Pixel Litigation: What You Need to Know

Caren Decter
Gina Gerhardt

May 6, 2025

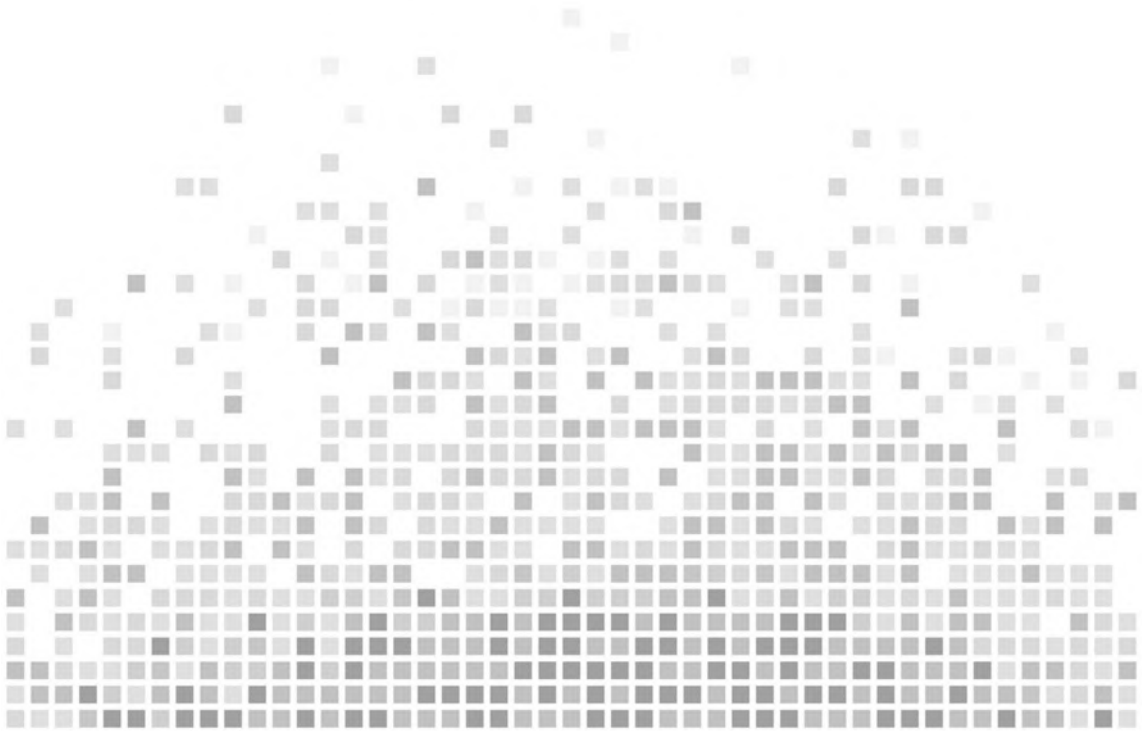
Frankfurt Kurnit Klein + Selz PC

What Are Tracking Pixels?

- A tracking pixel is a small, transparent image embedded in a webpage or email that can track collect information about the user's behavior, such as:
  - Pageviews
  - User data (IP addresses, device types, browsers, and geographic location)
  - Conversion tracking (when a user completes key actions such as making a purchase)
  - Ad performance (impressions, clicks, post-click conversions, etc.)

Common Types of Tracking Pixels

- Retargeting pixels
- Conversion pixels
- Analytics pixels
- Social media pixels



What's the deal with all of this tracking pixel litigation?

Tracking Pixel Litigation – Legal Theories

- California Invasion of Privacy Act ("CIPA")
  - Wiretapping
  - Pen Register / Trap and Trace
- Other State Wiretapping Statutes Requiring Two-Party Consent (Massachusetts, Pennsylvania, etc.)
- California Consumer Privacy Act ("CCPA")
- Video Privacy Protection Act ("VPPA")

Pixel Tracking Litigation – CIPA

- Theory #1: Wiretapping violation – aiding and abetting theory
- CIPA Section 631(a) imposes liability on any person who aids a third party who "willfully and without the consent of all parties to the communication, or in any unauthorized manner, 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 passing over any wire, line, or cable or is being sent from, or received at any place within this state."
- $5,000 per violation

CIPA Litigation – Defenses

Consent

- **Users consented to cookies and pixels on the website via a cookie banner and/or acknowledgment of privacy policy**
  - *Lakes v. Ubisoft, Inc.*, No. 24-cv-06943, 2025 WL 1036639 (N.D. Cal., April 2, 2025)
  - **But see**
    - *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1080–81 (C.D. Cal. 2021) (disclosure in privacy policy does not constitute consent)
    - *Lesh v. Cable News Network, Inc.*, No. 24-cv-03132, 2025 WL 563358 (S.D.N.Y. Feb. 20, 2025) (cookie consent not dispositive at the motion to dismiss stage)
- **Users consented to sharing information with Meta, etc. when signing up for a Facebook account**
  - *Smith v. Facebook, Inc.*, 745 Fed. Appx. 8 (9th Cir. 2018)

CIPA Defenses, Cont.

