May 9, 2024

Litigation Trends and Risk Management: VPPA, CIPA, and Other Class Claims

Carter Simpson,
Partner
Paul Hastings LLP

Matt Gardner,
Senior Privacy Counsel
Ro

Privacy+ Security Forum

Speakers

Carter Simpson

Partner
Paul Hastings

Matt Gardner

Senior Privacy Counsel
Ro

The California Invasion of Privacy Act, Cal. Penal Code § 630

Privacy+ Security Forum

Cal. Penal Code §§ 630–638

Privacy+ Security Forum

California Penal Code Section 631: Wiretapping

- Forbids anyone from illegally wiretapping a conversation. The law specifically prohibits the following:
- Using a machine to connect to a phone line.
- Trying to read a phone message without the consent of all the parties participating in the conversation.
- Using any information obtained through a wiretapped conversation.
- Conspiring with another person to commit a wiretapping offense.

California is a two-party consent state.

Cal. Penal Code §§ 630–638

Privacy+ Security Forum

California Penal Code Section 632: Eavesdropping

- The statute defines “eavesdropping” as the use of a hidden electronic device to listen to a confidential communication.

- The types of electronic devices that are often used to illegally eavesdrop include telephones, video cameras, surveillance cameras, microphones, and computers. If the device was concealed from one of the parties, it may constitute a violation of California’s eavesdropping laws.

- Many times, a wiretapping case also involves eavesdropping offenses where the offending party both taps a phone line and listens in on the conversation. The main difference between the two is that eavesdropping does not necessarily involve the tapping of a phone line.

Cal. Penal Code §§ 630–638

Privacy+ Security Forum

California Penal Code Section 638.50-51: Pen Register/Trap and Trace

- "Pen register" a device or process that records or decodes dialing, routing, addressing, or signaling information … but not the contents of a communication.

- "Trap and trace device" a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication.

The California Invasion of Privacy Act: Two Theories and Recent Updates

Privacy+ Security Forum

CIPA Claims - Wiretap & Pen Register

Privacy+ Security Forum

Wiretap

- Interception of communication.
- Two-party consent requirement.
  - CA is a two-party state.
- Intentional eavesdropping.
- Plaintiffs firms:
  - Not just applicable to phone lines -> internet.
  - Embedded pixel code, web session replay, or chatbot = intentional interception.
- Plaintiffs firms are still using this theory
- Courts are generally dismissing these based on:
  - The “party exception” (parties that are the intended recipients are not eavesdroppers).
  - A finding that the information shared is not content of a website visit, in transit or intercepted.
  - A conclusion that CIPA does not apply to web-based communications.

CIPA Claims - Wiretap & Pen Register

Privacy+ Security Forum

Pen Register

- Device or process that records or decodes dialing, routing, addressing, or signaling information transmitted, but not the contents of a communication.
- Prohibited without a court order.
- Greenley v. Kochava, No. 22-CV-01327-BAS-AHG, 2023 WL 4833466 (S.D. Cal. July 27, 2023):
- Claimed that defendant's SDKs secretly collected multiple types of data, which defendant in turn used to "fingerprint" each user, and to sell the resulting user profiles to third parties.
- The court rejected defendant's motion to dismiss given the "vague and inclusive" statutory definition, a pen register might include software "that identifies consumers, gathers data, and correlates that data through unique fingerprinting."

The Video Privacy Protection Act, 18 U.S.C. § 2710

Privacy+ Security Forum

18 U.S.C. § 2710(b)(1)

A [1] video tape service provider who [2] knowingly discloses, to any person, [3] personally identifiable information concerning any [4] consumer of such provider, shall be liable to the aggrieved person for the relief provided in subsection (d).

- § 2710(c)(2) – allows for actual damages but not less than liquidated damages of $2,500; punitive damages; and reasonable attorneys' fees and litigation costs
- § 2710(c)(3) – two-year statute of limitations
- § 2710(b)(2) – list of statutory exceptions

Key Terms, Part 1

Privacy+ Security Forum

Video Tape Service Provider

- "any person, **engaged in the business**, in or affecting interstate or foreign commerce, of rental, sale, or **delivery** of **prerecorded** video cassette tapes or similar audio visual materials"
- Business should be "centered, tailored, or focused" on providing video content
- Generally excludes businesses that feature videos only for "brand awareness" or that are peripheral to a Defendant's business

Personally Identifiable Information

- "includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider"
- Generally excluded: device ID, IP address, browser/device/operating system number, webpage name unless it reveals video content
- Generally included: Facebook ID, GPS coordinates, combinations of excluded info

