***The Consumer Finance Podcast* –** The New Wave of Web Tracking Litigation: Wiretap Statutes, VPPA Risk, and Consent Strategies
Host: Chris Willis
Guests: Jason Manning, Angelo Stio, and Rob Jenkin
Aired: November 13, 2025

Chris Willis:

Welcome to *The Consumer Finance Podcast*. I'm Chris Willis, the co-leader of Troutman Pepper Locke's Consumer Financial Services regulatory practice. And today we're going to be talking about a new wave of litigation against financial services companies dealing with tracking technologies on websites. But before we jump into that topic, let me remind you to visit and subscribe to our blogs, ConsumerFinancialServicesLawMonitor.com and TroutmanFinancialServices.com. And don't forget about all of our other great podcasts, *FCRA Focus* all about credit reporting, *The Crypto Exchange* about everything digital assets, *Payments Pros* all about the payments industry, and *Moving the Metal* our auto finance podcasts. You can find those podcasts on all popular podcast platforms. And speaking of those platforms, if you like this podcast, let us know. Leave us a review on the podcast platform of your choice and let us know how we're doing. Now, as I said, today we're going to be talking about a new wave of litigation that is very serious and generating a lot of trouble for various businesses, including those in the financial services industry. And joining me to talk about that are three of my colleagues, Jason Manning, Angelo Stio, and Rob Jenkin. Guys, welcome to the podcast and thanks for being here.

Jason Manning:

Glad to be here, Chris.

Angelo Stio:

Yeah, looking forward to talking about tracking technologies with you, Chris.

Rob Jenkin:

Great to be here.

Chris Willis:

Okay, so let's start by setting the table. Jason, do you mind just telling the audience what are the kinds of web tracking technologies that are at issue and giving rise to the claims being asserted in the litigation we're going to be talking about?

Jason Manning:

Yes, so there's been a very significant rise in litigation nationally, and it really is linked to, I would describe as different categories of technology. The first is tracking technology. This tracking technology is common on almost any, if not the vast majority of your interactions online, whether it's a browser or a chat or anything where you're landing on a webpage. There are programs that are running behind the scenes on those websites that will use cookies or pixels or a variety of ways to view the interactions of the consumer or the individual using the website. And then it's used for a variety of purposes by different companies that it could just to improve performance. It could be to build unique advertising or it could be for another company. And that tracking technology has been the core technology that is going to be relevant to a couple of these categories of types of lawsuits that we'd like to talk about today.

Chris Willis:

Thanks, Jason. Having told us about what the underlying technologies are that are giving rise to the cases, what are the laws that are at issue? In other words, what laws are these supposedly violating that are giving plaintiff's lawyers the idea to file lawsuits?

Jason Manning:

So there's a couple of different varieties of statutes that were enacted. I mean, some of these are 30 or 30 plus years ago, and usually they were enacted for law enforcement purposes or to restrict the usage of certain technology for law enforcement officials. For example. One of them is a surveillance act law, and there's a variety of these. They vary by state, but essentially the surveillance act laws are old wiretap laws, right? Tapping into somebody's phone. And a lot of states, as you probably have heard, have different requirements as to consent. Some states are single party consent, like Virginia, other states are two party consent. And if it’s a two party consent state, it's more challenging because then you have to effectively enable or elect into the “wiretapping.” Well, the application here to this technology is these old phone wiretap statutes have been repurchased for the new electronic technology for the computer tracking, and that was never their intention because they were never even contemplated, but they're being utilized by plaintiff's counsel across the country to push the limit of those state laws.

Chris Willis:

Okay. What about other forms of state laws that might be at issue?

Jason Manning:

Another one would be trap and trace. This again is an old law enforcement statute where if a police officer wanted to track a particular suspect with a GPS or some kind of form of location device, there were restrictions on it. Again, state and federal laws vary, but again, repurposing it for today's technology, this tracking technology we opened with is really after a digital footprint. These digital footprints, digital fingerprints, if you will, are really just ways of these various software programs to monitor and track your interactions with various websites. Where you go, what you do, what you click, what you don't click, what you see, what you pause on, and then

they build algorithms around this, right? Well, if that is a trap and trace type activity, well there are restrictions and state laws would apply, but the issue we're seeing is plaintiff's counsels are again, pushing the boundaries of this to places where it was never intended. And of course, we want to do two things. We want to both advise our clients on the front end and defend them on the backend.

