Podcast Transcript

The 'Long Arm' of CIPA and Its Newfound Pen-Trap Claims

Date: March 26, 2024

Guest: Matthew D. Pearson, **Host:** Randall Rubenking

Run Time: 19:57

For questions and comments contact:

Matthew D. Pearson

Partner
Costa Mesa
T: +1.714.966.8882 | mpearson@bakerlaw.com

Rubenking: Recently, many businesses have either been threatened with suit or been actually sued under an otherwise non-litigation provision of the California Invasion of Privacy Act, CIPA, the pen-trap statute. Now, these same businesses want to know just how far this law can reach, and what are the questions they should be asking themselves when faced with the threat of litigation? I'm Randall Rubenking, and you are listening to BakerHosts.

On today's episode, we explore the long arm of CIPA litigation with Matt Pearson. Matt is a partner in the Digital Assets and Data Management Group at BakerHostetler's Costa Mesa Office. He specializes in the group's Privacy and Digital Risk Class Action and Litigation team. Welcome, Matt.

Pearson: Hi, Randall. Thanks for having me.

Rubenking: You bet. Matt, to start things off, could you please give our listeners a brief overview of the current trend in CIPA litigation and define for us a pen-trap?

Pearson: Absolutely. Before we get into where we are now and how we got here, I think we first have to start with what a pen-trap is, because outside of the law enforcement world it is not really a frequently used term. A pen-trap is a term that covers two different types of devices or processes. It is a pen register and a trap and trace device. At a high level, these two devices or processes do very similar things. They both are used to determine the parties to a communication. They differ, though, in what information is being collected. In the simplest version, a pen register is installed on a phone and tells a third party, normally law enforcement, the number being called from that phone. In contrast, a trap and trace device is being installed on a phone to tell a third party, again, usually law enforcement, the number from which the phone is receiving calls. If you ever watch the show The Wire, you know what I'm talking about. A bunch of police officers sitting in a dark room staring at a computer that displays who is calling the subject, trap and trace, and who the suspect is calling, pen register.

Most people listening to this will think, well, we don't do that, and most people would be right under the scenario I just described. The problem is with the passage of the 2001 USA Patriot Act, the pen-trap definition was expanded to include not only a device, but a process, and it was done because the law needed to keep up with the advancement and evolution of Internet technologies and communications. In 2015, the California Legislature unanimously adopted this updated and expanded definition. But again, people listening to this will ask if the definition of pen-trap changed in 2015, why are we seeing this surge in litigation now? And the answer to that question is kind of fourfold. It is use, knowledge, an alleged change in the law, and uncertainty.

So first, use. Internet tracking technology has significantly advanced in the last couple of years. The widespread use of social media platforms has made it much easier for companies operating websites to identify who is actually visiting their website. In conjunction with that, the widespread use of cookies and pixels has made that identification easier and more precise. So, while the definition did change in 2015, the use of this alleged pen-trap device is a relatively new thing.

Second, knowledge. Website users now have access to programs that tell them what cookies are installed on websites they visit. In fact, Google Chrome has an inspect functionality that can show users the cookies present on the websites. If anyone listening to this podcast has ever received a pen-trap demand letter or a pen-trap complaint, they'll know exactly what I'm talking about. These demand letters and complaints usually include a screenshot taken by the user showing the cookies the user is claiming constitutes a pen-trap device.

Third, the alleged change in the law. In Greenlee, the Southern District of California held that software that identifies consumers, gathers data, and correlates that data through unique fingerprinting is a process that falls within CIPA's pen register definition. The reason I keep using the phrase alleged change in the law is because I don't think Greenlee actually changed the law that much at all. Greenlee was based on pretty unique facts. There, a data broker provided software developer kits to software application developers in return for the developers allowing the defendant to surreptitiously collect data from the app users. So that is a third party, i.e., the data broker, installed something on the user's phone in order to surreptitiously collect information about the user, and that was location data. That factual scenario falls pretty squarely in The Wire example I gave earlier. Lately, though, plaintiffs have not allowed Greenlee's unique facts to stand in the way of their filing claims. They read Greenlee to mean that any party, even an actual party to the communication, for example, a website operator who collects dialing, routing, addressing, or signaling information without a court order, as unlawfully utilizing a pen-trap device.