Key Terms, Part 2

Privacy+ Security Forum

Knowing Disclosure

- Conscious transmission of PII; deliberate installation of tracking technology

Prerecorded Audio Visual Material

- Excludes live streaming videos
- Not limited to materials of a certain content, medium, or duration

Consumer

- "any renter, purchaser, or **subscriber** of **goods or services** from a video tape service provider"
- Courts divided as to whether person must be a consumer of *video* goods and services, or of goods and services generally.
- Several Circuits consider six *Ellis* factors: payment, registration, commitment, delivery, expressed association, and/or access to restricted content

Other Common Defenses

Privacy+ Security Forum

Informed and Written Consent, § 2710(b)(2)(B)

- Must be in a form distinct and separate from any form setting forth other legal or financial obligations;
- Must be given (i) at the time the disclosure is sought or (ii) in advance for a set prior not to exceed two years or until withdrawn; and
- Must provide a clear and conspicuous opportunity for consumer to withdraw on a case-by-case basis or from all ongoing disclosures.

Ordinary Course of Business, § 2710(b)(2)(E)

- "only debt collection activities, order fulfillment, request processing, and the transfer of ownership"
- Legislative history reflects a more expansive application

First Amendment

- Data exchanges as commercial speech

Mass Arbitration

Privacy+ Security Forum

Background

How did we get here?

- FAA creates presumption in favor of enforcing arbitration agreements. 9 U.S.C. § 2.
- Supreme Court holds in *AT&T Mobility v. Concepcion* that FAA preempts state laws requiring the availability of a class-wide enforcement mechanism.
- To mirror the provision at issue in *Conception*, many businesses revised arbitration provisions to require business to pay all or most arbitration costs.

What are the defining characteristics?

- Hundreds or thousands of small-value arbitration claims, for which the initial arbitral fees far exceed the cost of defense.
- Most common in employment law and consumer/privacy law.
- Typically employ online advertising and recruiting efforts and social media to identify claimants.

Avoidance Strategies

Privacy+ Security Forum

- Formalize demand intake and investigation procedures;
- Review and revise arbitration provisions:
  - Incorporate mass arbitration rules of a credible arbitral services provider.
    AAA Mass Arbitration Supplementary Rules
  - Implement mandatory pre-arbitration informal dispute resolution process that requires a Notice of Dispute and an individualized teleconference with claimant.
  - Cost-shifting only under a predetermined number of claimants.
  - Consider expanding list of claims exempt from arbitration provision.
  - Implement batching procedure and periodic mandatory mediations.
  - Fee- and cost-shifting for harassing or patently frivolous claims
  - Toll the statute of limitations during relevant windows.
- Review text and prominence of update notifications to users/consumers.

Risk Management & Business Priority Considerations

Privacy+ Security Forum

Risk Mitigation & Business Considerations

Privacy+ Security Forum

Financial Considerations

- Penalties and Damages or cost of legal defense.
  - Motion to dismiss ($20k-40k on average).
- Many plaintiffs firms have a “known market rate” to settle their claims.
  - They will tell you what their market rate is.
- In many cases these plaintiffs firms are looking for a quick settlement.
- Plaintiffs firms will continue to send more demand letters to encourage settlement.
- Strategic settlement - if you have multiple claims, you may be able to bundle them together.

Risk Mitigation & Business Considerations

Privacy+ Security Forum

Reputational Considerations

- Plaintiffs firms will advertise and solicit potential claimants/plaintiffs on social media and elsewhere.
- Consumer trust - your consumers may be targeted with these advertisements.
- Some plaintiffs firms are focusing on particular industries or industries with certain types of data.
  - Sensitive data.
- Negative publicity - whether or not the claims are meritorious may not matter to consumers who see solicitations about a company's privacy practices.
- How to combat these concerns:
  - Transparent communication.
  - Robust privacy policies.
  - Compliance with applicable privacy laws and regulations.

Risk Mitigation & Business Considerations

Privacy+ Security Forum

Operational Considerations

- Review your consent flows to ensure they are robust and consumers have choices.
- Ensure you have a deep understanding of your advertising practices and how you deploy pixels, cookies, and other similar technologies.
- Consider pixel monitoring technologies and consent management technologies to automate your processes.
- Review your terms of service, especially your arbitration provisions, if applicable.
- Basic privacy controls matter - fundamentals:
  - Limit data collection.
  - Notice and Consent.
  - Security Controls.
  - Third-party management.

Questions & Contacts

Carter Simpson

Partner, Paul Hastings

cartersimpson@paulhastings.com

Matt Gardner

Senior Privacy Counsel, Ro

matt.gardner@ro.co