Business Better Podcast (Season 2, Episode 30): Cyber Adviser – Assessing the Surge in Wiretap Litigation

Speakers: Philip Yannella and Gregory Szewczyk

Steven Burkhart:

Welcome to Business Better, a podcast designed to help businesses navigate the new norm. I'm your host, Steve Burkhart. After a long career at global consumer products company, BIC, where I served as Vice President of administration, general counsel, and secretary, I'm now Of Counsel in the litigation department at Ballard Spahr, a law firm with clients across industries and throughout the country. This episode is part of a series where we discuss emerging issues in the world of data privacy and security. In the past several months, plaintiff's lawyers have filed dozens of class action lawsuits under state wire tab laws, some of which provide for statutory damages of $5,000 per occurrence or more.

The lawsuits focus on the use of chat bots, session replay software, and tracking code embedded in websites. Plaintiffs contend these tools enable the surreptitious sharing of personal information with third parties and are illegal wire taps. Today, we will explore the reason for this surge in litigation, discuss the status of pending cases and potential defenses. Participating in this discussion are Phil Yannella, a partner in our Philadelphia office, and Greg Szewczyk, a partner in our Denver office. Phil and Greg co-lead Ballard Spahr's Privacy and Data Security Group.

Phil Yannella:

Hi everyone, and welcome Ballard Spahr's monthly webcast, Emerging Issues in the World of Data Privacy and Security. Last month, we tackle compliance with the California Privacy Rights Act, which becomes effective on January 1, 2023. This month, we'll turn our attention to the recent surge in wiretap lawsuits. My name is Phil Yannella. I'm a litigator and the co-chair of Ballard's Privacy and Security Group, and I'm joined this afternoon by Greg Szewczyk, who is also a litigator, as well as the co-chair of our Privacy and Data Security Group. For many people, wire tapping is an old fashioned thing that happens on a police procedural involves clunky telephones with actual wires. Indeed, when states began passing wiretap statutes back in the 1960s, telephones were the primary focus, but over the course of time, state legislatures have amended these laws to cover electronic communications, including the kinds of ordinary interactions that consumers have with websites through their laptops or mobile browsers.

This has significantly expanded the potential pool of would be defendants under state wiretap laws as most businesses have websites and most use third parties for website analytics, marketing, or support. As we will discuss shortly, some courts have held that allowing a third party to monitor website communications in real time constitutes a wire tap. As many wire tap statutes allow for liquidated damages of a thousand to $5,000 per violation, the potential damages for these seemingly mundane website activities can be significant. Given the astronomical liquidated damages and the often murky way in which plaintiff's lawyers plead allegations of third party wiretapping or eavesdropping, these cases present a challenge for defendants.

Here's the outline for our discussion today, which will focus primarily on California and Pennsylvania, which the hotspots for this new wiretap litigation. Greg will kick things off with the discussion of the recent evolution of wiretap claims and then talk in more detail about California. I'll then address the surge in Pennsylvania cases and the potential defenses there, and then Greg will then discuss proactive steps companies can take to avoid wiretap litigation, And then we'll wrap up. Without further ado, let me hand things off to Greg to take us through the evolution of wiretap claims.

Greg Szewczyk:

Thanks Phil. I'm glad that you kind of went into a little bit of a prelude about how these kind of recall things from the 1960s or 70s and thoughts of procedurals with cops wire tapping phones. The reason I like that is because the way I was planning to start off about the evolution is reaching back a little further to when we saw a lot of customer service call class actions, essentially, when the plaintiffs bar started figuring out novel theories to apply wiretap statutes in a way that would let them bring class action lawsuits. We saw many class actions filed over the years related to customer service call centers because

frequently they were recorded and for a long time there was no consent whether implied or expressed, so we started seeing these class actions raised and the numbers and the damages that we saw were extremely high.

If you think about a dollar per violation, statutory damages, it really adds up when you talk about it in the context of consumers calling into a call center, but it really scales up when you start putting in the context of a website, and that's what we started seeing happen back in the 2017, 2018 timeframe. Where things first started focusing on was what we would call session replay technology. This is a type of analytical cookie or tracking pixel that is put on websites that allows companies to see where a user clicks and what they do on a website. The general form of allegations that we frequently saw was that this could violate a state wiretap law because the analytics provider is also receiving in real time information about what the user is doing on the website.