Lastly, the rise in claims now is largely based on the level of uncertainty surrounding these claims. No Court of Appeal has opined on the merits of plaintiff's pen-trap claims, and as far as I'm aware, only one trial court has and that has been in the last couple of weeks. That means a company who receives a pen-trap demand letter or lawsuit has no real way to determine whether the claim is valid or not. Now certainly, I don't think it is, but I can't promise a client that the court will agree with me. So, plaintiffs are really striking while the iron is hot, trying to scare companies into resolving these claims early. And doing so becomes a lot easier when one considers that if what the company is doing actually does violate CIPA, there is a possibility of a $5,000 per violation statutory penalty.

Rubenking: Well, that is a huge overview on a complicated issue, and given that most of this stuff now is being applied to social media and things over the Internet, that brings up the question, can CIPA apply to out-of-state defendants?

Pearson: Yeah. So, I get that question a lot and quite frankly, it is because a lot of the companies receiving these demand letters are not within California. For example, a Florida-based manufacturer of, whatever, socks, operates a website that people in California can visit. A California consumer goes to the manufacturer's website, notices that it is using cookies on its website, and sends a demand letter to the Florida company saying the company violated CIPA. The question is, by merely operating a website that can be accessed by California consumers, did the Florida companies subject itself to CIPA liability?

So first, it is pretty well settled California law that California statutes should not be applied to conduct that occurs outside of California unless it is pretty clear from the language of the statute that that is what the legislature intended. Now, there is not much, in fact, I would say there is nothing in CIPA that would suggest that the California legislature intended it to apply to conduct outside of California, what is called extraterritorial application. But that raises the question, which is much more difficult to answer, of where did the alleged unlawful activity occur? For example, the statute we're talking about, the pen-trap statue, really focuses on the installation and use of a pen register or a trap and trace device, but did that installation and use occur where the user was located, for example, in California? Or did it occur where the company is located, in Florida? Or did it occur where the company servers are located, which really could be anywhere? I mean, there are a number of possibilities here. Again, no court has yet opined on these issues, but I do believe that the answers to the questions will largely be dependent on what is being alleged and quite frankly, the facts of the case.

In this recent surge of CIPA claims, plaintiffs have alleged that the company has installed on its own website a web beacon, a cookie, a tracker that allows the company to capture these electronic impulses from the user in order to identify the user. But they have also claimed that the installation and use of this device is actually on the website user's browser, and that installation then sends the information back to the website. Where the plaintiff asserts that the company has installed something on its own website, the place of the wrong or the alleged unlawful conduct would be company, not user specific. For example, where the decision was made to utilize such a device, where the company's servers are housed, that kind. In contrast, where the plaintiff alleges that the company installed a tracker on his or her own browser, the place of the wrong may, in fact, be user specific, i.e., where the user was when the tracker was installed on his or her browser. All that is to say, and unfortunately, there is no clear-cut answer yet, but I will say that any non-California defendant who receives a pen-trap demand letter or a lawsuit would be remiss to simply assume that CIPA applies to it.

Rubenking: Okay. Well, there is a lot of factors going on there that haven't been decided. So, that leads us to another question for the out of state defendants, can they be sued in California under the CIPA statue?

Pearson: So, again, in typical lawyer fashion, I'm going to say it depends. Now, the law on jurisdiction is far more clear than it is as it relates to CIPA specifically. In California, courts can generally exercise jurisdiction over a non-California defendant, so long as that non-California defendant has a certain amount of what we call minimum context, such that exercising the jurisdiction doesn't violate due process. Now, that is a lot of words. It doesn't really mean much to anybody listening to it. What we're going to focus on here is specific jurisdiction.

Jurisdiction in California comes in two forms, general or specific. For a non-California company, general jurisdiction is pretty rare, if not, I mean, I'm not sure I've really seen it. So, specific is going to be the question. Specific jurisdiction is present when the cause of action, so the actual claim, arises out of or has some substantial connection with the defendant's in-state activities, right? That is going to raise the same question we talked about before of, where did the conduct occur? But if we look at specific jurisdiction a little more generally, it has three elements, all of which must be met. But for our purposes, the first element, which asked whether the defendant purposely directed its activities towards California, will be and has been really the focus of a jurisdictional analysis as it relates to Internet activity.