Participant Exception

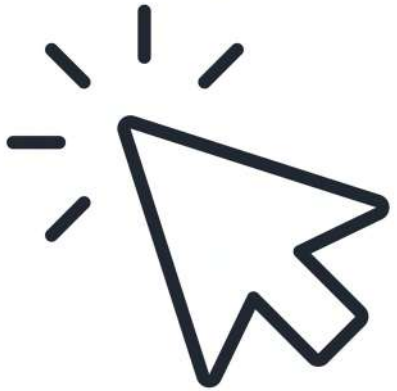
- "Is Quantum Metric a tape recorder held by Lululemon, or is it an eavesdropper standing outside the door? This is a question of fact for a jury, best answered after discovery into the storage mechanics of Session Replay. For the purposes of the instant Motion, Yoon's first claim for relief survives Quantum Metric's participant exception challenge because she alleges that QM captures, stores, and interprets her real-time data—which extends beyond the ordinary function of a tape recorder."

  Yoon v. Lululemon USA, Inc., 549 F. Supp. 3d 1073, 1081 (C.D. Cal. 2021)

CIPA Defenses, Cont.

No "content" intercepted

- Are mouse clicks, keystrokes, IP addresses, etc. "content" for purposes of CIPA?



CIPA: Trap & Trace/Pen Register Theory

- CIPA Section 638.51 prohibits anyone from installing "a pen register or a trap and trace device without first obtaining a court order"
  - Pen Register: "[A] a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication."
    - Outgoing information
  - 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."
    - Incoming information
- $2,500 per violation

PR/TT Defenses

No injury/standing because no protectable privacy interest in IP addresses

Compare

- *Casillas v. Transitions Optical, Inc.*, No. 23STCV30742, 2024 WL 4873370, at *6 (Cal. Super. Ct. Sep. 09, 2024): "That there is no privacy interest in IP addresses provided to a service provider or website is well established."
- *Gabrielli v. Insider, Inc.*, No. 24-cv-01566, 25 WL 522515 (S.D.N.Y. Feb. 18, 2025): Plaintiff voluntarily provided his IP address because he sought to access the company's website (IP address is *necessary* to access website)
- *Sanchez v. Cars.com*, No. 24STCV13201 (Cal. Super. Ct. Jan. 27, 2025): "Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."

With

- *Shah v. Fandom*, 754 F. Supp. 3d 924 (N.D. Cal. 2024): Plaintiffs plausibly alleged that they did not expect their IP addresses to be disseminated to the companies operating the trackers, and did not consent to the dissemination

PR/TT Defenses, Cont.

Trackers are not Pen Registers or Trap & Trace devices

- Pen register records *outgoing* phone numbers and TT devices record *incoming* phone numbers
- Plaintiff's own IP address/device info is not an outgoing or incoming number; the information at issue here is analogous to the telephone number on which the pen register or TT is installed
- Best cases:
  - *Palacios v. Fandom, Inc.*, No. 24STCV11264, 2024 WL 5494527 (Cal. Super. Ct. Sep. 24, 2024)
  - *Aviles v. LiveRamp. Inc.*, No. STCV19869 (Cal. Super. Ct. Jan. 28, 2025)

PR/TT Defenses, Cont.

Absurd Result: would criminalize normal internet behavior

"Public policy strongly disputes Plaintiff's potential interpretation of privacy laws as one rendering every single entity voluntarily visited by a potential plaintiff, thereby providing an IP address for purposes of connecting the website, as a violator . . . Such a broad based interpretation would potentially disrupt a large swath of internet commerce without further refinement as the precise basis of liability, which the court declines to consider."

- *Licea v. Hickory Farms LLC*, 2024 WL 1698147, at *4 (Cal. Super. Ct. L.A. Cnty. Mar. 13, 2024)

Compare with:

"[T]he question of whether the statute's scope should be narrowed ultimately rests with the Legislature, not the courts."

