Podcast Transcript

The Data Economy and You: Privacy Litigation Trends: Meta Pixels, Cookie Opt-Out, and Sale of Data

Date: November 14, 2023

Guests: Jeewon Serrato, Bethany Lukitsch, and Matthew Pearson **Host:** Amy Kattman

Run Time: 17:25

For questions and comments contact:

Jeewon Serrato

Partner
San Francisco
T: 1.415.659.2620 | jserrato@bakerlaw.com

Bethany G. Lukitsch

Partner
Los Angeles
T: 1.310.442.8856 | blukitsch@bakerlaw.com

Matthew D. Pearson

Partner
Costa Mesa
T: 1.71.966.8882 | mpearson@bakerlaw.com

Kattman: BakerHostetler is excited to bring you a three-part podcast series, The Data Economy and You. You might have heard the term data is the new oil. In this podcast series, we'll be taking a look at how the recent U.S. privacy laws are revolutionizing what it means to sell data; how data should be governed and managed by retail and tech industries in particular because of these new requirements, and what businesses can do to identify and mitigate against regulatory enforcement and litigation risks. I'm Amy Kattman, and you're listening to BakerHosts.

On today's episode, we'll dive into these privacy litigation trends with partners Jeewon Serrato, Bethany Lukitsch, and Matt Pearson. Jeewon is co-leader of the Group's Digital Transformation and Data Economy team. Bethany is co-leader of the Class Action Defense Practice team, and Matt is a member of the Group's Privacy and Digital Risk Class Action and Litigation team. Welcome to the show, Jeewon, Bethany, and Matt.

Serrato: Thanks for having us, Amy.

Lukitsch: Glad to be here.

Pearson: Yep. Happy to be here.

Kattman: Jeewon, let's begin with you. What do you think are the hot litigation trends in privacy today?

Serrato: As we talked about some of the revolutionary changes in the privacy laws landscape in the first podcast, I think what we're noticing in litigation and regulatory enforcement is that privacy is really, I think the expression that I have heard is privacy has grown up. It is not about best practices anymore. It is not about industry guidelines. A lot of the laws that have passed in the last three years have made some of the disclosure and notice requirements so explicit and technical and granular. And because of these disclosure requirements, the notice requirements in several of the states in the United States, the companies are really trying to grapple with what they say on their website about the collection of data and how the data is used.

Because of that, I think, litigation has also picked up. Litigation has picked up in really testing those statements that are publicly made. So, what information is collected? Is consent required for that collection? Is that particular way that the data is used within the consumer expectation? Those are the kinds of bedrocks in privacy related questions that we have been testing for a while. What is different with the litigation trends today is that now the companies have, on the one hand, the disclosure requirements for meeting the compliance with the laws and on the other hand, you've got the litigants and the private plaintiffs testing whether those notices are indeed true. We're seeing that trend in regulatory enforcements, as we hinted at during the first podcast, with the regulators testing whether what you say is indeed happening in the use of online tracking technologies and the question about sale, but we're also seeing that in the world of other types of technologies that are in digital assets on the websites and mobile apps.

Kattman: Thanks, Jeewon. Bethany, if privacy teams and e-commerce operators are looking solely at privacy statutes to avoid litigation risks, are they covered? Or are there other statutes or tools that they should be thinking about?

Lukitsch: So, unfortunately for the in-house privacy and legal teams, simply looking at the privacy statutes isn't enough. So, the recent AG settlement of $93,000,000 that came out in the last month is a perfect example of other statutes that could come into play. In that case, the California AG pursued claims under California's Unfair Competition law and False Advertising laws. And quite honestly, any state's consumer protection laws and false advertising laws could be added to a privacy claim, particularly those involving use of an e-commerce website because the websites are used to, quite honestly, advertise the products. If we're speaking about regulatory enforcement, Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices is another statute to consider.