Now, these claims were primarily filed in Florida, California, and Pennsylvania under those state wire tap laws in large part because they're two-party consent states, but they also have statutory damages in a private right of action. Now, in 2018, we started seeing these lawsuits filed, but they largely dried up over the years because there were several holdings that simply found that these aren't communications within the context of what the state wiretap laws have. By early 2021, we really weren't seeing many of these filed anymore, but then in March of this year, there was a case out of the ninth circuit that really breathe fresh life into these class actions, and then another in August of 2022 in the third circuit. Since then, we have seen just a huge resurgence of cases filed under California and Pennsylvania's law and then to really take us to current, in addition to the session replay, we're also seeing these cases filed alleging that the use of chat bots is a violation of the wiretap.

Now, chat bots, as many people will know are the artificial intelligent customer service chat box that pops up on certain websites. Now these are frequently used either to answer simple, straightforward questions or to do some pre-screening before they're sent to an actual person to help them with their customer service needs. We're also seeing these as a primary focus of the new wiretap laws. If we could go to the next slide, please, we will look at California a little more closely. The California wiretap claims are filed under the California's Invasion of Privacy Act or SIPA. Most of these claims that we are seeing have been filed under section 631. Under section 631 and more specifically, subsection A, it makes it illegal to, without consent of all parties to tap, make an unauthorized connection, read, attempt to read, or learn the contents of any message, report or communication while passing over any wire line or cable.

Importantly, it also makes it illegal to aid in abet or assist or conspire with something. More recently, we've started seeing claims filed under section 632.7. Under 632.7, that makes it illegal to, without the consent of all parties intercept receive or record communication transmitted between two telephone lines, and that also has the aiding and abetting liability. Now, both of these sections are subject to a private right of action that affords statutory damages of $5,000 per violations or three times the actual damages. Section 637.2 also provides that actual damages are not a prerequisite to having standing. With this as the framework, let's look go to the next slide and we'll talk about some potential defenses when these come.

Now, the first is the party exemption. There's a long history of case law in California that holds that a party cannot be liable for wiretapping its own. That is why we hit on that aiding and abetting statute because even though the party may not be, if the analytics provider is the one who may be subject, the website party could still be liable under the aiding and abetting. Another frequent defense we see is that what is an issue is simply not a communication. Now, a lot of this is going to depend on the technical aspects of what is actually in scope for the claim, and it can be hard to win on this on a motion to dismiss stage depending on how the plaintiff pleads the complaint because it may be an issue that can be successful in summary judgment, but if you just don't have the material available at the pleading stage, it can be difficult.

On that point, some of those recent cases that we talked about in the third and the ninth circuit have made this a little more difficult on this front. Where we expect the next real wave of issues to be is consent. A lot of privacy policies will disclose that there is some sort of collection going on. Is the mere fact that there is a privacy policy going to be sufficient? Will there need to be a browser app? Will there need to be a click wrap? How specific will the consent in a chat bot need to be? These are all issues that since this case law is still so new, there is a lot of ambiguity there. The other specific defenses that we see under SIPA, relate to both the 631 and the 632.7. Now, relating to that latter one, part of the reason that we're seeing this go to it is because of the specific types of actions that are actionable under 2.7 as opposed to 1A.Now, 1A relates to reading and for many of these situations, the analytics provider may not actually have access to the contents of what is being disclosed. That's part of the reason we're seeing this move towards 632.7. 632.7 has its own problems though, because that only relates to by definition what is going shared between two telephone lines, whether it's cellular or landline. In most of these situations, that's

not the case. Again, these have just been filed within the last month or two, so the case law just isn't there yet, but we do think that there's going to be some strong defenses, especially on that 632.7. Stay tuned to see where that goes. With that, I'll turn it over to Phil to talk about some of the Pennsylvania analogs to the California wiretap.

