



**Lowenstein Sandler's Insurance Recovery Podcast:  
Don't Take No For An Answer**

**Episode 75:  
"Keeping Track" of Your Cyber (and Other) Coverage  
Part I**

By [Lynda Bennett](#), [Heather Weaver](#)

**OCTOBER 2023**

- 
- Kevin Iredell:** Welcome to the Lowenstein Sandler podcast series. I'm Kevin Iredell, Chief Marketing Officer at Lowenstein Sandler. Before we begin, please take a moment to subscribe to our podcast series at [lowenstein.com/podcasts](https://www.lowenstein.com/podcasts). Or find us on Amazon Music, Apple Podcasts, Audible, iHeartRadio, Spotify, Soundcloud or YouTube. Now let's take a listen.
- Lynda Bennett:** Welcome to Don't Take No for an Answer. I'm your host, Lynda Bennett, chair of Lowenstein Sandler's Insurance Recovery Group. Today I'm joined by David Anderson, Vice President of Cyber at Woodruff Sawyer. Welcome back Dave.
- David Anderson:** Thank you.
- Lynda Bennett:** And I'm also pleased to be joined by Heather Weaver, counsel in the Insurance Recovery Group here at Lowenstein Sandler. Welcome, Heather.
- Heather Weaver:** Thank you. It's great to be here.
- Lynda Bennett:** Awesome. So today we've gathered to talk about the recent surge of litigation related to pixel and other tracking tools, and how those claims are impacting the insurance industry.

These are often big claims. By way of example, Google is currently in a 5 billion, yep, that's with a B, billion-dollar lawsuit in California over its tracking of internet activities after users switched to incognito mode. I certainly have fallen for that and believed that when I was incognito mode, it really was incognito, apparently not. And last August, the court denied Google's summary judgment motion and the case is now continuing toward trial. Also, at the end of last year, another major player in the social media space paid \$725 million to settle a privacy class action lawsuit.

So today we want to take a bit of a deep dive into what are these claims and are they covered by your company's insurance policy? And if so, which ones, because we know that insurance is a patchwork quilt of course? And most important for our listeners, what are the underwriting processes associated with these policies and will they be become more stringent?

So with that table sitting, let's dive in. And Dave, I want to start with the basics. What is a pixel tracking tool and how is it used?

**David Anderson:** Lynda, that's a great question. Good to be back. This might be one of the episodes for your most diehard fans.

Pixel tracking really was born of companies wanting to be able to target you with more relevant advertisements, right? It's based on your browsing behavior. Basically, it's a piece of code that companies embed on their website to track your activities. For example, your shopping carts, your prior purchases, anything that you might put on a wish list, any pages that you move from within a website.

It's used to basically amalgamate that information to give you a more targeted advertising experience, usually on social media platforms based on your interests, what retailer you're looking at, et cetera.

**Lynda Bennett:** So that's why when I go onto my social media, I get all kinds of ads based on a Google search perhaps that maybe I ran and suggesting that I really might want to buy yet another pair of sneakers that I don't need. Right?

**David Anderson:** That's exactly right.

**Lynda Bennett:** So Big Brother is watching. Are there other tracking technologies that are also spurring litigation around these privacy issues?

**David Anderson:** There's a lot, right? The sort of OG tracking technology that's been in place for years is the cookie tracking, which is basically it's small batches of text that personalize and save information about your browsing session.

Session replay is another very common tracking tool. It basically reconstructs what you are doing on that webpage or mobile application to capture your clicks, your mouse movements, and your scrolls. Just for reference, a lot of loan applications, insurance applications, financial institutions that are looking to accept your requests for one of their products services, will use this specific type of technology to deduce how much they think you're telling the truth or not. Like how many times you change the annual income box on a specific screen.

And then the sort of novel new kid on the block from a tracking perspective is our favorite, ChatGPT, which is used for customer service chats. Lynda, can you give me your tracking number for your package, and I'll search it for you? There isn't a person on the other end, there's just a robot that knows to take your information, process it and give you an answer.

**Lynda Bennett:** So we really are just steps away from being in The Matrix. Dave. Thanks for scaring me straight on using my internet browser for anything anymore. Thanks for that.

So Heather, I have a funny feeling that privacy lawyers are having quite the field day with all of this unbelievably useful tracking technology that maybe

you don't necessarily have permission to use. So what are some of the claims that we're starting to see emerging from the use of this technology?