So, one of the biggest trends we're seeing in the privacy space are actions under the various states' wiretapping laws, and actions under the Video Privacy Protection Act. The wiretapping laws in most states relate back to the 1950s and the Video Privacy Protection Act was passed in 1988 in conjunction with Robert Bork's confirmation hearings. Neither of these statutes were ever intended to cover Internet activity, let alone the sophisticated technology that we are now seeing used on various different e-commerce sites such as session replay, pixels and cookies. But I think because most of the privacy statutes that exist don't provide for a private right of action outside of the data breach context, we're seeing plaintiffs' lawyers become very creative. These claims are particularly scary because they're still being brought against companies who could be 100% compliant with those U.S. privacy laws.

Finally, we're seeing various different common law theories alleged in litigation. Simple theories like fraud and negligent misrepresentation. And as Jeewon alluded to, if you are making certain representations in your privacy policy, they need to be accurate. For example, if you told me I could click this button and you would opt me out of use of that particular technology, you need to make sure that that opt out is actually working. Otherwise, you could be subject to these very simple theories.

Kattman: Matt, to expand on Bethany's response, what other laws are being used by plaintiffs in privacy litigation cases?

Pearson: There really is no limit to the types of laws plaintiffs' counsel are using in privacy class actions. Some, obviously, are privacy-related. Others, like Bethany mentioned, were never intended to have anything to do with privacy or not intended to apply to what they're being applied to. Litigation and particularly privacy litigation, is a game of whack-a-mole. Defense attorneys like me, we defeat one claim and plaintiffs' counsels come up with a new one.

That said, we are seeing some trends in privacy litigation. First, to the extent that any statue has a statutory damages provision, and that is a provision that allows for automatic damages per violation, plaintiffs are going to sue under them. These include, but they're not limited to, California's Confidentiality of Medical Information Act, often referred to as the CMIA. That carries with it a statutory penalty of about $1,000 per violation. Same with California's Consumer Privacy Act, between $100 and $750 per violation. And like Bethany mentioned, the Video Privacy Protection Act, that one comes in at about $2,500 per violation. We're also seeing claims under various state right of publicity acts which, like we discussed, probably doesn't apply here, but if they have statutory damages, they are going and are being asserted.

Second, there are various tort claims, and these include invasion of privacy, bailment, breach of fiduciary duty, breach of confidence, negligence, negligence per se, could go on and on and on and on. Many of these claims are dead in the water when it comes to certain types of privacy claims. For example, invasion of privacy generally requires an affirmative disclosure, and we know that in cyber-attacks there is no affirmative disclosure. But that doesn't stop plaintiffs' counsel. The way they look at it, every time they assert a claim, it is another attempt to expand the jurisprudence and give them an opportunity in the next class action.

Third, we're seeing contract and quasi-contract claims, like breach of contract, breach of implied contract, and unjust enrichment. These claims, unfortunately, are generally pretty easy to plead and therefore pretty hard to defeat on the initial motion. Whether that is a motion to dismiss in federal court, or a demurrer in California court. We've had some pretty good success establishing that statements made in a company's privacy policy are not actually contractual promises, but the Catch-22 there is it generally depends on what is in the privacy policy, and the more a company wants to boast about what they're doing, the more likely they are to get hit with one of these claims.

Thus, while most privacy class action complaints fall with the same basic outline, they are limited really only by the plaintiff counsel's creativity. As privacy class actions progress through the courts, so too will the claims inserted in these actions, and we're seeing that now.

Kattman: Thanks, Matt. Jeewon, why do you think there is this recent focus on the use of online tracking technologies?

Serrato: As Matt said, I think the litigation trend is really favoring the claims where you have automatic damages and it is easy to plead. And if you look at the use of online tracking technologies, because of these recent disclosure requirements that came online, it is easy to test. It is easy for the plaintiffs to say what you are saying on your website in terms of the use of online tracking technologies seems to be deficient, or seems to be deceiving, or seems to be faulty in some way. And so, you're really going to start to see the litigation claims come in where they are looking to, and as Bethany and Matt said, it doesn't have to be a CCPA violation and a lot of these lawsuits are really not in a pleading CCPA. It is pleading 30, 40, 50 years in old laws going back to UCL claims and false advertising and deceptive claims. And so, these theories are not new. They're applying it to this particular technology because in the past, this type of use of technology on the website may not have been the biggest litigation risk, right? This is a new risk. And as Matt said, it is playing whack-a-mole, and maybe in the next couple of years it will be something else. But for this year and for the near, foreseeable future, what we see is that there is a healthy demand for the plaintiffs to test how third parties are engaged in what kinds of cookies, and pixels, and online tracking technologies are deployed, and whether that use is within the consumer's expectation, and whether that transfer of data is amounting to what some of the plaintiffs will argue is wiretapping. So again, it is this healthy dose of skepticism and misunderstanding of how these online checking technologies work combined with how easy it is to bring these lawsuits.