Phil Yannella:

All right. Thanks, Greg. My home state, Pennsylvania, has also seen a recent surge in wiretap cases. The Pennsylvania statute is the Pennsylvania Wiretapping and Electronic Surveillance Control Act, WESCA, which is another one of these state laws that allows for aiding and abetting claims, requires two party consent, and imposes liquidated damages, which under WESCA can be as high as a hundred dollars per day of a violation or a thousand dollars per individual. Now, the recent surge in litigation in Pennsylvania is driven by an August 2022 opinion issued by the third circuit that limited the direct party exception. This is a provision in most wiretap laws that states that a direct party to a communication cannot be deemed to have intercepted or eavesdropped on the communication. The case at issue is Popa v. Harriet Carter cards, and I'm going to go through the facts in detail because they're important to understanding how the law is evolving.

The plaintiff in the case had visited the Harriet Carter gifts website and begun the process for completing an online purchase of cat stairs. As occurs during these interactions, Harriet Carter gifts sent HTML code to the plaintiff's browser that caused the plaintiff's browser to simultaneously send a GET request to a third party, NaviStone. When NaviStone received the GET request, it sent code to plaintiff's browser that enabled the installation of a cookie, which both identified the browser and tracked plaintiff's activity on a website. The communications stream also enabled NaviStone to facilitate targeted advertising with plaintiff. The lawsuit alleges that this HTML code rerouted electronic communications to NaviStone and constituting a legal interception under Pennsylvania's wiretap law. The district court in the case granted summary judgment against the plaintiff, but the third circuit recently reversed. The third circuit's analysis really focused on whether NaviStone was a direct party to the communications between Harriet Carter and the plaintiff.

Like most states, Pennsylvania had previously adopted a direct party exemption, but they did so in a unique context, and the unique context was for law enforcement investigations where police officers had masqueraded as intended recipients of communications. This is the kind of thing that you normally see on Law and Order. The third circuit rule that this was the only scenario under WESKA which recognized a direct party exception. Critical to the court's determination that Pennsylvania's direct party exception was limited to law enforcement was a 2012 amendment to the law that expressly revised the law's definition of intercept to exclude monitoring by law enforcement masquerading as third parties, and under rules of statutory construction, if we can go back to law school, the court held that this express limitation foreclose broader exceptions, thus limiting the scope of the direct party exception. In other words, only law enforcement officers under expressly identified scenarios set forth in WESKA can avail themselves of the direct party exception.

NaviStone could not, and therefore, the third circuit found that the plaintiff had a viable claim against NaviStone for wiretapping, and against Harriet Cards for aiding and embedding that. Although this case is potentially quite impactful, and as we've noted, there's been a surge in new class actions in Pennsylvania, all is not lost. There are a number of viable defenses that can be still raised to these kinds of claims. First and foremost, consent. Greg talked about this in the context of SIPA, and Pennsylvania is very similar. Pennsylvania requires prior consent to wiretapping and it has to be two party consent, but they have also said that this consent can be demonstrated when the person being recorded knew or should have known the conversation was being recorded. In other words, it can be implied consent. The defendants in the case argued that the Harriet Carter privacy policy disclosed the sharing of personal information with third parties, and thus, plaintiff impliedly consented to the interception of her communications by NaviStone.

Plaintiff argued that she had neither read the policy nor agreed to its terms. The Third Circuit ultimately declined a rule on this and remanded the issue to the district court for further considerations. We should all pay close attention to how this case is ultimately resolved. A ruling that consent can be inferred through privacy policy disclosures may quickly chill future litigation MPA. On the flip side, a negative ruling will likely increase filings as websites scurry to revise their online disclosures. Another important defense relates to the nature of the information being intercepted. Pennsylvania's law, like others protects the contents of communications, but in many cases, the information being collected through website code or cookies is anonymized website usage data, what is often referred to as header info such as IP address as well as clicks and keystrokes and not the contents of any actual written or oral communications. Defendants have had success arguing under other state laws

that this kind of information collected through analytic tools or cookies are not communications within the meaning of those laws.

Another potential defense involves the locus of interception, Pennsylvania and other state wire tap laws only cover interceptions that occur in state. In the Harriet Carter's case, the third circuit held that the interception occurred at the point where the communication between plaintiff and Harriet cards was rerouted to NaviStone, which the court held was on plaintiff's browser and presumably the plaintiff was in Pennsylvania, but this is a technology dependent assessment. Harriet Carter involved a browser-based redirection, but other technologies may not. Now, this of course, is a factual issue that may require discovery, but don't assume that all third party website integrations involve browser base redirection protocols. Lastly, consider article three standing. A plaintiff must demonstrate an injuring fact to establish standing in federal court.

