Podcast Transcript

The Data Stream: Episode 9 with Paul Karlsgodt

Date: May 7, 2026

Guest: Paul Karlsgodt **Host:** David Sherman, Nichole Sterling

Run Time: 20:12

For questions and comments contact:

David Sherman

Partner
Philadelphia
T: +1.215.564.8380 | dsherman@bakerlaw.com

Nichole L. Sterling

Partner
New York
T: +1.212.589.4282 | nsterling@bakerlaw.com

Paul Karlsgodt

Partner
Denver | Seattle
T: +1.303.764.4013 | +1.206.332.1380
pkarlsgodt@bakerlaw.com

May: Welcome to the Data Stream, the podcast that dives deep into the fast-moving currents of data, technology, and the law. BakerHostetler's Digital Assets and Data Management Practice Group brings you this series, hosted by partners David Sherman and Nichole Sterling, to explore how companies navigate the complex and often intertwined life cycle of data, from privacy and cybersecurity to advertising, AI, and other emerging technologies. I'm Charlie May, and you're listening to BakerHosts.

On today's episode, David and Nichole are joined by Paul Karlsgodt, a partner at BakerHostetler and co-lead of the firm's privacy and digital risk class action and litigation team. Paul has spent more than two decades defending companies in complex, high-stakes privacy, data security, digital advertising, and emerging technology matters, helping organizations navigate litigation risk in areas where the law is still evolving.

Sterling: Hi Paul. Thank you for joining us today. It is nice of you to take the time. We've been trying to get somebody from the Privacy Litigation team to join us for a while, and we understand you guys are super busy all the time. So, as we understand it, you have been working on the front lines of privacy litigation for quite a while, and I believe class action litigation even longer. When you're looking at the landscape today, what has been changing over the last few years?

Karlsgodt: Well, a pleasure to be with you both. And I think the biggest thing that's changed over the last few years is just the volume of cases. When I started 15 plus years ago, data breach litigation was just in its infancy. And there were a few plaintiffs' firms making creative arguments and applying old statutes to new technologies. And now there are dozens, if not hundreds, of plaintiffs' firms out there pursuing these types of cases. And so, the volume of litigation has skyrocketed within the last five or six years. And there's both more data breach cases being filed for smaller incidents. There probably are more incidents being reported now than there were 15 years ago. And the explosion of internet tracking cases is keeping defense firms very busy in defending privacy cases.

Sherman: So, thinking about the universe of privacy and cybersecurity cases that are out there, I know many organizations, a lot of our clients even, still think about cybersecurity and ad tech and compliance as separate disciplines. From a litigation perspective, where do those areas most often intersect in ways that perhaps surprise teams later on?

Karlsgodt: Well, there is a lot of situations where that happens, but I think a really good illustration of it is in the latest trend of web tracking cases. That would be class actions and other lawsuits that are filed based on the idea that user activity on websites is being tracked by third parties. And that could be companies that are well known like Meta or Google, or it could be lesser-known companies that are involved in the ad tech environment. And just about everybody that has a website in the world is now susceptible to one of these lawsuits. Some are more serious than others.

But what we found when we started defending these cases is that there was a huge disconnect in terms of the organizations or most organizations in terms of the understanding of what legal knew, what compliance knew, what IT knew, and what marketing knew. And in a lot of the cases involving web tracking, there may be one or two people in the marketing department that have a good understanding of what a company is doing on its website, and no one else did.

And so, I think most organizations now are aware of this as being a litigation trend and are doing much better from a corporate governance standpoint in

having those different areas of the organization talk to each other, but when we really started, we didn't see a lot of that. And that was one of the biggest eye-opening things for me. An example was of the first couple of cases that came in, we made the assumption that because it involved technology and internet sites, that IT would be involved in some way. And in many cases, IT departments had no idea what was going on the website. Either it was being handled exclusively by a marketing team or in many cases, a third-party advertising company or web company.

Sterling: And that, I will just add, getting rid of some of these tracking technologies is very difficult as well. I've been through a couple of scenarios now where nobody could figure out even the account logins to get in to remove things because they'd been set up by somebody that had left two or three people ago in the chain of people that may have had control over that particular piece of ad tech. And that can be problematic for companies as well.

Karlsgodt: Yeah, and we're seeing a lot of that, a lot of situations where the technologies that are being attacked in a lawsuit are technologies that somebody installed years ago and forgot about, and no one really uses for any purpose, but they're still on the website firing and causing information to be transmitted to a third party. And so that is a fact pattern that has the attention of both the plaintiff's bar and some regulators, and it is the source of a lot of litigation these days.

Sterling: I think you're making a good argument for ad tech governance.

Karlsgodt: And that is one of the things that we always talk to clients about when we're involved from a defense of a lawsuit's perspective is, what can they do going forward to mitigate? I don't know that there is any company out there that can completely insulate themselves from advertising and website class actions and litigation because the plaintiffs are really speculating and they're finding something on every website that they feel like they can attack. That doesn't mean the claims have merit. It simply means that everybody is a target. And so, one of the things that we often talk to our clients about is what are the best ways to understand what you're using, why are you using it, and do you really need it? And if you do need it, then what disclosures are you making about it?

