Transcripts are generated automatically using AI and may contain errors or omissions.

Becca Rainey (00:00)
Welcome to The FP 5: Five Things for Your 9-to-5. We help employers make sense of the fast-moving world of workplace law and compliance by breaking down topics into five parts. I'm Becca Rainey from the Fisher Phillips Content Team.

California's decades-old wiretapping law is fueling a surge of lawsuits over everyday website technologies, like cookies, pixels, and chat tools. Usama Kahf joins us this week to talk about it. Usama is a partner in Fisher Phillips's Irvine office, and he co-chairs both the firm's AI, Data, and Analytics Practice Group, and the firm's Privacy and the firm's Cyber Practice Group. He's a busy guy. And he also has the honor of being our first repeat guest on the podcast. Usama, thanks for being on the show today.

Usama Kahf (00:51)
Wow, I didn't know I'm the first repeat guest.

Becca Rainey (00:54)
You are, you get the award!

Usama Kahf (00:56)
It's a privilege and an honor.

Becca Rainey (00:59)
Before we get into the legal issues, your practice is right at the intersection of employment law, privacy, cybersecurity, and AI, a combination that's become incredibly important over the last few years. Give our listeners a quick overview of what you do and the kinds of clients you help.

Usama Kahf (01:17)
So our sweet spot at Fisher Phillips is privacy in the HR context. However, you cannot be an effective privacy lawyer and be limited to that context only. Most of our clients want to hire one privacy firm that will address all of their privacy and AI-related needs and not simply those in the HR employment context. So in the Privacy, Cyber and AI Practice Groups, we advise clients on compliance with privacy and cyber and AI regulations, we help them implement privacy and cyber and AI programs; we also defend businesses when they get sued for privacy related or AI related issues. For example, we are defending companies in class actions involving the use of pixels on websites. It is not an employment issue, but yet those are the clients that come to us for that kind of work in addition to our labor and employment expertise, because privacy is really interdisciplinary. It impacts not just HR, it impacts, you know, every aspect of your business. So we are a full-spectrum privacy shop.

Becca Rainey (02:28)
All right, well moving into our five-part conversation. The first thing, for listeners who haven't been following this, how did a California wiretapping law from the 1960s suddenly become the basis for lawsuits over everyday website tools like cookies and pixels?

Usama Kahf (02:50)

It started as plaintiffs' attorneys trying to assert very clever, novel legal theories for wiretapping against companies that use technology on websites. And it has taken many strands. But the trend really took off when a court decided in May of 2022 that a user's interaction with a website constitutes a communication for purposes of the wiretapping law. Once you've established that threshold, the floodgates opened up of litigation.

There have also been a number of court decisions over the last few years that have also opened more of the floodgates. For example, in June of 2023, a court decided that a website's use of a software development kit or a type of tracking technology on the website can potentially constitute a pen register or trap-and-trace device, which is part of the statute in California prohibiting the use of such devices, without a court order. But the statute itself says nothing about how it applies to the internet, or even if it does, but one court said it does, and therefore we saw a lot of litigation arising out of it.

Becca Rainey (04:00)
What does the law say that makes it easy for lawyers to potentially exploit it? How does it define a trap-and-trace device or a pen register? How are they arguing that it could also equal, you know, pixels or this other tracking technology? What's the crux driving these lawsuits?

Usama Kahf (04:21)
Sure. The language says that you can't use a pen register or trap-and-trace device, or process. So it has the words "or process" in it. And those are the words that litigants and courts have harped on in combination with the fact that that part of the statute is very broadly written and doesn't specifically say that it applies only to the internet. And so courts will read this and say, at least some courts, not every court, will read the statute and say that, "Well, the pen register statute is very broadly written. We're supposed to construe it liberally because it's trying to protect privacy rights. The word 'process' could mean an electronic type of surveillance process or system, aka software, right?" And so that's where that's those decisions come from.