- *Shah v. Fandom*, 754 F. Supp. 3d 924 (N.D. Cal. 2024)

Pixel Tracking Litigation – VPPA

The VPPA makes it unlawful for a "video tape service provider" to "knowingly disclose[], to any person, personally identifiable information concerning any consumer of such provider." 18. U.S.C. § 2710(b)(1)

- Statute was enacted in 1988. How does it apply to technology today?

- **Consumer**: "any renter, purchaser, or subscriber of goods or services from a video tape service provider" (§ 2710(a)(1))
- **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, or any person or other entity to whom a disclosure is made" (§ 2710(a)(4))
  - Who is a consumer today? Who is a video tape service provider?

Pixel Tracking Litigation – VPPA

Salazar v. National Basketball A'ssn, 118 F.4th 533 (2d Cir. 2024)

- Plaintiff signed up for NBA online email newsletter and visited NBA's website and watched videos
- Court asked: Is Salazar a "consumer" under VPPA?
  - NBA argued that email newsletter did not constitute "goods or services" under VPPA's definition of consumer because the email newsletter was not "audiovisual" (District Court agreed)
- Second Circuit held that the plaintiff plausibly plead he is a "consumer" under VPPA because he adequately alleged he was a "subscriber of goods or services", and that phrase is not restricted to "audiovisual" goods or services

Pixel Tracking Litigation – VPPA

Salazar v. Paramount Global, 133 F.4th 642 (6th Cir. 2025)

- Same plaintiff as Second Circuit, same argument, different outcome
- Sixth Circuit held that Salazar was not a "consumer" under VPPA because the digital newsletter he subscribed to was not "audio visual materials"
- Circuit Split

Tips for mitigating pixel-related litigation risk

Frankfurt Kurnit Klein + Selz PC

What Can You Do?

Make sure you have a clear Privacy Policy that explains (a) what data you collect, and (b) whether/how it is shared

- Use everyday, easy-to-understand language

What Can You Do?, Cont.

Utilize a cookie consent or consent management platform (CMP)

- Allows users to provide or withdraw consent for pixel tracking clearly and transparently
- Enable users to select specific types of tracking—such as analytics or marketing—rather than an all-or-nothing approach
- Keep records of user consent, including timestamps and choices, to have proof if a dispute arises

What Can You Do?, Cont.

Implement regular legal and compliance audits

- Review pixel usage, consent mechanisms, and third-party agreements
- Regularly conduct vendor audits to ensure compliance
- Limit data sharing with third parties unless necessary (and making sure users have given consent)

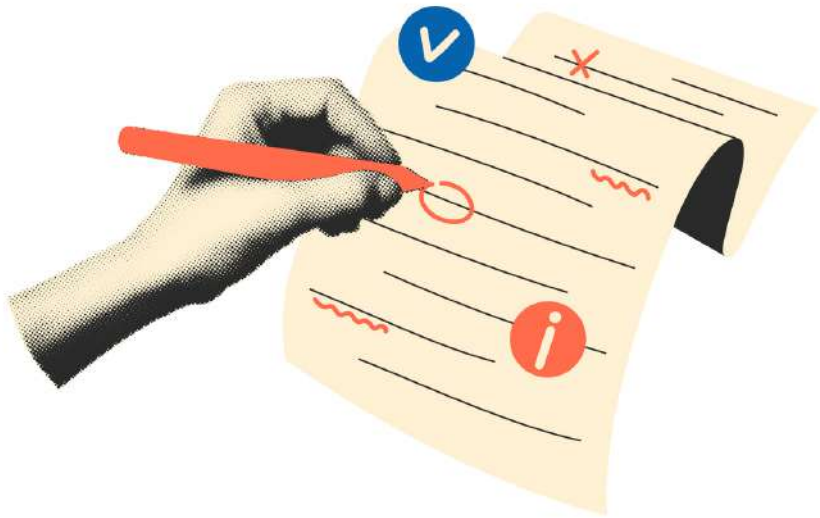
Create a data minimization and anonymization program

- Collect only the data necessary for your purpose to minimize privacy risks
- Implement techniques like anonymization and pseudonymization to protect users' identities

What Can You Do?, Cont.

Include a mandatory arbitration clause and class action waiver in your Terms of Use

- Make sure your arbitration provision is drafted to mitigate the risks of mass arbitration



Thank you!

Caren Decter
(212) 826-5525
cdecter@fkks.com

Gina Gerhardt
(212) 750-8835
rgerhardt@fkks.com

Frankfurt Kurnit Klein + Selz PC