LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
WEDNESDAY, APRIL 1, 2026
Published In the Leading Commercial Litigators 2026 Supplement

Why privacy law needs specialized courts in California

Jennifer L. Keller and Akhil Sheth

Judge Josefina Lee confronts the most recently filed complaint on her 824-case docket. The plaintiff alleges that the defendant helped a social media company intercept the plaintiff's PHI and PII—including full-string URLs, user IDs, and behavioral telemetry transmitted via a specific API and a session replay SDK—without the plaintiff's knowledge or consent. By doing so, the complaint continues, the defendant violated CIPA, the CMIA, the CDAFA, and the UCL (based on predicate violations of the CCPA, CPRA, and HIPAA), along with the California Constitution and other state common law. The plaintiff points to a parallel enforcement action by the CPPA.

Privacy is complicated.

It is also, increasingly, what judges like Judge Lee face.

A quarter of the way into this century, privacy is one of the defining legal battlegrounds. At least 20 states have enacted privacy legislation, as society tries to catch up with the consequences of a prior century whose rapid technological advances saw us go from Kitty Hawk to Mars. California led the way when it enacted the California Consumer Privacy Act (CCPA) nearly a decade ago and strengthened it with the California Privacy Rights Act (CPRA). Congress is considering national legislation.It's not just new legislation that keeps California at the center of it all. The California Invasion of Privacy Act (CIPA) was enacted in 1967 to stop wiretapping of phone lines. It's now being used to tackle tracking pixels, session replay software, and the third-party scripts embedded in many commercial websites. Statutory damages add up: $5,000 per violation. Multiply that by millions of website visitors and you have enough to keep an entire practice group or firm busy.

These cases can raise genuinely hard questions. Is embedding a third-party pixel wiretapping? Is an IP address a "trap and trace device"? Is clicking "Accept Cookies" consent to surveillance? Courts are reaching different decisions on many of these issues. As one example, California courts have split on whether CIPA's "pen register" provisions extend to the internet at all. By the time these questions are settled, the next technology will be here. The courts weren't set up to handle an issue that evolves so quickly.

That raises a question: should we set up our courts differently?

General jurisdiction trial courts are extraordinary institutions that we often take for granted. The same judges handle slip-and-fall cases, billion-dollar commercial disputes, custody battles and murder trials. That breadth reflects important principles—chief among them, the (perhaps naïve) notion that one need not be a specialist to understand the law. But there is a cost. A judge trying

Jennifer L. Keller *is a partner, and* **Akhil Sheth** *is senior counsel at Keller Anderle Scolnick.*

to manage a heavy civil docket isn't always going to develop and maintain deep fluency in a rapidly evolving world. It's unreasonable to expect them to understand (even with gifted advocates explaining it) the architecture of online advertising, the technical operation of session replay software, or the interplay between a 1967 wiretapping statute and modern data collection, all while staying up to speed on the rest of their docket.

We've faced this problem in other contexts and come up with a solution we should consider here: specialized courts. We created the Federal Circuit to handle patent appeals, based on their complexity and to ensure uniformity. We created the Court of International Trade to hear international trade-related civil actions, because those too involve specialized knowledge and need a consistent body of law. And here in the Central District, we had the Patent Pilot Program, in which patent cases were routed to district court judges who had received specialized training. In each of these cases, the solution to complexity wasn't to muddle through—it was to build institutions designed to handle that complexity well.

Privacy disputes aren't going anywhere. The cases pouring into California courts aren't just legally complex—they are technically complex in ways that compound the legal complexity. Often, they implicate some of our core constitutional rights. With those stakes, we're asking the judges, juries and our fictional Judge Lee to evaluate claims that turn on how tracking software works at a code level, what data is transmitted and when, and whether a particular script "reads" a communication in a statutory sense. These are questions that benefit from consistency, expertise and institutional memory.

A specialized court—or a specialized panel or division within the existing court structure—provides all three. It could develop a consistent body of case law instead of a patchwork of conflicting decisions. It could build judicial familiarity with the underlying technology (and adapt to new technologies). And it could reduce the transaction costs that come about every time a judge receives one of these cases for the first time.

There are downsides, of course. Specialized courts risk capture, with a revolving door between the court and the companies that appear before it creating bias (or the appearance of bias). Specialized courts cost money, create a new administrative regime and cause logistical issues. And specialized courts are insulated from the cross-pollination of ideas that inform the development of the law in courts of general jurisdiction. These are legitimate concerns and call for careful institutional design.

But these concerns counsel careful design, not inaction. The status quo is also a choice—and not a neutral one. Leaving privacy law to develop haphazardly, a step behind the technology it governs, is its own kind of decision. That decision deserves to be made deliberately.