**Heather Weaver:** Yes, Lynda, I think that's right. There are many different types of legal issues and claims that arise from the use of these tracking technologies. For example, there are claims against entities in the healthcare sector alleging violations of HIPAA and consumer protection statutes. There have been dozens of class action lawsuits filed against major hospitals, for example, in the last few years. For example, a patient might schedule an appointment online on a hospital's website for a particular doctor. Pixel tracker could collect the physician's name and expertise to figure out what types of treatments or services somebody might be receiving for targeted advertisement purposes.

We are seeing class action lawsuits alleging violations of state or federal wiretapping laws on the grounds that there have been interceptions of communications. And the plaintiff's bar specifically gravitate towards these high stakes claims because in a class action, there can be thousands of website visitors or more that could have a claim theoretically for thousands of dollars each. And so there's a big attraction there for those types of claims.

We're seeing invasion of privacy claims, common law tort claims based on an alleged duty or promise not to share such information. A lot of times this is often based on the sensitive nature of the data shared. In the healthcare sector in particular, we're seeing breach of fiduciary duty claims, breach of the covenant of good faith and fair dealing, breach of contracts, and unjust enrichment claims as well.

**Lynda Bennett:** Dave, do you see any other industries? I mean, it seems to me anyone that's got a website that has visitors can and may, or they are likely using the technology, right?

**David Anderson:** Heather pretty much covered the gambit of it. The other areas that we're seeing a very interesting scenario play out, and I'll just start with Heather's point. Our friends at the plaintiff's bar that are bringing these claims aren't necessarily privacy walks or privacy attorneys. So sometimes I get the vibe, and usually I expect to get some hate mail from his podcast, but sometimes I get the vibe that some of these plaintiff's attorneys are throwing pasta at a wall and seeing what sticks and what doesn't.

We have seen another sort of angle come in with the Video Privacy Protection Act, which was that law that came out in the late nineties about Blockbuster disclosing a politician's video violation. So to Heather's point, if you're scrolling on a website and there happens to be a video and you watch it and they collect the fact that you were watching that video and can attribute it back to you, that's a pretty black and white violation.

And in terms of just straight legal theories that are coming in through the claims, we are seeing a little bit of negligence and negligent misrepresentation thrown in as well.

And just the last point I would make to support Heather is we're seeing hundreds of these claims coming, hundreds across the country, especially in two party consent states like Pennsylvania, California, or Washington. So it's going to get messy before it gets better.

**Lynda Bennett:** Yeah. I want to just sort of double down also on what Heather said and why these claims are so concerning to companies. And that is the plaintiff's bar is really anchoring them in statutory violations where it's a per violation. So even one visitor that comes to your site 10 times exposes you to potentially 10 violations of that statute. Many of these statutes that they're relying on at the federal and state level also include attorney fee shifting and other types of pretty big financial hammers. And so I think we know why these claims are coming. Now we've got to figure out, hey, is there insurance for that? So I'm going to throw that jump ball and either Dave or Heather, you can answer that question.

**Heather Weaver:** I can take a first stab at that one. So as always, the answer to that question is it depends. And the first thing that you need to do is think about where should I look? What types of insurance policies are most likely to respond to these claims? And the first and most obvious and relevant place to look would be your cyber insurance policy. Cyber insurance policies, they vary, but they typically contain third party coverages such as privacy and network security liability, which very well could be applicable to these types of tracking claims.

We could talk a little bit more about some of the nuances and things to look out for, but these types of policies and these coverage grants in particular typically cover claims due to the unauthorized disclosure of sensitive data, like the types of personal and confidential information being collected through these tracking technologies.

A cyber policy might also have a media liability coverage section for things like invasion of privacy, which could be applicable. So it's important to do a thorough review of your cyber policy because there could potentially be more than one coverage grant that could apply to these claims.

Professional liability policies such as errors and omissions, E&O, directors and officers. E&O policies, that's another place to look. And those policies could also cover these types of claims. For example, E&O policies, which at a high level generally cover errors and omissions and performing professional services, they'll sometimes contain a third-party cyber liability coverage section.

So as an insured, again, it's important to do a thorough review of these policies as well. And this coverage could especially be applicable to the tech companies that are selling these technologies. And similar to cyber policies, E&O policies could also have a media liability coverage part.

You should also look at your general liability policies and if you have any management liability or media liability policies, those would be good places to look as well.

