Procopio

Privacy Litigation & Enforcement Update

An update on recent privacy litigation and enforcement and practical takeaways to protect your business

April 30, 2025

Elaine F. Harwell, CIPP/US, CIPM
Partner and Privacy Officer
Elaine.Harwell@Procopio.com
619.906.5780

Overview of Discussion

- Online Technologies and Tracking (CIPA, etc.)
- Recent Regulator Activity and Enforcement Trends
- Litigation Trends in Artificial Intelligence (AI)
- Data Breach Litigation Update
- Other Notable Litigation Updates
- Questions?

Online Technologies and Tracking: Background

- Last few years courts have seen influx of putative class action lawsuits targeting businesses with websites that utilize technology to track users' website interactions
- Many lawsuits filed in California are under California Invasion of Privacy Act (CIPA), Cal. Penal Code sections 630 – 638.55
- Section 631 of CIPA, protects against:
  - intentional wiretapping of any telegraph or telephone wire, line or cable;
  - willfully and without the consent of all parties attempting to learn the contents of a communication in transit; and
  - attempting to use or communicate information obtained as a result of engaging in either activity

Online Technologies and Tracking: Types of Tech

- Types of technologies at issue:
  - Chatbots
  - Session Replay: mouse movements, clicks, typing, browsing
  - Cookies/Pixels: MetaPixel, Google Pixel, Google Analytics
  - Trap & Trace or Pen Register claims
  - Privacy of video-viewing behavior: Video Privacy Protection Act (VPPA)
  - Search bar claims

Online Technologies and Tracking: Cases

- State cases sustaining demurrers:
  - Sanchez v. Cars.com (LA Superior Court): Court dismissed case without leave to amend, ruling that website tracking technologies capturing IP address do not fall under CIPA's trap & trace and "pen register" restrictions
  - Aviles v. LiveRamp, Inc. (LA Superior Court, Case No. 24STCV19869: Trap and trace case – demurrer granted with leave to amend citing that more specificity needed in pleading privacy allegations
  - Rebeka Rodriguez v. Fountain9, Inc. (Cal. Sup. 24STCV04504, July 9, 2024): A website user cannot sustain a CIPA claim without demonstrating a concrete injury resulting from a beacon's collection of their IP address
- Federal trap & trace cases making it past motion to dismiss:
  - Moody v. C2 Education Systems, No. 2:24-CV-04249-RGK-SK, 2024 WL 3561367 (C.D. Cal. July 25, 2024);
  - Shah v. Fandom, Inc., No. 24-CV-01062-RFL, 2024 WL 4539577 (N.D. Cal. Oct. 21, 2024);
  - Mirmalek v. Los Angeles Times Commc'ns LLC, No. 24-CV-01797-CRB, 2024 WL 5102709 (N.D. Cal. Dec. 12, 2024).

Online Technologies and Tracking: Cases (cont'd)

- Session Replay cases:
  - Torres v. Prudential Financial, Inc., Assurance IQ, LLC, Case No. 22-cv-7475 (N.D. CA), session replay case where court granted class certification
  - Jones v. Bloomingdales.com, LLC, No. 23-3304, 2024 WL 5205528 (8th Cir. Dec. 24, 2024), affirmed dismissal for lack of standing, explaining that it failed to see how defendant's use of session replay technology invaded plaintiff's privacy where information voluntarily conveyed
- Few appellate court decisions interpreting viability of CIPA claims
- Development of cases outside of California – more favorable to defense?
  - Gabrielli v. Insider, Inc., No. 1:2024cv01566 (SDNY), trap and trace case alleging violations of CIPA dismissed for lack of Article III standing, allegations involved collection of IP addresses only
- Ninth Circuit cases, session replay standing cases:
  - Popa v. PSP Group, LLC, No. 24-14
  - Daghaly v. Bloomingdales, No. 23-4122, dismissal of complaint for lack of personal jurisdiction

Online Technologies and Tracking: Mitigation

- **Review privacy policies** to ensure transparency regarding data collection practices and third-party data sharing
- **Audit websites** to understand use of tracking technologies
- **Consider** whether consent is required
- **Evaluate** what jurisdictions the business operates in and the impact of applicable laws
- **Stay up-to-date** on case law developments and regulatory changes that may impact data collection on websites
  - What impact do these things have on CIPA litigation?

