Digital Privacy Compliance: 2023 Trends and Risks

Presented to DEG: The Digital Entertainment Group

Jennifer Mitchell, Partner, BakerHostetler
Field Garthwaite, CEO, Co-Founder, IRIS.TV

July 19, 2023
Agenda

• Ad Tech and Tracking Technologies
• U.S. State Privacy Laws
• Litigation Risks
• Key Take-aways
Ad Tech and Tracking Technologies
Cookies

- Small text files stored on a visitor’s web browser
- Originally for non-advertising uses (logging in, shopping cart)
- Store and share data with the domain that sets the cookie to recall visitor preferences and choices

Tags, Pixels, Web Beacons

- Allows the visitor’s browser to communicate with another domain
- Often used for analytics, reporting, etc. within the digital ad ecosystem

SDKs

- Software Development Kits (“SDKs”) help developers build apps to work on mobile (where cookies don’t work)
- Can be used for mobile advertising, measurement, and verification
Ad Tech Prevalence

For illustrative purposes only.
Hot Topics in Technology

• Meta Pixel
  • Analytics tool that helps to measure effectiveness of ad campaigns

• Chat Bots
  • Software applications that simulate human conversations, particularly used for customer service support

• Session Replay
  • Session replay is a common analytics tool that captures certain website activity data—such as mouse movements, clicks, and page visits— that may be analyzed to understand and enhance customers’ online experiences
Ad Tech and Privacy Tension

- Evolving U.S. state law
- Increased scrutiny and regulation around behavioral/targeted advertising (CA AG, HHS OCR, FTC)
- Litigation risks
  - VPPA
  - Wiretapping Claims
Sources of Privacy Obligations

- Laws and Regulations
- Industry Standards
- Internal and External Policies
- Contracts
Privacy Laws Around the World

Source – DataGuidance (https://www.dataguidance.com)
The Race for U.S. State Privacy Laws

US State Privacy Legislation Tracker 2023

STATUTE/BILL IN LEGISLATIVE PROCESS
- Introduced
- In committee
- In cross chamber
- In cross committee
- Passed
- Signed
- Inactive bills
- No comprehensive bills introduced

Last updated: 7/7/2023
U.S. State Privacy Laws- New for 2023

The application of these new laws to a business is fact-dependent and varying exemptions may apply.

California Privacy Rights Act (CPRA) • January 1, 2023
Virginia Consumer Data Protection Act (VCDPA) • January 1, 2023
Colorado Privacy Act (CPA) • July 1, 2023
Connecticut Privacy Act (CTPA) • July 1, 2023
Utah Consumer Privacy Act (UCPA) • December 31, 2023

Common Features

- Consumer Rights
- Sensitive Personal Information Protections
- Processing Limitations
- Contractual Obligations on Vendors
- Risk Assessments
- Notice & Transparency Requirements
The California Consumer Privacy Act of 2018 (CCPA) has been in effect since January 1, 2020.

The California Privacy Rights Act (CPRA) amends the CCPA and most of the new provisions came into effect January 1, 2023.

California privacy law protects the personal information of California consumers.

The (new) California Privacy Protection Agency (CPPA) and California Attorney General have enforcement powers.
CCPA- Right to Opt-Out of Sales/ Shares

**Sell**
- “…selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.”

**Share**
- “…sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.”
What Does This Mean for Businesses?

- Right to opt-out of the sale or sharing with third parties
- Businesses must include language in privacy policy and “Do Not Sell or Share” link in footer of website
- Must implement Global Privacy Control
- All of this will result in some impact to marketing teams
CA AG CCPA Enforcement- Sephora

- After conducting an enforcement sweep of online retailers, the CA AG alleged that “Sephora failed to disclose to consumers that it was selling their personal information, that it failed to process user requests to opt out of sale via user-enabled global privacy controls in violation of the CCPA, and that it did not cure these violations within the 30-day period currently allowed by the CCPA.”

- Sephora's arrangement with its vendors allegedly constituted a “sale” of consumer information under the CCPA, and it triggered requirements, such as telling consumers that they are selling their information and allowing consumers to opt-out of the sale of their information.