**David Anderson:** I was just going to throw in to Heather's point too, we are seeing a lot of the carriers that are very adjacent to the space, like the cyber and the media. And a lot of the E&O carriers really perk up to this exposure and start to manage it through amendments to their language.

But when you look at the slew of claims that Heather listed off, unjust enrichment, negligence, breach of contract, there might be coverages elsewhere as well. So if you find yourself stuck in one of these claims, Lynda, I would say right now in 2023, there is probably going to be a far less likelihood or chance that this is excluded on other policies you may not have expected than you will five years from now. So you really need to find someone like Lynda and Heather probably to skim all those coverages and look at what's going on because there might be a sliver of hope.

**Lynda Bennett:** Yeah, I mean, I'm glad Dave, you brought that up, because in addition to the laundry list of claims that Heather put out there, she brought up CGL coverage. We've seen some of these claims where there's a defamation claim included, and that's a perfect place where your CGL is going to intersect with this type of a claim. And we talk about this a lot on Don't Take No for an Answer. When you get a claim, you've got to think broadly, and you've got to notice broadly and you can sort it out later.

And I want to pick up on the thread that you just said Dave, too, which is there's still a lot of variety and lack of consistency, I want to say it that way, across our clients' different coverage programs. I mean, I sometimes refer to these policies as Frankenstein policies because the crime policy is typically a first party loss, but all of a sudden there's an endorsement slapped on the back of that that gives some level or at least some cyber coverage.

And so we can't overstate the importance of looking at every single policy. Even if it doesn't naturally pop to the top of your mind when this claim comes in, it's really important to just notice broadly and you can sort it out later. Because if the worst thing that you have to do is withdraw the claim under a policy that doesn't provide the coverage, no harm, no foul. Whereas the converse is not true. If you overlook that coverage and you're three years into the litigation, you may have really put yourself in the suit.

**David Anderson:** Late notice applies above all else.

**Lynda Bennett:** Yep. Well, listen, I think that we've covered a lot of ground here and I want to take a deeper dive, but I don't want to cut anybody short. So let's just talk at the high level and we'll pick it up next time. What is the most important thing to do when you get served with one of these claims right at the get-go.

**David Anderson:** I would say to your point, Lynda, step one, make sure that you have really, really expert privacy counsel on this matter. And it may not be a data breach incident response attorney or someone who really deals in ransomware or business email compromise. It might be a media-focused defense attorney who understands the nuances of liable and slander and right to seclusion and right to privacy. So you're going to want to find counsel that addresses that in a really more targeted way.

And then second, you got to make sure that your coverages are aligned to notify and see where it goes, to your point. I hesitated to say a second ago, all these different random insurance policies like CGL and MedMal that bolted on little supplements for cyber and privacy cover thought that they were protecting themselves from claims. And they were. But you could actually leverage that to your advantage because perhaps those little bolt-ons may have a sliver of invasion of privacy cover without any of the fine print associated with wrongful collection or wire-tapping exclusion.

So yeah, first thing, when you get served, Lynda, get the right attorney. Get the right attorney for the matter at hand. And then second, notice everyone, because we're not at a place where this risk is systemically excluded at this point.

**Lynda Bennett:** All right, well, this has been a great table setter, but we obviously have much more to do. So in our next episode, we're going to take the deep dive after that lawsuit is there and you're starting to look at your policies, we're going to talk about what are the coverage grants, what are some things to be aware of? And I would ask both David and Heather, get your crystal balls polished up because we're also going to talk about where we're headed and what's going to happen with these policies.

I do appreciate both of you joining me today to set the table and to remind us all that incognito mode is not incognito, and Big Brother is constantly watching us. So thank you both for joining me today, and I look forward to having you come back next time to give us a little bit more detail on how to access this coverage and tee it up the right way.

**David Anderson:** Thanks, Lynda.

**Heather Weaver:** Thank you.

**Kevin Iredell:** Thank you for listening to today's episode. Please subscribe to our podcast series at [lowenstein.com/podcast](https://lowenstein.com/podcast) or find us on Amazon Music, Apple Podcasts, Audible, iHeartRadio, Spotify, Soundcloud or YouTube. Lowenstein Sandler Podcast series is presented by Lowenstein Sandler and cannot be copied or rebroadcast without consent. The information provided is intended for a general audience and is not legal advice or a substitute for the advice of counsel. Prior results do not guarantee a similar outcome. Content reflects the personal views and opinions of the participants. No attorney-client relationship is being created by this podcast and all rights are reserved.