Although wiretap cases can be analogized to an invasion of privacy claim, which have a long history in U.S. common law, some courts have held that plaintiffs do not have a privacy interest in anonymized header information, which is not personal information under historical common law, and therefore these plaintiffs have not established an injury in fact. Some courts have dismissed wiretap claims on those grounds. This defense, however, is very fact intensive and will depend on the underlying technology and what is allegedly being collected. Standing can also be a puric victory for defendants as plaintiffs could theoretically refile their claims in state court. That's particularly true with WESKA, which is a Pennsylvania state statute and could give rise to Pennsylvania claims in state court. That's a rundown of the potential defenses to WESKA claims. Let's turn now from the legal to the practical. Greg, what can companies do now to protect themselves from potential wiretap lawsuits?

Greg Szewczyk:

Thanks, Phil. The absolute most important first thing that every company should be doing is knowing what they're actually doing. Up until fairly recently, there were many, many companies where the different types of analytical tools that were being used or the decision to put up some kind of an automated chat bot just didn't necessarily get across the right legal or privacy folks desk. They were seen as non-legal issues that didn't really need the review. If you don't know what you have or what your practices are, it is extremely difficult to try to actually mitigate or hedge against that risk. Step number one is actually knowing what you are doing and making sure that it's getting in front of the right individuals. Now, once that happens, then you can start assessing whether there are some ways to incorporate consents or notices to try to build in implied or express consent.

It is going to depend on the specific technology being used. It's going to depend on what the risk profile is, and there may be some judgment call to be made, but in many instances, there will be some way to work in some form of additional protection that there is at least implied consent. You also almost certainly should be updating your privacy policy. There are certain defenses that we talked about that may be difficult to bring at the motion to dismiss stage that are a little easier to bring if it is in the privacy policy because the privacy policy is frequently cited in the complaint, but even if it's not, it likely can be something of which the court could take judicial notice. One other thing to mention here is staying up to date on what's going on in this type of an area is extremely important. As Phil mentioned a second ago in going through the WESKA potential defenses, some of these, if the court goes in one way, it could chill all of these cases. In another, it could end up expanding them dramatically.

Either way, this is a rapidly changing area of the law where plaintiffs are testing new theories of liability about fairly cutting edge and new technologies. As much as we would rather be able to be fully proactive, there is a component of reacting to what is being alleged in the complaints, and as we start getting the case law, what the findings are. These may be small changes to the mechanisms of consent. They may be small changes to the privacy policy, but if you're staying up to date on what's going on in the case law, you're going to be able to position yourself to hopefully stay out of the cross hairs of the next class action, but if you find yourself in the unfortunate position of being on the wrong side of the V, you will at least hopefully have some built in defenses, including at the pleading stage. Stay tuned, stay up to date, watch what's going on in the case law, read the privacy law blogs, and make sure that you know how that risk is changing because it could be chilled or it could expand. It is hard to predict at this stage.

Phil Yannella:

Well thanks, Greg. This brings us to the close of today's webcast. Before we leave, one last word. In addition to speaking and blogging about cyber litigation, we've written a book on it. It's called Cyber Litigation. It's published by Thompson Reuters, and it's available at https://store.legal.thomsonreuters.com/law-products/Treatises/Cyber-Litigation-Data-Breach-Data-Privacy--Digital-Rights-2021-ed/p/106731568. If you're interested in this, please check it out. It covers everything from retail data breach litigations to online tracking litigations, like wiretap claims, to website accessibility claims. Again, if you're interested in this area, check out this book. Thanks again for joining us today, and we'll talk again next month.

Steven Burkhart:

Thanks again to Phil Yannella and Greg Szewczyk. Make sure to visit our website, www.ballardspahr.com, where you can find the latest news and guidance from our attorneys. Subscribe to the show on Apple podcast, Google Play, Spotify, or your favorite podcast platform. If you have any questions or suggestions for the show, please email podcast@ballardspahr.com. Stay tuned for a new episode coming soon. Thank you for listening.