WilliamsMcCarthy LLP

When the Demand Letter Arrives:

A Practical Guide to Pixel-Tracking Privacy Claims, Defense Strategy, and Insurance Coverage

By Joel M. Huotari, WilliamsMcCarthy LLP
Commercial Litigation • Intellectual Property • Privacy Defense

If your business operates a consumer-facing website and uses third-party tracking technology — Meta Pixel, Google Analytics, TikTok Pixel, LinkedIn Insight Tag, or any of the dozens of similar tools embedded in most e-commerce and marketing platforms — there is a meaningful and growing chance that you will receive a demand letter from a plaintiff's law firm alleging that your website violates consumer privacy laws. These demand letters have become one of the most active areas of consumer-side privacy litigation in the country, and most companies are not prepared for them when they arrive.

What is Pixel Tracking?

A tracking pixel is a small piece of code, historically a single transparent 1x1 image, embedded in a web page. When a visitor loads the page, the code causes the visitor's browser to send a request directly to a third party's server, such as Meta, Google, TikTok, or LinkedIn. That request typically carries the visitor's IP address, the URL of the page viewed, the referring page, browser and device identifiers, and cookie values. It can also carry actions taken on the page, such as clicks, form submissions, and purchases. Businesses use pixels to measure advertising conversions, build retargeting audiences, and analyze site traffic. Because the transmission to the third party happens at the same moment the visitor communicates with the website, plaintiffs characterize it as interception of the visitor's communications. That characterization is the foundation of the claims discussed below.

The numbers tell the story. In 2022, fewer than 60 lawsuits were filed nationally under the California Invasion of Privacy Act targeting website tracking technologies. By 2024, that number had grown to nearly 700. Total online-privacy lawsuit filings reached approximately 4,000 in 2024, up from just over 200 in 2023. Industry projections for 2026 anticipate more than 3,500 CIPA-related filings alone, with pixel tracking and AI profiling as the dominant targets. A separate analysis of court dockets identified online tracking claims filed in 315 courts across 45 states and the District of Columbia against more than 3,500 unique defendants over a three-year period. The volume of pre-litigation demand letters, which are not matters of public record, is substantially higher.

California remains the epicenter of this litigation, but Florida, Illinois, and Pennsylvania have emerged as significant secondary venues. The defendant landscape has expanded from healthcare and financial services — where the highest-dollar settlements have occurred, including a $21.5 million Sutter Health settlement and a $3.1 million Inova Health settlement in April 2026 — to retail, hospitality, consumer goods, and any other business operating a transactional website. Small and mid-sized businesses are increasingly targeted as plaintiffs' firms move down-market in search of defendants who will settle quickly to avoid defense costs. Any business with a consumer-facing website that handles California traffic is now a realistic target.

WilliamsMcCarthy LLP

What The Demand Letters Allege

The typical pixel-tracking demand letter follows a predictable template. It identifies the plaintiff as a state resident who recently visited the recipient's website. It asserts that the plaintiff's law firm conducted a "forensic analysis" of the website confirming transmission of visitor data to third-party tracking servers without consent. It identifies specific third-party recipients — typically Meta, Google, TikTok, and LinkedIn — and lists the categories of data allegedly transmitted, including IP addresses, page URLs, referring page data, browser and device identifiers, and cookies and session identifiers. It asserts a series of legal theories and demands pre-litigation resolution within a short window, usually two to four weeks, failing which the firm will file suit and seek class certification.

The legal theories are familiar to defense counsel who have handled these matters. The federal Wiretap Act (18 U.S.C. § 2511) is invoked on the theory that the website operator and the third-party tracker have together "intercepted" an "electronic communication" between the visitor and the website. The California Invasion of Privacy Act is invoked on two distinct theories: a Section 631 wiretap theory parallel to the federal claim, and a Section 638.51 "pen register and trap and trace" theory premised on the argument that tracking pixels capture "dialing, routing, addressing, or signaling" information about the visitor's communications. The California Comprehensive Computer Data Access and Fraud Act is asserted on the theory that the tracking software "copied" information from the visitor's device without authorization. Common-law claims for intrusion upon seclusion and unjust enrichment round out the package.