Sherman: Fair enough. The whole concept of, my goodness, there is a cookie and it is segmented, right, or siloed, just to come back to a point you were making earlier, or, hey, we have a security flaw or a vulnerability of some sort. I mean, how often do these technical issues, right, or I'll say segmented technology issues, at what point do they start looking like a legal narrative problem rather than troubleshooting a technical glitch or a collection that we weren't aware of?

Karlsgodt: Well, from my perspective, and I don't mean to make light of it, but it is when they get sued.

Sherman: That is a good answer.

Karlsgodt: And so, one of the things that we see, and of course, because my role is exclusively litigation, I'm only involved in those cases that result in a lawsuit or are highly likely to. So, for example, if there is going to be a breach notification these days, there is almost certainly going to be at least one lawsuit. And it almost doesn't matter how many people are going to be notified. And so now, if it is an issue that is more in the realm of customer data collection or disclosure, It may not be an issue that is going to require notification, but the fact that, website tracking is a great example, the fact that what is going on your website is visible to plaintiff's lawyers and their experts, that puts you at risk of being named in one of these lawsuits or receiving some claim.

And so, oftentimes it is a glitch that causes the issue that is underlying the claim. But in other cases, it is not. It is simply we're using a technology that everyone used. And a great example is Google Analytics. I've seen statistics that more than two-thirds of all websites in the world were using Google Analytics several years ago, and it wasn't until this wave of lawsuits that anybody saw anything wrong with it. And so oftentimes it is not a glitch, it is not a problem, it is not an institutional failure. It is just creative lawyers making technical arguments in courts that don't necessarily understand the technology.

Sherman: Pivoting for a moment then to cybersecurity incident response, teams understandably focus on containment, investigation, and notification as core elements of what they're working through in a fire. When we do a look back months later, what early decisions tend to have an outsized impact on how litigation unfolds?

Karlsgodt: Yeah, there are a couple of big ones. One is the decision to create or have someone prepare a forensic report and or a remediation report. When those types of reports are created, they become the singular focal point of plaintiff's efforts to gather information about the incident. And that is true, notwithstanding the fact that most of the time, they simply provide a summary of what happened and what gave rise to the breach notification.

And so oftentimes, what we see is a report that is created when it didn't need to be. There was no, say, regulatory requirement for its preparation, and it was easy to gather the facts without having a formal report created. And in those instances, it is typically better to not have a document than to prepare one and then try to protect it as privilege, knowing good and well that the plaintiffs are going to fight to the death to try to overcome that claim of privilege. So that is one issue.

Another one is really just how the communications around the incident are siloed and where they occur and efforts to make sure that you don't have people talking off the cuff about what they think happened or who was at fault. Oftentimes, in litigation, we see situations where everyone is in a C.Y.A. mode because they feel like the organization is going to blame them. And so, one, trying to control those types of communications, and two, trying to provide assurances to the folks that are involved that we're trying to solve a problem here. We're not looking for somebody to blame. Those can be really helpful in avoiding the creation of

documents that may be negative in terms of having to defend a data breach class action.

Sherman: So out of curiosity, quick pivot on that. When we think about preparing, let's say, non-privileged factual summaries, whether they're on company letterhead, in theory, forensic firm letterhead or otherwise, have you found success leveraging the distinction between privileged and non-privileged work streams successful in helping to shield privilege where it is applicable?

Karlsgodt: Not necessarily in the way that you asked the question. I think what we've seen is if you, for example, prepare two reports, one that is a factual summary and one that is purported to be a privileged document, the plaintiffs aren't going to care about the factual summary. They just want the privileged document. They will be focused on that.

Now, whether the judge rules in their favor or not remains to be seen, but judges do tend to, particularly when the defendant has exclusive control over the source of truth, they tend to be very lenient on the plaintiff's position on privilege and are very strict on the defendant's assertion of privilege. And so, in many cases, the forensic report that may be created in incident response has a dual purpose or, for example, it is needed for some business reason, typically, there is some regulator involved that is going to want the summary. And so, in those cases, it is very, very unlikely that if you try to claim privilege over a document, but you're going to share it with third parties, like many regulators, it is very unlikely that it is ever going to be protected.

And so having a source of truth is useful. So, I like in cases that I'm involved in, I like that there is a factual summary that expresses the factual events that were discovered during the forensic examination. But it is when you get into other issues like trying to attribute the threat actor to a particular group, things that are more opinion-based, those are the things that are very intriguing to the plaintiff's lawyers and are things that it may not be necessary to even do that in a particular case. And it may not be necessary to understand who the threat actor is in order to do the things that need to be done for breach notification, for example.

Sterling: This is all taking me back to my days as a litigator. My one time in court, by the way, David, I'll tell you this, was with Paul on an issue about a forensic report.

Sherman: Really? I never do that. Wow.

Sterling: Yeah, it was. Many years ago now, but yes, I got to go to court with Paul once.