The opposite side of this are courts that are reading the exact same statute saying that, "Well, even though this section that prohibits the use of pen registers and trap-and-trace devices, it doesn't specifically say it applies only to telephone lines. It cross-references a couple of other sections of CIPA that do only apply to telephone lines." Specifically, it says you can't use pen registers or trap-and-trace devices or process without a court order pursuant to this other section. You go to this other section that describes how you can get a court order, and that is very specifically limited to telephone lines.

So the courts that have looked at this, there are least five state-level decisions by state trial courts, not federal courts, that have looked at the statute and said, because of this cross reference to this other section, you have to read both sections and context together, which means that the pen register prohibition only applies to the use of pen registers with respect to telephone lines, actually connecting these devices to a telephone line, which is how law enforcement used to use it or still use it to determine your incoming and outgoing calls without listening in to the phone call.

Becca Rainey (06:17)
Moving into thing two. So a lot of folks hear the word "California law" and think, that doesn't apply to me. I'm not in California. Why isn't that the case?

Usama Kahf (06:33)

Two reasons, the Long-Arm Statute and the personal jurisdiction bar that has been dropped significantly last year in the *Briskin v. Shopify* Ninth Circuit decision. So that's the first reason. The second reason is because the same legal theories that have been applied in California under the California Invasion of Privacy Act, it's under the California wiretapping law, are being applied across the country under federal law with nationwide class actions, as well as under particular state wiretapping laws like the wiretapping laws in Florida, Pennsylvania, and several of the other states that are two-party consent.

So this is not just a California problem. Even if you're not doing business in California, businesses are getting dragged into California courts and arbitrations because their websites potentially are you know, at least alleged to be targeting visitors in California, tracking visitors in California.

So the bar has been dropped significantly, based on that Ninth Circuit decision last year, about a year and a half ago, that has resulted in a lot more litigation against companies outside of California. But then federal law has also been applied in a number of court decisions that have opened the door for more litigation on the federal level. So we're seeing lawsuits in, you know, Texas, in Florida. Florida is now the number two state behind California. Florida is exactly where California was three, four years ago. So it's at the cusp of exploding into becoming the next battleground for digital wiretapping litigation. It's almost there. I mean, it's got 800 lawsuits filed in the state of Florida already, which means that outside of court, you probably got 10 times that number, 8,000 or more in demand letters and arbitrations that are not filed as part of the public record. So this is not just a California problem. This is now a federal, nationwide problem.

Becca Rainey (08:24)
So in these cases, you've mentioned businesses. Who are these businesses that are getting sued? Is it the big players or people going after large corporations? Or, who's getting wrapped up in these cases?

Usama Kahf (08:36)
No, most of the litigation is actually against small businesses. This is the mind-boggling part. People think this is a high, you know, a big tech issue where large companies are getting sued. No, there are some large companies that getting sued, sure. But most of the litigation is driven against small businesses and medium businesses. And that's a strategic decision by the plaintiffs’ bar because those are the businesses less willing to fight, with less resources. Those are the ones you can pressure to settle.

There are lawyers in California, for example, who have made it their mission to only target small, family-owned businesses in California. There's one lawyer, for example, you know, 200 plus law lawsuits, almost all of them are coffee shops, small coffee shops, not franchise, you know, chain coffee shops, small single, you know, operation or multi-operation, but private. And then plumbing companies, your neighborhood plumbing companies, your neighborhood HVAC companies, your, you know neighborhood roofer and solar installation company, and the list goes on. There are nonprofits that are getting, you know, attacked. There are claims against government agencies and you know K-8 private schools and in different states. You know, there are of course healthcare companies or financial services companies. There are manufacturers that are getting sued, a lot of manufacturers, in addition to the retail establishment. So you got a lot of retail companies, it's all over the map. Every industry is hit one way or the other. But the ones that the, you know, the biggest trend here is that most of them are actually small businesses.

Becca Rainey (10:14)

Yeah, it might have been easier to ask you who hasn't gotten it hit by these kinds of lawsuits.
All right, moving to our third thing. Courts are ruling in different ways on this. So where does the law stand today, generally, when it comes to this law?