- According to the CA AG, Sephora did neither.

- $1.2 million in penalties and injunctive terms.
CA AG Latest Enforcement Sweep – Mobile Apps

• January 27, 2023, AG announcement of “investigative sweep” of mobile apps
• Alleged failures to provide a mechanism or honor requests to opt out of “sales”
• Expanded focus to mobile apps
Deceptive Practices in Targeted Advertising

• Easy Healthcare
  – Sharing without consent
  – Promises that all data collected was non-identifiable

• BetterHelp, Inc.
  – Promises to use data collected only for counseling services
  – Displaying privacy misrepresentations
  – Failing to limit third-party secondary uses

• GoodRx Holdings, Inc.
  – Promises to never share personal information with advertisers
Litigation Risks
Tracking Technology Litigation

- Video Protection Privacy Act ("VPPA")
- Wiretapping and state privacy laws
- Breach of contract
- Breach of negligence and fiduciary duty
- State consumer protection laws
What is the VPPA?

- Congress passed the VPPA (18 U.S.C. § 2710(b)) in 1998 to address video rental privacy concerns after Blockbuster disclosed a U.S. Supreme Court nominee’s video rental history to a news outlet.
- In 2012, the VPPA was updated to cover digital streaming and on-demand services.
- The VPPA prohibits any videotape service provider (VTSP) from knowingly disclosing, to any person, personally identifiable information concerning the VTSP’s consumer.
VPPA’s Evolution with Technology

• Recent lawsuits allege that websites running the Meta Pixel are violating the VPPA by sharing information about visitors' video viewing habits and history with Meta

• Complaints allege that websites use the pixel to share PII with Facebook about viewership

• At least 70 VPPA actions filed against operators of websites that offer online and common third party analytics tools
VPPA Defenses

Key defenses are still being litigated in the VPPA context, including:

- The defendant is not a VTSP;
- The disclosure is not PI;
- The defendant is unaware of what information the website tracker is collecting;
- For providers of free video content, the plaintiff is not a “renter, purchaser, or subscriber of goods or services” from the VTSP; and
- The defendant provided the plaintiff informed consent in a distinct and separate form.

And First Amendment challenges.
VPPA Risks

- Companies that are found to be liable under the VPPA are potentially subject to actual or liquidated damages of at least $2,500 per affected consumer, punitive damages, attorneys' fees and costs, and other equitable relief.

- The continued increase in VPPA claims is anticipated given the lack of clear consensus among the courts.
What is CIPA?

• In 1967, CIPA was enacted to protect the privacy of Californians from newly developed “devices and techniques” used for eavesdropping.

• The current wave of CIPA litigation predominantly arises under two sections:
  • §631: Makes punishable “[a]ny person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, ... or who willfully and without the consent of all parties to the communication ... reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit ..., or is being sent from, or received at any place within this state ....”
  • §632.7. Added to CIPA in 1992 to protect cellular phone calls in a similar way that landline calls were already protected by CIPA.

• Violation occurs when a party who “without the consent of all parties to a communication, intercepts or receives and intentionally records ... a communication” involving a “cellular radio telephone” or a “cordless telephone.”

• Statutory Damages: “the greater of $5,000 per violation or three times the amount of actual damages, if any, sustained by the plaintiff.”
Wiretap Act Claims- Chat Bots & Session Replay

• Nearly 100 CIPA chat cases filed since July 2022.

• Targets entities that operates a website with a “chat” feature operated by a third-party that does not require affirmative consent and acknowledgment of the third-party’s involvement in the communication.

• Evaluate whether “contents” of communications are at issue, and whether the statute requires two or one party consent
Key Take-aways
Take-aways

• Know what tracking technologies you are using, how and why.
  • Run cookie scans.
  • Understand how pixels are configured.
  • Establish governance process.
  • Talk with Legal about implications.

• Consider risk/reward, especially for higher risk technologies.
• Review website privacy notices and terms of use.
• Consider methods to obtain opt-in/opt-outs from consumers.