Kattman: Bethany, what are the potential benefits or efficiencies you see in web tracking technologies?

Lukitsch: Something we debate in litigating these cases is always, what is the harm to any particular plaintiff or claimant? Why does it matter if any cookie drops that shouldn't drop? Or, what is the harm associated with any given pixel? Claimants often only think of the negatives, the diminishing of the control of their data or autonomy over their information. But I think one thing that is often overlooked are the efficiencies and benefits of these tracking technologies. For example, some of these tracking technologies, they save time. They save time when you go to look for certain products. For example, sometimes those products just show up on your browser or show up in your social media. And they also can lead to more competition and lower barriers to entry in the marketplace. And therefore, that has a great consumer benefit of potentially lower prices. So, I think there are a lot of benefits of these technologies that have to be taken into account when you're looking at the harm associated with potentially an extra cookie or a tracking technology being on a website.

Kattman: And Matt, as our final question, what are the practical implications for companies when they're faced with these privacy litigation claims?

Pearson: Truthfully, and I don't think this is going to come to, as a surprise to anybody listening to this, but it really is a scary world out there right now. With the ease with which companies can get new technology and implement new technology, and quite frankly, the overall engagement companies are experiencing on their website, one foot fault, one minor foot fault can result in significant litigation exposure.

Quite frankly, it reminds me a lot of the call recording litigation that we are seeing taper off now. I had a case where the company thought they had done everything right in the right disclosures, the right notices. Turns out one of the disclosures didn't make it on one of the toll-free telephone lines, and because the company was receiving so many calls which, quite honestly, is what companies want, right? Customer engagement. But because they were receiving so many calls, the litigation exposure was immense.

But in terms of actual practical advice, I think I would say just slow down. It is so easy to go fast right now. Companies want to know how their customers are engaging with their website. They want to know how to leverage the information they have on customers to better tailor the customers' experience. I know companies want to identify and take advantage of every growth opportunity, and they should. But they just need to do it the right way. Taking the time on the front end really makes a big difference. Working with experienced counsel and advisors. Making sure they're getting the information they want, but in a manner that complies with the law. Doing those things while at times can be time-consuming, it really can avoid a lot of headaches down the road, not to mention a lot of litigation costs and expenses. There is a right way to do it and, quite frankly, there is really no reason to make plaintiffs' counsel's job any easier here.

Serrato: And I love working with Matt and Bethany on these issues because from my perspective on the advisory side, it is incredibly valuable to have litigators that understand the technologies, that understand the compliance requirements. And so, for us on the advisory side, we reach out to the litigators to keep in mind what are the hottest litigation trends and I think that conversation has to be two ways. I think we're seeing more and more that on the client side, when you get a piece of litigation, when you get a claim, a demand letter, sometimes the litigators are not talking to the privacy team or vice versa. Maybe the privacy team is not talking to the litigation team and so, on our side at BakerHostetler, we try to connect the dots that we are really connected to help think through some of the compliance requirements while keeping in mind some of the litigation risk as well.

Kattman: Thank you, Jeewon, Bethany, and Matt.

Serrato: Thank you, Amy.

Lukitsch: Great being here.

Pearson: Yeah. Thanks, Amy.

Kattman: If you have any questions for Jeewon, Bethany, or Matt, their contact information is in the show notes. Join us next week as we close out our series by answering the question, what is personal data worth? As always, thanks for listening to BakerHosts.