The Supreme Court of the United States set forth a three-part test called the Calder Effects Test, but again, much like California's analysis of specific jurisdiction, it is really the second factor of the Calder Effects Test that is going to come into play. Did the non-resident defendant, in deciding to implement trackers, cookies, whatever it did on its website, expressly aim those trackers and cookies at California? Now, it goes without saying that allowing personal jurisdiction anywhere that a web platform can be accessed would raise serious, serious due process concern. For that reason, the 9th Circuit has been drawing a line between merely operating a website and operating a website in connection, and this is a direct quote, with something more. So that, again, leaves us to try and figure out what is that something more? And that something more is, again, largely fact dependent.

Nevertheless, if you were to look at the case law from the 9th Circuit, you can draw certain questions that should be answered that would allow you to determine or help you determine whether or not a company is subject to personal jurisdiction. Those questions are, is the subject matter of the website specifically tailored to Californians? Right? There are certain websites, and the 9th Circuit has found certain websites, that are geared toward and really capitalize or exploit California markets. Companies operating websites like that are much more likely to be subject to personal jurisdiction than, for example, a website or a company operating a website whose content is basically, forum neutral. In my example of a Florida company selling socks. Everybody needs socks, they're not socks that are specific to California. That would be content neutral.

Does the company engage in activities to drive California residents to its website? This largely focuses on advertising. For example, the 9th Circuit has held that a company who specifically makes money advertising to Californians, as opposed to other individuals, more likely to be subject to personal jurisdiction. Whereas, if a company is making money advertising to any individual, whether or not they live in California, and that even includes if we're using geolocation to target the ads, if those ads are targeted not based on someone being a California resident, but just based on wherever that person is, that website and the company operating it is less likely to be held, be subject to personal jurisdiction. There is obviously a factor that takes into consideration how many California users are actually going to your website? If you're looking at some percentage that so far exceeds the percentage of California population has compared to the US population, you are much more likely to be subject to personal jurisdiction.

The last factor or, it is not really the last factor, but the last one we're going to discuss right now is, are the websites' terms and conditions and/or privacy policies aimed at Californians or users as a whole? Now granted, this case where the factor came up was really discussing whether or not a company could be subject to jurisdiction in the United States generally, as opposed to a foreign country. And quite frankly, I'm not sure how much this factor is still going to come into play, given that under the CCPA, nearly every company operating or having some business in California does need to have a California specific provision in their privacy policy. So, I don't believe that any court is going to find that by complying with the CCPA, you have essentially subjected yourself to personal jurisdiction in California generally. But again, and I hate to do this, but deciding whether CIPA applies, and if so, whether a company is subject to personal jurisdiction in California is really fact and a claim dependent analysis. But it really is an analysis that every non-California company must undergo even before considering any merit-based offenses to CIPA claims.

Rubenking: That is a lot to consider, Matt. Do you have any closing thoughts that you'd like to convey to our audience?

Pearson: I do. I completely understand the reaction to getting one of these CIPA demand letters and, or even an actual complaint filed, but what I tell clients is, time is on our side here. This is a novel theory that largely has not been tested by the courts. So, the more information we can gain through decisions through litigation, the better off a company is. The more information a company knows, the easier it is to evaluate what it is doing, what it is not doing, what the value of the claim is. So, I often counsel clients not to rush in and try to engage or resolve immediately but take a step back and consider the options and as we've discussed today, there are multiple options. You need to know whether CIPA even applies to you. You need to know whether you can be sued in California court, and quite frankly, you need to know the scope of the law and the landscape of what is to come. We've seen one decision rendered. We will see more and the more those come out, the better off a company is to defend itself in these lawsuits.

Rubenking: Thank you, Matt. If you have any questions for Matt, his contact information is in the show notes. As always, thanks for listening to BakerHosts.

Comments heard on BakerHosts are for informational purposes and should not be construed as legal advice regarding any specific facts or circumstances. Listeners should not act upon the information provided on BakerHosts without first consulting with a lawyer directly. The opinions expressed on BakerHosts are those of participants appearing on the program and do not necessarily reflect those of the firm. For more information about our practices and experience, please visit bakerlaw.com.