Statutory damages drive the leverage. The Wiretap Act provides for $10,000 per violation or $100 per day; CIPA Section 637.2 provides for $5,000 per violation. Multiplied across a putative class of every California visitor to the site over a multi-year period, the headline numbers in these letters can run into eight or nine figures. Realistic settlement values are far lower, but the headline numbers are designed to frame the negotiation and to make even a low-six-figure settlement feel like a discount.

The Technology Problem at the Center of These Claims

Most pixel-tracking demand letters target a specific operational gap that exists on a surprisingly large percentage of consumer-facing websites: the difference between displaying a consent banner and actually gating the underlying tracking technology. A consent banner that asks visitors to accept cookies, but does not actually prevent third-party tracking pixels from firing until consent is given, provides no real legal protection. The visitor sees a banner, the visitor declines or ignores it, and the pixels fire anyway. The legal theory in the demand letter then becomes: the website obtained no consent, and tracking nonetheless occurred.

The underlying issue is that most consent banners are installed as a layer on top of an existing tracking infrastructure rather than as a gate in front of it. Properly implemented consent management requires that tracking pixels be loaded conditionally, that they respect the visitor's consent choice in real time, and that they do not transmit data to third-party servers before consent has been affirmatively given. This is the standard that Google Consent Mode v2, Shopify's Customer Privacy API, and similar industry frameworks are designed to implement. Whether a particular consent banner installation is actually doing

what it appears to do, however, requires technical verification — and the verification is often not done after initial installation.

Plaintiffs' firms have developed sophisticated forensic tools that capture website behavior in HAR files (HTTP Archive format) and generate reports identifying every third-party domain that receives data on a typical page load. These reports are the evidentiary foundation of the demand letters. A business that receives such a demand letter is typically reading, for the first time, an accurate and detailed catalog of every tracking pixel and analytics tool active on its own website — and in many cases, the catalog reveals that the company's consent infrastructure is not functioning as the company believed it was.

Effective defense of these matters requires counsel who can engage productively with the technology, not just the legal theories. Understanding the architecture of consent management platforms, the operational differences between client-side and server-side tracking, the role of tag managers and consent frameworks, and the actual behavior captured in a HAR file is essential to evaluating whether the demand letter's factual premises hold up against the site's actual configuration. Defense counsel who treat these as pure legal matters — and who cannot meaningfully engage with the client's developers or the plaintiff's technical evidence — often miss the operational gaps and defenses that drive the realistic settlement outcome.

Available Defenses

The defenses to a pixel-tracking demand letter fall into three categories: consent and disclosure defenses, statutory and case-law defenses, and class-certification defenses. None is automatic, but together they support meaningful resistance to most pre-litigation demands when developed and deployed credibly.

The strongest defense for most defendants is disclosure-based consent. CIPA, the Wiretap Act, and CDAFA all contain consent or authorization exceptions. A website privacy policy that clearly and accurately discloses the categories of data collected through tracking technologies, identifies the categories of third-party recipients, and describes the use of the data for advertising and analytics purposes — and that the visitor was on notice of before continuing to use the site — supports a substantial consent argument. Courts have increasingly accepted this defense at the pleading stage where the disclosures are clear and where the visitor's continued use of the site constitutes implied consent. A recent federal case in the Northern District of California dismissed pixel-tracking claims on consent grounds where defendants demonstrated adequate disclosure and banner-based consent infrastructure.

The statutory and case-law defenses have grown stronger over the past eighteen months as courts have refined the application of older wiretap statutes to modern website technologies. The Ninth Circuit ruled in 2025 that CIPA Section 631 applies only to telephone wire, line, cable, or instruments and not to internet communications. The Third Circuit held in November 2025 that third-party tracking companies are direct recipients of browser communications rather than illegal interceptors. The Second Circuit's May 2025 decision in *Solomon v. Flipps Media* adopted an "ordinary person" standard for personally identifiable information under the Video Privacy Protection Act that has implications across the broader pixel-tracking litigation landscape. Multiple federal courts in California have dismissed CIPA pen-register claims for lack of Article III standing where plaintiffs alleged only collection of generic device and

browser metadata. The case law is far from settled, and outcomes remain mixed, but the trend on the defense side has been favorable.

