1:23-cv-3107 (N.D. Ill. Jun. 22, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2023.06.22_easy_healthcare_signed_order_2023.pdf

BetterHelp

- Complaint: BetterHelp, Inc., F.T.C. No. C-4796 (Jul. 7, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2023169betterhelpcomplaintfinal.pdf
- Decision and order: BetterHelp, Inc., F.T.C. No. C-4796 (Jul. 7, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2023169betterhelpfinalorder.pdf

3. Betterhelp and Vitagene: Health Information (and Its Sensitivity) is Contextual and Situational

Vitagene

- Complaint: 1Health.IO Inc., F.T.C. No. C-4798 (Sep. 6, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/1Health-Complaint.pdf.
- Decision and order: 1Health.IO Inc., F.T.C. No. C-4798 (Sep. 6, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/1Health-DecisionandOrder.pdf.

4. Epic Games: FTC Focuses on Impact of Design Choices on Teen Privacy

Epic Games

- Complaint: United States v. Epic Games, Inc., No. 5:22-CV-00518 (E.D.N.C. Dec. 19, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2223087EpicGamesComplaint.pdf.

- Stipulated order: United States v. Epic Games, Inc., No. 5:22-CV-00518 (E.D.N.C. Feb. 7, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/1923203epicgamesfedctorder.pdf.

Edmodo

- Complaint: United States v. Edmodo, LLC, No. 23-cv-2495-TSH (N.D. Cal. May 22, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/edmodocomplaintfiled.pdf.
- Stipulated order: United States v. Edmodo, LLC, No. 23-cv-2495-TSH (N.D. Cal. Jun. 27, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/Edmodo-Dkt15%28Order%20Signed%20by%20the%20Court%29.pdf.

5. Cothron v. White Castle: Multiple Actionable Harms from Single Privacy Violations Spur Legislative Change

Cothron v. White Castle

- Illinois Supreme Court Judgement: Cothron v. White Castle Sys., Inc., 2023 IL 128004, https://ilcourtsaudio.blob.core.windows.net/antilles-resources/resources/e304b011-82d9-4832-9cae-d8205749a2ec/Cothron%20v.%20White%20Castle%20System,%20Inc.,%202023%20IL%20128004.pdf.
- District Court Decision: Cothron v. White Castle Sys., Inc., 477 F. Supp. 3d 723, 732 (N.D. Ill. 2020)

Rosenbach v. Six Flags

- Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186, https://www.illinoiscourts.gov/Resources/f71510f1-fb2a-43d8-ba14-292c8009dfd9/123186.pdf.

6. FTC v. Kochava: How Location Data Sales Impact Privacy Interests

Kochava

- Complaint: Fed. Trade Comm'n v. Kochava Inc., No. 22-cv-00377 (D. Idaho Aug. 29, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf.
- Memorandum and order on first motion to dismiss: Fed. Trade Comm'n v. Kochava Inc., No. 22-cv-00377 (D. Idaho May 4, 2023), https://cases.justia.com/federal/district-courts/idaho/iddce/2:2022cv00377/50683/24/0.pdf.
- Amended complaint: Fed. Trade Comm'n v. Kochava Inc., No. 22-cv-00377 (D. Idaho Jun. 5, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/26AmendedComplaint%28unsealed%29.pdf
- Memorandum and order on second motion to dismiss: Fed. Trade Comm'n v. Kochava Inc., No. 22-cv-00377 (D. Idaho Feb. 3, 2024), https://epic.org/wp-content/uploads/2024/02/FTC-v-Kochava-22-377-opinion-mtd-020324.pdf.

X-Mode

- Complaint: X-Mode Social, Inc., F.T.C. No. C-4802 (Apr. 11, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialComplaint.pdf.
- Decision and order: X-Mode Social, Inc., F.T.C. No. C-4802 (Apr. 11, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf.

InMarket

- Complaint: InMarket Media, LLC, F.T.C. No. C-4803 (Apr. 29, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/InMarketMedia-Complaint.pdf
- Decision and order: InMarket Media, LLC, F.T.C. No. C-4803 (Apr. 29, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/InMarketMedia-DecisionandOrder.pdf.

1350 Eye Street NW Suite 350
Washington, DC 20005

info@fpf.org

FPF.org