Chris Willis:

Okay, so Jason, you've told us about two flavors of state statutes that are involved here. Is there yet a third to add to the mix?

Jason Manning:

The third category, if you will, would be the Video Privacy Protection Act, which again is another statute which is being repurposed for a new electronic technology. And there's developing law on all of these issues. And a lot of times knowing it is half the battle, right? You have to know what's out there. And you also have to know how your client's website is functioning and not just your website, but the engine behind it, the program that causes it to run and what cookies, if you will, are enabled and which ones are not enabled.

Chris Willis:

Okay, got it. Thanks a lot for that table setting, Jason. Now, I assume that there are certain states where this litigation is more active than others, and it will probably surprise no one listening to this podcast that California is one of them. So Angelo, do you mind breaking down what's going on in California and under California's state law with respect to these kinds of tracking technology lawsuits?

Angelo Stio:

Yeah, I think just to take a step back, the big driver on what statutes, state statutes and federal statutes being used are (1) statutory damages that are available, and (2) whether as Jason said, it is a two-party consent state, which essentially means I not only need to have my consent to intercept a communication or to track, but I need to get the website user's consent. So, in California, it's a two-party consent state. California has, as to all of the 50 states, the largest amount of statutory damages, which is $5,000 per violation. And it's being used in two ways. First is interception of an electronic communication under the wiretap statute, and it prevents a company from intercepting the content of an individual or web user's interactions with the website. Primarily, you'll see it with the enablement of a pixel on the webpage for checkout when you go to purchase.

People go and they have all these items they wish to purchase, but they never hit checkout. Oftentimes you'll see two or three days later, someone will get an email, Hey, you are about to purchase these products. Guess what? There's going to be 10% off if you purchase them today. That's the way the surveillance, the content of your interactions, works. The second one, trap and trace, is often used in California. It prohibits the use of a tracking technology that creates a digital fingerprint on your web browsing device without either a court order or both parties'

consent. That too, has the statutory damages of $5,000. Courts in California have interpreted both provisions within CIPA broadly, even though they're originally criminal statutes. And there is supposed to be a rule of lenity with regard to the application of ambiguous criminal statutes when there's civil penalties. But both of those statutes are being used in California and in addition to those two statutes, because a lot of the companies have come forward and said, wait a second, it wasn't me who did the interception. It was a social media company or an advertising company. California's law has an aiding and abetting provision as well that applies to both of those statutes. So even though you may not actually technically do the tracking, if you are allowing the tracking technology to be deployed on your website, it could give rise to a claim or an allegation that you're aiding and abetting either interception of electronic communication or trap and trace, and therefore you're liable under CIPA.

Chris Willis:

Got it. And let's flip ourselves over to the opposite coast of the country and talk for a second about Pennsylvania. Rob, what's going on with this kind of litigation there?

Rob Jenkin:

Yeah, so what we're seeing in Pennsylvania is similar to what Angelo was just describing in California though as Angelo noted, because California has $5,000 statutory damages, the majority of the action we're seeing does in fact occur in California. But Pennsylvania has the Pennsylvania Wiretapping and Electronic Surveillance Control Act, which is a similar wiretapping statute like CIPA. It was a criminal statute that also provides a civil remedy. Under Pennsylvania statute, you see a thousand dollars statutory damages, which is often appealing as well to the plaintiff's bar. And it similarly requires two party or all party consent, meaning that if I go visit your website and the website is recording or launching one of these tracking technologies, it's not enough that the website consented. I, as the visitor also have to consent. It's why anyone who visits websites these days are seeing a lot of those cookie banners popping up.

It's in large part in reaction to these laws and trying to receive consent to satisfy these two party or all party consent requirements. The big difference under the Pennsylvania statute as opposed to the California statute we were just discussing is really the court's treatment. We've seen the Pennsylvania courts be much stricter on these actions, less open to expanding them to the modern age and modern tracking technologies. And particularly we see those challenges in the standing arena where Pennsylvania courts have routinely now found that plaintiffs lack standing because they don't have an expectation of privacy when they visit websites. And if you don't have an expectation of privacy, there can't be a privacy violation.