Class-certification defenses are also stronger than they appear in the demand letters. The need for individualized consent and configuration analysis, the variability of consent banner interactions, the choice-of-law problems for putative California classes against out-of-state defendants, and the heightened Article III standing requirements following *TransUnion v. Ramirez* all make class certification a difficult prospect for plaintiffs' firms in most of these matters. Plaintiffs' firms know this, which is why the vast majority of demand letters resolve pre-litigation rather than proceeding to motion practice.

Successful pre-litigation resolution of these matters — whether at no payment, a nominal payment, or a contained individual settlement — typically requires defense counsel to develop a credible defense posture quickly, signal the strength of that posture to plaintiff's counsel in writing, and negotiate from a position of substantive strength. The first written response to a demand letter sets the tone for the entire negotiation that follows. Defense counsel who treat the demand as a settlement-cost optimization problem, rather than as a substantive legal matter with real defenses, often pay more than they should.

Insurance Coverage: The Most Important and Most Overlooked Piece

Cyber insurance coverage for pixel-tracking claims has become one of the most contested and rapidly evolving areas of the cyber insurance market. The short version: many cyber policies will respond to these claims, but coverage is increasingly fact-specific, increasingly narrow, and increasingly subject to carrier-side restrictions through exclusions, sublimits, or endorsement requirements. A company that does not affirmatively confirm its coverage before a demand letter arrives may find that its cyber policy provides far less protection than expected.

The current cyber insurance landscape reflects insurers' reaction to the wave of pixel-tracking and biometric privacy claims that have emerged over the past three years. Carriers have responded in several ways. Some have added specific exclusions for "wrongful collection" of personal information, often paired with biometric privacy exclusions that originated as a response to BIPA litigation in Illinois but that are written broadly enough to potentially capture pixel-tracking claims. Some have narrowed the policy definition of "personally identifiable information" to limit coverage to categories of data that statutes require to be protected — a definition that may or may not capture the IP addresses, browser identifiers, and cookie data at issue in pixel claims. Some have introduced sublimits specific to wrongful collection claims, capping recoverable defense costs and indemnity at a fraction of the policy aggregate. Some have moved coverage for these claims to dedicated endorsements that must be purchased separately, leaving the base policy ambiguous or silent on the issue.

Coalition, one of the leading cyber insurance carriers in the small and mid-sized business market, has publicly described its base Active Cyber Policy as containing "exclusions for claims arising out of BIPA (biometric) and pixel tracking," which are removed by purchase of its Enhanced Privacy Liability Endorsement. Other leading carriers have taken similar positions, though the specific language varies. Brokers and counsel reviewing cyber policies in this market need to look closely at how the policy treats wrongful collection, how it defines personally identifiable information, and whether any endorsement is in place to provide affirmative coverage for pixel-tracking and similar claims.

The practical takeaway for businesses: do not assume that a cyber policy covers pixel-tracking claims, and do not wait for a demand letter to find out. The right time to confirm coverage is at policy renewal, when there is leverage to negotiate endorsement language or to switch to a carrier with broader privacy coverage. A few specific items to verify with a broker:

- Does the base policy contain a "wrongful collection" exclusion or a similar exclusion targeting pixel tracking, biometric privacy, or unauthorized data collection? If so, is it removed or modified by endorsement?

- How does the policy define "personally identifiable information"? Does the definition reach the categories of data at issue in pixel claims — IP addresses, browser identifiers, cookies, device fingerprints, behavioral data — or is it limited to statutorily protected categories such as Social Security numbers and financial account information?

- Does the policy contain a sublimit for wrongful collection or privacy liability claims that is lower than the overall policy aggregate? If so, what is the sublimit, and is it adequate given the realistic defense and settlement costs of a class demand?

- Does the policy provide coverage for regulatory proceedings arising from privacy violations, in addition to private litigation? Many state attorneys general have begun investigating pixel-tracking practices, and a separate regulatory defense coverage may be valuable.