Sherman: I am resisting the urge, Paul. As you may know, I'm also a recovering class action defense lawyer. I'm trying really hard to resist the urge to do a deep dive on privilege, so I'm going to bite my tongue.

Sterling: Returning to pixels and tracking tech, but also chatbots and AI and some of the things that we're seeing in that space, and I think especially with this California invasion of privacy litigation that has been going on, one of the things we get

asked a lot, at least on the compliance side, is, but I'm doing what I have to do to comply with the privacy law. Why do I then have to do these other things? And trying to explain that there can be these diverging theories under different laws. And it seems sometimes there is a bit of a lag in the law and that litigation is starting to fill that in a bit. Is that something that you feel like you're seeing on the privacy litigation side of things as well?

Karlsgodt: Yeah, and that's really been an issue since I started getting involved in privacy litigation 15 plus years ago. That's been the focus of several firms, going back to that timeframe, that we're always looking at ways to apply old laws that weren't really intended to deal with modern technology, but are broadly worded enough to potentially cover those technologies. And so that is exactly what we're seeing in wiretapping claims.

Wiretapping statutes were originally intended to protect against police surveillance and similar actions where someone is listening in on your phone call without you knowing about it. And they weren't really created with the internet in mind. But now you see plaintiffs' firms out there coming up with creative theories about why a particular internet communication. And what I mean by that is the transmission of data from one computer to another is somehow subject to wiretapping laws like the California statute, and many other states have similar statutes.

And so, the difference right now, though, is there are numerous more firms now doing that than there were 15 years ago when there might have been one or two really trying and often losing cases and trying to find theories that would stick. Now we have dozens of firms that are doing the same thing, and it really just ramps up, one, the number of lawsuits that are being filed across the country, but two, it increases the amount of collective creativity in the theories that are being presented to the courts. And so, both of those present a challenge to defendants, to companies, anybody that has a website, for example, or anyone that controls consumer information.

Sherman: So, Paul, we've done a lot of discussion of risk and judgment and legal, you name it. What do you do for fun? How do you take the, how do you get away from the pressure?

Karlsgodt: Well, I live in Colorado, so I'm a big skier. And so I like to, as much as I can, get out on the slopes and this has not been the best year for skiing, but I've still been able to take advantage of the conditions as we have them this year and bought a place up in Winter Park, Colorado last spring and have been enjoying spending time. And one thing that is great about being able to stay at a place up there is that you can maybe get a few turns in the morning and then still have most of your workday yet ahead of you. So that gives me a little bit of a release from the rigors of defending privacy lawsuits.

Sterling: I have to ask, so I picked up skiing about a decade ago. My husband is a big skier. Is there a particular ski destination that is still on your bucket list? If you had perfect combination of time and calendar alignment, where would you go?

Karlsgodt: I have the luxury of having been able to go all across the West. I suppose if there was a place that I haven't gone yet that I'd like to try, it is Japan. We've had a couple of our colleagues here at Baker that have been there recently and had great things to say. And the big difference this year from Japan to North America is Japan has snow. So that helps.

Sterling: Yeah, they've had a lot of snow in Japan this year.

Karlsgodt: But I'm a little bit spoiled because in addition to living in Colorado, I have a son that goes to school in Montana and I'll be out in Big Sky next week skiing. So, I'm looking forward to that.

Sterling: And to tie this into your litigation piece, what is harder to predict, the outcome of a litigation or a mountain weather report?

Karlsgodt: Oh, that is a tough call. I'd like to say for me personally, I can predict better what is likely to happen in a lawsuit. But I have some really good weather people that I rely on to tell me when the powder day is coming.

Sherman: I think the last question we have as we wrap up is, what is something you tell every in-house counsel to pay attention to right now?

Karlsgodt: Cyber insurance. A lot of these risks are, as I said before, you can mitigate them, but you can't avoid them entirely. And so, one of the things that is really important is having good full-some cyber insurance coverage that is appropriate to the organization. Not all of the types of privacy cases that are out there right now are covered by all insurance policies. Although there are insurance policies that will cover a lot of even the web tracking and customer data collection cases. You just have to have a very good broker that'll help you find the right choice. But one of the things that we do see over and over again is a company that's been sued in one of these creative, novel privacy cases that comes to us saying, our cyber insurer denied coverage, and so we don't have any insurance to pay for this.

Sherman: So long story short, not all first-party or third-party cyber policies are created equal. The question is, how can a business go about trying to pick a suite of policies and endorsements that is best aligned to their needs? Any experiential wisdom to lend there?

Karlsgodt: Get a really good broker that specializes in cyber. Not all brokers are created equal either.

Sterling: Well, thank you, Paul, for joining us. I was hoping that David was going to ask you some questions about dogs, but he didn't get there.

Sherman: I didn't, I was waiting for the opening. I didn't hear it.

Karlsgodt: We'll leave that for the next one when we talk about forensic reports.

Sherman: And privilege and everything else, which by the way, I have a lot of thoughts on.

May: If you have any questions for David or Nichole, their contact information is in the show notes. As always, thanks for listening to BakerHosts.