ALM | LAW.COM

THE AM LAW LITIGATION DAILY

Where Privacy Laws and Litigation Trends Collide: A Conversation with Covington & Burling's Lindsey Tonsager and Kate Cahoy

By Kat Black
September 19, 2024

Since joining the ALM team in May, a mainstay of my coverage has been the explosion of online privacy litigation within the last few years, particularly cases filed under the California Invasion of Privacy Act (CIPA), the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA) and the Video Privacy Protection Act (VPPA).

As I tackle subjects such as the uptick in online "wiretapping" claims and suits targeting businesses' use of tracking pixels, I've become curious about the origins of this surge and how attorneys are navigating the application of older state laws to constantly evolving and emerging technologies.

To dive deeper into this issue, I caught up with **Covington & Burling** partners **Lindsey Tonsager** and **Kate Cahoy.** Tonsager co-chairs the firm's global data privacy and cybersecurity practice and is based in Covington's San Francisco office. Cahoy, based in the firm's Palo Alto office, is highly experienced in litigating cases brought under California privacy laws.

After an informal chat, I still had some burning questions, which they worked together to address in a Q&A for readers.

The following has been edited for length and clarity.

Courtesy photos

Lindsey Tonsager, left, and Kate Cahoy, right, of Covington & Burling.

To begin, let's talk about how we got here. Why are we seeing this sudden explosion in online privacy litigation now? Can you pinpoint when the surge began and what conditions set the stage for it?

Tonsager and Cahoy: The recent trend in privacy litigation we're seeing is claims under state wiretapping and invasion of privacy laws. Numerous companies have been hit with demand letters claiming novel theories based on use of search bars, cookies, pixels and other widely utilized technologies—some of which have been around for decades. This surge seems to have followed court decisions making it more difficult for plaintiffs to sustain claims under the Video Privacy Protection Act (VPPA). As the case law became unfavorable to plaintiffs under the VPPA, we saw these

plaintiffs pivoting and getting more creative in trying to apply other laws with statutory damages to these online technologies, where the law is untested.

We talked at length about how state privacy laws can both overlap and conflict with trends in online privacy litigation (e.g., wiretapping, tracking pixel and Video Privacy Protection Act violation claims). What are some of the biggest examples that you have seen of this, particularly at your firm?

One significant example is how the theories plaintiffs are pursuing in their wiretap claims are in conflict with the regulatory requirements in the state comprehensive privacy laws. For example, the California Consumer Privacy Act requires that companies provide consumers with an opportunity to opt out of having their personal information collected for purposes of cross-context behavioral advertising [which the CPRA defines as targeted advertising based on "the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts"].

However, plaintiffs' theory under the California wiretapping claims is that consumers must affirmatively consent (or opt in) to having their personal information collected for these purposes. It is difficult to imagine how the wiretapping laws, which have been on the books for decades, are intended to cover this conduct. There would have been no need for not only the California legislature to have enacted the CCPA, but also for there to be a ballot initiative amending the law to explicitly address sharing personal information for cross-context behavioral advertising if, all along, businesses had to get affirmative consent under the wiretapping laws. And the fact that the more recent laws expressly require only opt-out, not opt-in, consent is support that the wiretapping theories are overreaching.

It seems hard for these types of claims, which effectively dust off dated statutes and retrofit them for new technology, to survive motions to dismiss. Why is this? How much impact do they really have?

The claims as pleaded often fail to meet one or more elements of the wiretapping statutes. For example, some plaintiffs have not been able to demonstrate that they even used the defendant's online services, or that the contents of electronic communications were intercepted. As a result, judges are granting motions to dismiss where the elements of the laws are not satisfied. Because so much of the law remains untested, however, plaintiffs are continuing to aggressively pursue claims.

In our previous discussion, you explained that California is one of the states where we're seeing this activity—i.e., an uptick in CIPA violation claims—the most, partially because of the state's two-party consent requirements. Could you unpack that for our readers? Are there any other factors you've identified? Are there any other states or areas where you have noticed surges in this kind of activity?

We tend to see the most activity in those states with wiretapping laws that both (1) require all parties to a communication to consent to that communication being intercepted and (2) have statutory damages available. In the scenario where someone intercepts the telephone conversation between two people on a call, the federal law and a number of state laws allow that interception as long as at least one person on the call agrees to the interception of the communication. But in some states, including California, all of the people on the call must consent to that communication being intercepted, unless various exceptions apply.

Under the plaintiffs' new theories, plaintiffs argue these wiretapping laws should apply to a broad range of common online activities and that companies should obtain affirmative consent from all website users. Plaintiffs also tend to focus on states where statutory damages are available so they do not have to prove consumers suffered any actual damages.

In addition to California, litigation has been active in Pennsylvania, Massachusetts, Washington and Florida.

In our previous conversation, you noted that companies facing these lawsuits have often "done absolutely everything right in terms of regulatory compliance" but are still vulnerable to lawsuits invoking these decades-old statutes. Given that this is the case, what more can businesses do to insulate themselves from this type of litigation? How are you advising your clients to proceed and prepare?

Given the breadth of plaintiff's theories, many companies have become targets of these lawsuits, even though they are providing opt-out mechanisms for cross-context behavioral advertising consistent with the CCPA. Eventually, stopping these lawsuits will require further development of the law so courts can create precedent explaining why 1950s wiretapping statutes weren't intended to create staggering liability for routine internet conduct. As these cases proliferate, it will be important for companies to push back on these claims so that favorable law can develop.

We talked about how, sometimes, this kind of litigation seems to simply run counter to how modern technology and the internet were designed to work—aka, interpreting using a search engine as "wiretapping." How do you think these claims will continue to evolve in the future as the technology does?

At the end of the day, these laws are criminal laws requiring notice and due process, which seems to be lacking for some of the current theories. Moreover, in some other contexts where there has been overreach in litigation, legislatures have stepped in to amend the statute. For example, earlier this year the Illinois legislature amended the state's Biometric Information Privacy Act (BIPA) in response to plaintiffs seeking aggressive interpretations of how to calculate statutory damages under the law. How claims will continue to evolve will depend on how the courts and legislators react to rapidly evolving technologies.

In our discussion, you talked about "attempts to use state law to layer on causes of action that would allow plaintiffs to try to recover for alleged regulatory violations." What are some examples that you've seen of this? Can you recall a specific case you worked on in which you and a client navigated this climate of complex privacy litigation head-on?

Even in cases where privacy statutes do not provide a civil private right of action, plaintiffs have become increasingly creative in attempts to base alleged violations of state consumer protection laws or common law protection on an underlying regulatory violation. We've been able to get a number of these cases dismissed in early stages.

One of the great things about working at Covington is that the two of us—and our other colleagues across the litigation and regulatory privacy practices—get to work together to scan the full landscape of litigation, legislative and regulatory developments to advise our clients on how to assess and mitigate legal risk.

A class action litigation can sometimes spark a regulatory investigation, and vice versa, so it is important to develop a strategy that addresses both the litigation and regulatory issues.

California often leads the way when it comes to online privacy laws. How do you think this surge in CIPA claims will influence regulatory approaches to online privacy in other states?

We have not seen CIPA claims influence the legislative approaches taken in other states. Instead, and significantly, states around the country that have enacted comprehensive privacy laws have followed the CCPA in pushing for businesses to provide consumers an opportunity to opt out of targeted advertising, rather than imposing an affirmative opt-in consent requirement.

This is one of the confounding aspects of the novel CIPA theories—they conflict with the way legislatures have been approaching these issues in all of the privacy statutes developed to address modern-day technologies.