Usama Kahf (10:36)
So with respect to CIPA, the courts are still divided. There is no consensus. There is some consensus in federal court regarding the pen register statute applying to the internet. So most federal courts are actually refusing to dismiss these claims, despite the fact that there have been at least five state trial court judges that have found that this section of CIPA does not apply to the internet. And the federal courts would just simply ignore; they're not persuaded by state trial courts that have made that decision.

And those decisions are currently being reviewed by the court of appeals in a case involving Variety Media that is getting a lot of attention with over a dozen amicus briefs being filed, most of them on the defense side, some for the plaintiff side. And the court is expected to hear oral argument on August 25th. It could come out each way. It could be a positive decision for businesses, for website operators, it could also be a devastating decision that's going to embolden the plaintiff's bar until an appeal is filed with the California Supreme Court. So the law is currently divided on the pen register issue.

On the wiretapping claims under Section 631, which will you know continue regardless of how *Variety Media* is decided, the courts are still divided on whether to allow these claims, but there is starting to emerge one trend, which is legal standing. At least in federal court, in order to establish a claim, you have to have been harmed in some way, in a way that the law had traditionally recognized in the common law, as a tort. When you allege as a plaintiff that your device identifiers and electronic fingerprint and your activity on a website was somehow, you know, disclosed to third parties through cookies, courts are rejecting that, saying that's not enough. Plaintiffs are alleging these technical violations claiming that they're entitled to money, even if they're not injured. They just say that it's a statutory violation and that should be enough because the statute says so, right? And the courts are starting to reject that, at least on the federal level, that there has to be more. There has to be something sensitive. For example, actual health information that was disclosed, a credit card number, a social security number, not just simply the fact that browser ABC with these hashtag identifiers visited this website and clicked on this or clicked on that. You know, none of that kind of information is sufficient to establish actual harm to survive in federal court.

Becca Rainey (13:16)
You're listening to the FP5. I'm Becca Rainey, and we're here with Usama Kahf. Usama is a partner in Fisher Phillips's Irvine office, and he co-chairs the firm's AI, Data, and Analytics Practice Group, as well as the firm's Privacy and the firm's Cyber Practice Group.

Thing four: There's a bill in the California legislature to address this. What's the goal of SB 690?

Usama Kahf (13:41)
The goal of SB 690 is to fix the abuse of CIPA. It's to eliminate litigation abuse so that businesses are not getting caught off guard. That's the original goal of the SB 690. It has been amended, however, right before the July 1st privacy committee hearing in Sacramento; it has been amended to limit the scope of what it's going to do to only the pen register section.

So CIPA litigation is going on under multiple sections of CIPA: 631, 632, and others, as well as section 638.51, that is the pen register trap-and-trace section. Now, as it is currently drafted, it would eliminate the private right of action with respect to this kind of online conduct under the pen register statute only. And it would allow for enforcement by the attorney general, by the California Attorney General. So only the AG would be able to enforce the pen register prohibition against websites if it deemed that there is a problem with the way that websites are operating or with the technology that's on websites or in apps. It does not, however, SB 690 does not fix litigation abuse as it currently stands that is happening under the other parts of CIPA.

And that's important to note because only a third of the lawsuits out there under CIPA are exclusively a pen register claim, meaning there's no other claim alleged under CIPA other than a pen register claim, which means that the rest of the lawsuits will continue. And there are at least a third of the lawsuits out there contain both a pen register claim and a CIPA wiretapping claim. So if the pen register claim goes away, the CIPA wiretapping claim under Section 631 would continue. And as we know and as we've experienced, many of these litigants and lawyers will simply pivot to a different part of CIPA to continue to litigate the same theory of liability against the business.

Becca Rainey (15:42)
What is the likelihood of this becoming law?

Usama Kahf (15:45)
It is very likely. I mean, it unanimously passed the privacy committee in the state assembly on July 1st. It is now in front of the appropriations committee. There is significant support for it. The opposition has all but faded based on how the legislation has been limited specifically to only the pen register section. So it is very likely that it could pass in its current form. However, some may argue that it actually makes things worse by not solving the entire problem.