Chris Willis:

Got it. So Angelo, turning back to you, Jason and Rob told us about some of the state laws. What's going on with respect to federal statutes under these kinds of subjects that might be giving rise to litigation as well?

Angelo Stio:

There is a federal wiretapping act, it's called the Electronic Communication Privacy Act. Unlike the two state laws that we discussed, Pennsylvania and California, the Electronic Communications Practices Act is a one-party consent statute, but it has been used most recently by a number of firms who are asserting claims under it, and they attempt to use, there's a crime tort exception, to the one party consent. So essentially, the way the statute works, I only need one-party consent in order to intercept, share or record your communication with me. However, if the purpose of the interception, recording or sharing of the information is to later commit a crime or a tort, it turns into a two-party consent statute. So, what we have been seeing over the last six months are entities being accused of violating the crime fraud exemption because they're sharing information with a third party and that would be a crime under another statute or regulation.

The main one that we see this allegation for is a healthcare entity where there's an allegation that HIPAA protected health information is being shared. HIPAA has a criminal component to it, and you'll see a complaint that says one-party consent doesn't apply because the sharing of protected health information, that's a violation of HIPAA; that's a crime. Courts have treated that differently. Some courts have said, no, the crime has to be independent of the actual interception itself. Others have said at the pleading stage, that's enough to get you over the hump and past a motion to dismiss. The other area where it's being applied, and it's not just to a healthcare entity, but to all entities is the tort piece of the crime tort exception. Mostly in the Northern District of California, we've seen a number of cases survive a motion to dismiss based on allegations that there was an interception of information in violation of the entity’s privacy policy.

And the tort exception applies because the privacy policy that the entity has on its website misrepresents what is being collected and what is being shared. And in those circumstances, courts have said at the pleading stage, that's enough to survive a motion to dismiss primarily, again, in the Northern District of California, there are contrary decisions in the Central District of California, but that's out there. And the big driver when I first started talking about these types of cases is statutory damages. Under the Electronic Communications Practices Act, statutory damages are $10,000 per violation, which provides the motivation incentive for individuals to try to pursue these claims.

Chris Willis:

Got it. And Rob, Jason had mentioned the federal VPPA earlier in the podcast. Is there litigation going on under that statute?

Rob Jenkin:

There is. So I think it's worth laying the history out because frankly, it's the most interesting of any of these statutes. As many of your listeners will remember, there was a time where Judge Bork was nominated in the late 1980s to the United States Supreme Court and was undergoing a senate confirmation. And during that Senate confirmation, a reporter decided to go out and get a list of all the movies Judge Bork's household had rented from a standalone video rental business. Something that in itself sounds old to describe now. And though there was nothing

particularly notable on the list of videos, apparently that scared Congress enough. And out of that in 1988, we saw the VPPA enacted. At its core the VPPA says you can't disclose what videos someone watches without their consent. What we've seen is litigation reviving the statute and saying, okay, everyone agrees it applies to the standalone business that rents movies that used to exist. But what about if a website through these tracking technologies we're discussing discloses what videos I watch on their website? And that's where this litigation stems from. Plaintiffs are bringing actions against website owners using these tracking technologies saying that they violated the statute by disclosing what videos I watched while I was on their website and seeking the $2,500 in statutory penalties that are associated with violations of the Act.

Angelo Stio:

The companies that are being targeted are streaming services that offer movies, but also all of the major sports leagues that have their own website that show video clips, and also digital media companies that deliver news not only in print but also in video components. So, a lot of digital advertising revolves around, well, what's driving the consumer or the user to the website? And what we're seeing is if there's a video that really is attracting a large number of individuals who otherwise might not go to the website, the social media companies, the digital advertisers, and even the entity itself want to know that. So that's how this tracking technology with respect to the VPPA works.

Chris Willis:

Angelo, thanks for that. Rob, back to you. What are the kinds of defenses that are available to defendants under these VPPA cases?

Rob Jenkin:

We've seen a number of defenses raised over the years in defense to these actions, but most recently where we've seen success and actually the creation of a circuit split is over what the standard should be to satisfy an action, particularly around disclosure. And there's two schools of thought. The one school of thought, which a majority of the circuits who have reached a decision have adopted, is known as the ordinary person standard. And that asks, could an ordinary person actually understand that a video that a user watched was being disclosed to a third party? And what we see there is when courts apply that standard, most often they look at the code and the tracking technology we're looking at and discussing and says, no, it's a bunch of letters, numbers and information. It's computer code. And an ordinary person looking at that would not be able to decipher the identity of the person who visited the website or the video they watched.