- Does the policy include a duty to defend, or only a duty to indemnify? Duty-to-defend policies provide stronger protection in pre-litigation demand situations, because the carrier may be obligated to fund defense costs from the moment the claim is tendered.

- Is wrongful collection coverage offered as a separate endorsement? If so, what is the premium, what are the sublimits, and what underwriting conditions does the carrier require — such as documented consent management infrastructure or periodic privacy audits?

A company that confirms broad wrongful collection coverage at policy renewal, with reasonable sublimits and a duty to defend, has substantially better protection against the realistic risk than a company that simply renews its cyber policy on whatever terms the carrier offers. The conversation with the broker should happen well before any demand letter arrives. Once a claim has been made, the company's ability to negotiate coverage terms is gone.

WilliamsMcCarthy LLP

When Coverage Is Disputed: The Value of Defense Counsel Who Can Fight On Two Fronts

Carriers do not always accept these tenders cleanly. When a pixel-tracking demand letter is tendered to a cyber carrier, the carrier may accept the defense under a reservation of rights, deny coverage outright on the basis of a wrongful collection or PII-related exclusion, or take a preliminary position pending fuller coverage review. Each of these outcomes requires the insured to manage a coverage workstream in parallel with the underlying defense, often under time pressure created by the demand letter's deadline.

Defense counsel who understand both sides of the equation — the underlying privacy litigation and the cyber coverage analysis — are substantially more valuable to insureds in these matters than counsel who handle only one side. The coverage analysis turns on policy interpretation principles, the specific defined terms in the cyber policy, the application of exclusions to the underlying claim's legal theories, and the duty-to-defend standard under the policy's choice-of-law provision. Coordinated defense and coverage strategy — including a written response to any preliminary denial that engages with the policy text and the policy structure — often determines whether the insured ends up paying its own defense costs or whether the carrier accepts the defense.

For insurance carriers, the calculus runs in the other direction. Carriers benefit from panel counsel who understand the coverage analysis well enough to defend cases without inadvertently expanding coverage through careless concessions, who can coordinate effectively with coverage counsel on reservation-of-rights matters, and who manage the underlying defense efficiently within the carrier's reporting and billing requirements. Defense counsel who can credibly handle both the substantive defense and the operational requirements of working with a carrier are useful to carriers in a market where panel counsel for privacy matters is in growing demand and relatively short supply.

What To Do If You Receive a Demand Letter

Five steps, in order of priority:

1. Get the demand letter to counsel immediately. Do not respond to plaintiff's counsel directly, do not negotiate with plaintiff's counsel directly, and do not engage with the substance of the demand without legal advice. The deadlines in these letters are negotiating postures, not procedural deadlines, and there is time to develop a considered response. The right counsel can often resolve these matters at no payment or at substantially lower numbers than the demand letter suggests — but only if engaged early enough to develop the defense before the negotiation begins.

2. Tender the claim to your cyber insurance carrier and any other potentially responsive policy. Tender should be in writing, with the demand letter attached, and should request a defense or, alternatively, a written coverage position from the carrier. Carriers must be on formal notice promptly to preserve coverage; oral notice or informal communication may not be sufficient under the policy's notice provisions. If the carrier takes a preliminary position denying coverage, push for a written coverage determination and engage counsel to evaluate that position before accepting it.

3. Conduct an immediate technical review of the website. Pull the website's privacy policy and verify that it is current, accurate, and consistent with actual practice. Run a forensic capture of the site's current behavior from the relevant jurisdiction to document what is actually happening. If the consent infrastructure is not functioning correctly, identify the gap and plan remediation. Do not communicate technical findings to plaintiff's counsel without first reviewing them with defense counsel.

4. Develop a response strategy in consultation with counsel. The right response depends on the strength of the disclosure-based defense, the technical record, the realistic settlement range for the matter, the cost of defense if the matter is litigated, the availability of insurance coverage, and the company's appetite for risk. Most pre-litigation demand matters resolve through negotiated individual settlements, but the best outcome — including a possible no-payment resolution — requires a credible defense posture from the outset.