And by just simply giving plaintiffs and their lawyers the ability to pivot to these other claims that are going to continue. For example, I mentioned the story of plumbers, your local plumbers and your local HVAC companies that are getting sued. Well, there's that one firm that's focusing almost exclusively on that type of small business. That firm usually alleges a Section 631 claim along with a pen register claim. So if the pen register claim goes away because of SB 690 that same, you know, abuser of CIPA will continue to be able to abuse small businesses.

Becca Rainey (16:53)
So our final thing for today, for businesses that are listening, what are the first steps they should take to reduce their risk?

Usama Kahf (17:01)
First is identifying and learning what technology do you have on your website? Do you even need it in the first place? Is it collecting data that is valuable to you? If it is not, turn it off. Get rid of it. That's the first answer. The second answer is: consult with an attorney on whether you should be implementing an opt-in consent solution or if you need to geofence to certain jurisdictions based on your risk tolerance and your need for the information that's being gathered through cookies and pixels.

But, review and update your consent management solution and process on the website, whether it's an opt-in or an opt-out. Also consider as part of that evaluation, whether you are gonna implement a gatekeeper-type banner, a blocker that blocks people from accessing the website until they have consented to certain things that are gonna happen once they're on the website. If you want the perfect example of that, go to fisherphillips.com. You will see that is the gold standard for how a gatekeeper cookie banner would be set up with all of the third party cookies inactive at that stage until someone has affirmatively opted in. That is a good way to eliminate the risk, but it is not the only way. There are many other solutions and avenues and pathways to get to a similar result. And that all depends on your need for the information, and then your risk tolerance and what jurisdictions and what laws apply.

Becca Rainey (18:22)
Yeah, and if you're a business looking for a place to start, you can always reach out to Usama or a member of the FP Privacy and Cyber team.

This is the part of the episode where we get to know you a little better in five questions. You ready? All right, we heard your surfer. So what's the best beach in Orange County for a weekend session?

Usama Kahf (18:51)
Definitely Doheny.

Becca Rainey (18:53)
Oh yeah? So what what's the best part about that?

Usama Kahf (18:56)
Very consistent waves. It's always calm most of the time, and it's fun. It's a long ride too.

Becca Rainey (19:06)
Yeah. Well I hope we didn't blow your cover on the secret spot.

Usama Kahf (19:11)
For longboarders. If you're a longboarder, you know, you love that spot. It gets crowded, but I always go super early. I'm like the first one in the water.

Becca Rainey (19:19)
So second thing, what's your favorite place you've ever traveled?

Usama Kahf (19:23)
Italy.

Becca Rainey (19:25)
Oh, yeah, which part of Italy?

Usama Kahf (19:27)
Positano, on the Amalfi Coast. Yep.

Becca Rainey (19:31)
Okay, adding that to my list. Next, you used to teach public speaking before law school, which is tougher, teaching a classroom or arguing in court?

Usama Kahf (19:41)
Oh man. Apples and oranges. Definitely teaching, is tougher than arguing in court.

Becca Rainey (19:53)
Yeah. Yeah. I feel like in court people hopefully are engaged, but I mean in school it's a little different to get everyone to pay attention. What's your favorite comfort food?

Usama Kahf (20:08)
Oh man. Probably hummus.

Becca Rainey (20:11)
Ooh, yes. Yes, agreed. All right, last question. What's something your colleagues would be surprised to learn about you? That you have an espresso machine at your desk?

Usama Kahf (20:24)
No, everyone knows. The entire world knows. They always ask me about it. They're like, you know, they comment about the babies over there. And I say, you know, you mean this baby?

Becca Rainey (20:36)
For those who can't see, he's got some very cute baby pictures behind him and then a very nice-looking espresso machine.

All right, that's all the time we have for today. Thanks again for being on the show, Usama.

Usama Kahf (20:48)
Thanks for having me.

Becca Rainey (20:51)
And thank you for listening to the FP 5. For more info, you can find a link to more of FP's work on digital wiretapping litigation in the show notes. We'll see you next week.