However, there is a second school of thought which a minority of circuits including the First Circuit have used, and that's the reasonable foreseeability standard. The reasonable foreseeability standard looks at a completely different question. That standard asks, did the company that is using the tracking technology reasonably foresee that the company intercepting the video watching habits would be able to understand and figure out who the person is and what video they watched. So, they look completely past the code. Instead asking was it foreseeable that that marketing company would be able to determine the identity of the person who visited the website and the video they watched? And it's a really interesting question

because what we've actually recently seen is a writ for certiorari to the United States Supreme Court being filed and asking the Supreme Court to weigh in and decide which of these standards are appropriate. And the determination will be very meaningful for the future of litigation under the VPPA because as I've noted before, the majority of circuits that have adopted the ordinary person standard are essentially the death knell to this litigation because an ordinary person cannot look at this code and actually find out who the person is and what video they watched. But of course, if the Supreme Court was to endorse the reasonable foreseeability standard, we'd expect to see a lot more of this litigation filed in the near future.

Chris Willis:

Got it. Well, that sounds like something very interesting for us to watch and probably report on this podcast if cert is granted right, Rob.

Rob Jenkin:

Definitely. And I will shamelessly plug to also follow the privacy group here at Troutman Data Privacy blog, which also will be tracking the filings and briefs filed.

Chris Willis:

I think that's a great recommendation and thanks for mentioning it. Let's wrap up the podcast with you, Angelo. With all this onslaught of litigation that you, and Jason and Rob have been talking about throughout this episode, what should companies do to try to protect themselves from being the latest victim of it?

Angelo Stio:

Yeah, so the main way to mitigate risk is consent, and there's a number of ways to do it. The primary way is through the use of what's known as a cookie banner. So, when you visit a website, you'll see a banner pop up at either at the bottom or the top right that discloses the use of tracking technologies and asks for consent. So, it's an affirmative opt into consent or at least discloses the use and allows the individual to exercise their rights to review and opt out of sharing. That's the first component. Consent. Second is disclosure. Consent is not very good if the disclosure behind it doesn't work. So, you want to review your privacy policies. You want to make sure that you are accurately disclosing how you collect process, share, dispose of information related to consumers or website visitors. And then the third way that you would want to do this, if there is any type of membership or purchase acknowledgement, even through a click wrap of the privacy policy or acknowledgement through the click of the consent management tool that this consent is in fact existing.

Those are the best ways. Finally, a lot of companies that we deal with don't know what tracking technologies are deployed on their website. They have a marketing or advertising company. Someone who's an employee may implement a tracking tool. That employee leaves and it remains on the website. It's not being used by the company for any purpose, and it's not taken off because no one knows about it. So, I recommend creating an index, doing an audit annually to see what tracking technologies are on there, what they're collecting, do we really need them,

and update your privacy policies accordingly or remove technologies that are not essential or not necessary anymore.

Chris Willis:

Okay. Thanks very much Angelo, and Rob and Jason, thank you as well for being on the podcast today. This has been really interesting and I know very valuable for our clients who might be subject to this kind of litigation or certainly if they're not, would like to avoid it. And so thanks for being on the podcast today and of course, thanks for our audience listening in today as well. As I mentioned at the beginning, don't forget to visit and subscribe to our blogs, TroutmanFinancialServices.com and ConsumerFinancialServicesLawMonitor.com. And Rob, give us the privacy blog again, please.

Rob Jenkin:

Of course. It's Troutman's Data Privacy Security and AI blog.

Chris Willis:

And what's the website address?

Angelo Stio:

It's www.TroutmanPrivacy.com.

Chris Willis:

Got it. Thanks very much. So obviously check that blog out as well. And while you're at it, why not visit us on the web at troutman.com and add yourself to our consumer financial services email list. That way we can send you copies of the alerts and advisories that we publish from time to time as well as invitations to our industry only webinars. And of course, stay tuned for a great new episode of this podcast every Thursday afternoon. Thank you all for listening.