5. Plan for remediation regardless of how the underlying matter resolves. Even if the immediate demand resolves favorably, the same plaintiffs' firms and copycat firms continue to target the same operational gaps. Remediating consent management infrastructure, updating the privacy policy, and documenting compliance practices are the best long-term defense against future demands. A company that resolves one pixel-tracking demand but does not fix the underlying technical issue is exposed to the next demand from the next plaintiff.

The Best Defense is Preparation

The volume of pixel-tracking demand letters and class action filings is unlikely to decrease in the near term. The plaintiffs' bar has built a profitable, repeatable practice around these claims, the underlying technology issues are widespread across consumer-facing websites, and legislative efforts to clarify or narrow the underlying statutes have stalled — California's SB 690, which would have excluded routine commercial tracking from CIPA, did not pass in 2025 and remains a "two-year bill" with uncertain prospects. Businesses that operate consumer-facing websites should expect to receive a demand letter at some point and should plan accordingly.

The companies that handle these matters best are the ones that took action before any demand arrived: they audited their consent infrastructure, updated their privacy policies, confirmed their cyber insurance coverage, and documented their compliance practices. The cost of that preparation is modest. The cost of responding to a demand letter from an unprepared posture, with uncertain coverage and uncertain technical facts, is substantially higher.

How WilliamsMcCarthy LLP Handles these Matters

Our firm handles pixel-tracking and similar website privacy claims, from initial demand letter through pre-litigation resolution, motion practice, and beyond. Our approach to these matters is built around three principles.

First, we engage with the technology, not just the legal theories. We work directly with our clients' development teams and compliance vendors to understand how consent management is actually

implemented, to evaluate plaintiffs' forensic captures against the site's real configuration, and to identify operational gaps that need remediation regardless of how the underlying matter resolves. We read HAR files. We understand the difference between client-side and server-side tracking, between Google Consent Mode and OneTrust, between Shopify's Customer Privacy API and a third-party banner overlay. Defense of these matters requires this kind of substantive engagement.

Second, we treat the insurance coverage workstream as integral to the defense, not as a separate problem for the client to manage. We tender promptly, we engage carrier claims counsel substantively, and where coverage is disputed we develop written coverage positions that engage with the policy text and the carrier's reasoning. For insureds, that coordination often determines whether the carrier funds the defense. For carriers, we can operate as panel counsel who understand the coverage analysis and do not create coverage problems through careless concessions in the underlying defense.

Third, we negotiate from substantive strength. Pre-litigation pixel-tracking demands are negotiable, but the realistic settlement number depends substantially on how credible the defense posture is and how well plaintiffs' counsel understands the obstacles to litigating the matter to certification. We develop the defense posture early, signal it clearly in the initial written response, and use it to anchor the negotiation. Pre-litigation resolutions at no payment are achievable in the right cases; nominal settlements are achievable in many cases; six-figure individual settlements are almost never necessary in matters that have been properly defended from the outset.

Whether you have received a pixel-tracking demand letter or simply want to review your website tracking, consent infrastructure, privacy policy, and cyber coverage before one arrives, we can help. We also accept engagements from insurance carriers needing defense counsel for insureds across a range of covered claim categories, including privacy and data protection, advertising injury, trademark and copyright infringement, defamation and other media liability, and TCPA or "junk fax" cases. We have experience coordinating with coverage counsel where coverage is disputed and managing matters under reservation-of-rights and panel arrangements.

Joel M. Huotari is a partner at WilliamsMcCarthy LLP in Rockford, Illinois, with a diverse practice in state and federal courts. His work spans commercial litigation, intellectual property (including trademark, copyright, and trade secrets), insurance coverage, and other complex business disputes, with growing involvement in privacy and data protection matters. WilliamsMcCarthy LLP • 120 West State Street, Suite 400 • Rockford, Illinois 61101 • www.wilmac.com

This article is provided for general informational purposes only and does not constitute legal advice or a solicitation for specific representation. Readers should consult qualified counsel regarding the application of these issues to their specific circumstances. The legal landscape described in this article is developing rapidly and may have changed since publication. Prior results do not guarantee a similar outcome.