Recent Regulator Activity & Enforcement: Honda Decision

- The California Privacy Protection Agency issued Order of Decision against American Honda Motor Co.
- Agency claimed Honda violated California Consumer Privacy Act (CCPA) by:
  - requiring California consumers to provide excessive personal information to exercise their rights, including the opt-out of sale/sharing right;
  - using an online privacy rights management platform that did not offer consumers a "symmetry of choice" in exercising their privacy choices;
  - making it difficult for Californians to authorize other individuals or organizations (known as "authorized agents") to exercise their privacy right; and
  - sharing consumers' personal information with ad tech companies without producing contracts that contain the necessary terms to protect privacy.
- Agency imposed $632,500 fine on Honda calculated based on the number of consumers whose right were alleged to have been implicated by Honda's practices

Recent Regulator Activity & Enforcement: Key points of Honda Decision

- Requests to opt out of sale/share and requests to limit are rights that consumers should be able to exercise “without undue burden”
  - No need for businesses to “verify” requests to opt out
  - Requests to delete and to know are verifiable requests, but businesses must still only ask for the data points needed to identify the consumer and facilitate the request
- Authorized agents must be treated the same as consumers
  - Nonverifiable requests (to opt out) should not be confirmed directly with the consumer
  - Businesses can still confirm directly with a consumer for verifiable requests
- Cookie Management Tools should be vetted for symmetry and compliant language
  - DO NOT RELY UPON THE DEFAULT SETTINGS OF VENDORS
  - Watch out for confusing interfaces, difficult to understand language, and more clicks to opt out than in
- Verify contracts with third party advertising companies (and others where data is shared) comply

Recent Regulator Activity & Enforcement:
Takeaways from Honda Decision

- Review your Rights Management Platforms
  - Do your forms require more information that required to identify individuals?
  - Have you considered what type of right the consumer is attempting to exercise and whether that impacts your response?
- Review your Consumer Request and Consent Mechanism
  - "Accept all" or "Decline all"?
  - Does your website recognize the Global Privacy Control (GPC) signal?
- Audit your vendor contracts
  - The CCPA requires that any covered business disclosing personal information o a third party, service provider, or contractor enter into contracts that have specific requirements set forth in CCPA Regulations section 7051 and 7053
  - Advertising vendors should be considered in this mix

Artificial Intelligence

- AI use has become pervasive
- Privacy risks, include:
  - Unauthorized use of personal data to train AI models
  - AI systems affected by bias in its processing or outputting
  - Deceptive marketing of AI products or services, such as exaggerations about capabilities or failure to disclose risks
- Where use of AI already matters
  - Initial decisions out of Europe indicate that users of an AI product may be primarily liable to their contractual partners, even if they did not develop the AI product themselves
  - Use of data to train AI models is evidence that a third party is a distinct eavesdropper, and not a “tape recorder” under the CIPA

Artificial Intelligence

- AI issues in future litigation
  - Data breaches are almost inevitable
    - Once data is in a model, there's essentially no way to take it out
    - Controls needed to limit employee abuse, not to mention outside access
  - Fights over injunctive relief
    - Algorithmic disgorgement
  - Bias in AI decisionmaking/outputs
  - Consent, not just to use data currently being collected, but to use data already collected for different purposes

Data Breach Litigation Update

- Data breach litigation continues to rise, many MDLs
- Many cases still revolve around questions of standing, and whether a plaintiff has sufficiently alleged “actual or imminent” harm fairly traceable to defendant’s conduct
- Plaintiffs often rely on an increased risk of identity theft or misuse of their data, rather than actual identity theft
- Other claims involve resulting mitigation costs, loss of value in personally identifiable information, benefit of the bargain losses, invasion of privacy, emotional distress
- Continuing litigation regarding privilege over forensic reports
- Case examples:
  - In re MOVEit Data Security Breach Litigation, 23-3083 (D. Mass.) finding standing where few plaintiffs experienced actual identity theft
  - In Re San Francisco 49ers Data Breach Litigation, Case No. 3:22-cv-051 (N.D. CA), arguments related to plaintiffs’ failure to comply with CCPA’s notice-and-cure provisions

Other Notable Case Law Developments

- CCPA claims permitted despite no data breach:
  - M.G. v. Therapymatch, Inc., No. 23-CV-04422-AMO, 2024 WL 4219992, at *7 (N.D. Cal. Sept. 16, 2024), recognizing that courts have let CCPA claims survive a motion to dismiss where a plaintiff alleges that defendants disclosed plaintiff's personal information without consent due to the business's failure to maintain reasonable security practices
  - In re BetterHelp, Inc. Data Disclosure Cases, No. 23-CV-01033-RS, 2024 WL 3416511, at *2 (N.D. Cal. July 15, 2024)
- Social Media addiction cases:
  - In re: Social Media Adolescent Addiction/Personal Injury Products Liability Litigation (MDL No. 3047), Northern District of CA
  - Moody v. Netchoice, LLC, 144 S. Ct. 2383 (July 1, 2024), SCOTUS finds first amendment protections for social media companies when publishing third party content, including when they exercise discretion to promote, demote, block, or assign labels to third-party posts.
- Geolocation tracking lawsuits:
  - Google, Kochava, Weather Channel
  - Selling and collecting location data without consent that can be used to identify people visiting sensitive locations, which could lead to discrimination, stalking, and violence
- Washington's My Health My Data Act
  - First class action complaint recently filed: Maxwell v. Amazon

Thank you!

Questions?

Elaine F. Harwell, CIPP/US, CIPM
Partner and Privacy Officer
elaine.harwell@procopio.com
619.906.5780

Procopio