Podcast Transcript

2023 DSIR Deeper Dive: Pixel & Other Website Technologies

Date: September 27, 2023

Guest: Melissa Bilancini & Alexander Vitruk, **Host:** Amy Kattman

Run Time: 18:30

For questions and comments contact:

Melissa Bilancini

Associate
Cleveland
T: +1.216.861.7094 | mbilancini@bakerlaw.com

Alexander Vitruk

Associate
Seattle
T: +1.206.566.7092 | avitruk@bakerlaw.com

Kattman: Managing digital assets requires the efforts of the whole enterprise. The 2023 issue of the Data Security Incident Response Report, or the DSIR, includes more content than ever regarding the data ecosystem and how companies can best manage their digital assets as they move through the life cycle of data. The DSIR, of course, dives deep into the annual incident response trends and analytics our clients and friends depend on. It also covers topics such as global privacy, ad tech, the increase in litigation, healthcare privacy and compliance, and the latest in emerging technology. I'm Amy Kattman, and you're listening to BakerHosts.

We are back with the Deeper Dive series covering key topics in this year's DSIR. On today's episode, we discuss Pixel and other website technologies as it relates to hospital websites. Our guests today are Melissa Bilancini, an associate on the Privacy and Digital Risk Class Action and Litigation team, and Alex Vitruk, an associate in the Litigation Practice Group. Welcome to the show, Alex and Melissa.

Vitruk: Thank you very much. Glad to be here.

Bilancini: Thanks for having us.

Kattman: To begin, Alex, could you tell us what is Pixel litigation, and how does it impact hospitals?

Vitruk: Absolutely. So, let's start with the big picture. Third-party online analytics tools, that is really what it is all about. Like many businesses and website operators, hospitals often deploy third-party analytics tools. What is that? It is essentially source code on the website that analyzes certain data. And why use these third-party analytics tools? Hospitals use them in order to do things like measure browser traffic, to increase awareness of their websites, ensure website optimization for the various patient service offerings, provide healthcare information to the public generally.

And recently there's been a proliferation, and when I say proliferation, that is not exaggerated. It is not a euphemism. There have been very many class action lawsuits alleging that through these analytics tools, hospitals actually disclose patient identities and online activities without their knowledge and consent. PII and PHI, personally identifying information, personal health information, that is really the focal point of these types of cases.

So that is healthcare Pixel litigation in a nutshell. These cases tend to involve similar facts to one another, but there may be some important factual nuances, such as some cases focus on patients only. Others focus on users of the website more broadly. Some cases involve just the public website portion. Others involve the secure patient portal. These are the sorts of distinctions that can really impact the litigation. They can really impact, as we're seeing, the nature of the claims for purposes of evaluating pleading arguments or dispositive motions, the size of the putative class, best arguments in opposing any motion for class certification. Those kinds of things.

The jurisdiction where the case is filed also matters. It may impact whether statutory or nominal damages are available, as those are factors that really impact the potential exposure of the case. So, for instance, the Wiretap Act claims and the Medical Information Act claims typically allow for statutory damages, as we've seen ranging between $1,000 and $5,000. And sometimes they're even framed in terms of being available per violation, under California's wiretapping act, for instance. So, this creates potentially significant, if not, frankly, potentially catastrophic litigation risk for healthcare providers. So, it is a really big deal. And these are some of the things that we've been seeing in these cases.

Kattman: Melissa, what trends are you seeing in these Pixel litigation cases?

Bilancini: Sure. So as Alex mentioned, there's been a proliferation of this litigation around the country, and it is still being filed as we speak in both state and federal courts. Our team is litigating in at least 15 different states right now, including Florida, Massachusetts, Ohio, and Pennsylvania.

Vitruk: That is really a lot of states, Melissa. I don't mean to interject, but it is, I know this firsthand because, well, you know it too, because we litigate these cases all over the country. But it is still jarring to hear those statistics. I mean, it is a lot of cases. Are there any particular hotspots for Pixel litigation?

Bilancini: Yes. Actually, we've seen California is a big hot spot. Our team has over 25 cases in California alone, and we believe this is likely because several California statutes allow statutory damages of the, a variety that you mentioned before. But despite the growing number of cases, there is limited precedent regarding the potential for liability.

None of these cases have gone to trial yet, and we're not aware of summary judgment or summary adjudication rulings in any cases. Often, motions to dismiss will dispose of some claims but not all cases. Some dismissed claims might include contract claims based on website privacy policies or notices, state law privacy claims alleging unauthorized disclosures of patient information, Wiretap Act claims at both the federal and state versions of those laws alleging intercepted communications, and a variety of other claims, including those based on statutes that have traditionally targeted computer hacking under criminal codes.

However, recently a Southern District of California court granted a motion to dismiss a hospital website Pixel case in its entirety. In that case, the plaintiffs brought claims for common law and constitutional privacy violations, breach of fiduciary duty, and statutory claims, including state wiretap act claims. The Court held that plaintiffs could not maintain their claims based upon a theory that sharing browser activity on a public website was a disclosure of sensitive medical information, and we hope to see similar rulings like this in the future.

In addition to motions to dismiss, another inflection point in healthcare Pixel litigation is at class certification. But there are only two class certification rulings that we're aware of at this point, both in state court, one in Washington granted class certification, while one in Maryland denied class cert.

There are also three settlements that we're aware of to date. The first, in Massachusetts state court was settled for $18.4 million; the second, in Wisconsin state court, was recently granted preliminary approval of a $2 million settlement; and, actually, just this week, a Wisconsin federal court granted preliminary approval of a $12.25 million settlement.

Vitruk: That is such a wide range. Are these settlements based on similar circumstances, or are they pretty different from one another? Or is it just the case that some lawyers are better at negotiating than others?

Bilancini: Well, the parties in the room can certainly impact the outcome of negotiations. But if you look at the Massachusetts case with the $18.4 million settlement versus the other two, there are some differences. In that case, the parties briefed a preliminary injunction motion. They also briefed a motion to dismiss. And those

parties had engaged in discovery pre-settlement. So, all of that briefing and all of that action led to higher attorney's fees and a higher settlement overall.

The other thing that impacted these settlements is the size of the class at issue. In the $2 million settlement in Wisconsin, for instance, there was a much smaller class, less than 500,000, versus the other two settlements. The Wisconsin one for $12.25 million had a 2.5-million-person class, and the $18.4 million Massachusetts settlement had a 3-million-person class. So, the more people that there are, the larger the settlement will be.

Kattman: Alex, in your opinion, what are the most important considerations for hospitals facing website Pixel litigation?

Vitruk: Of course. So, let's start with motions to dismiss. They've been successful in disposing of certain claims depending on the particular allegations in the complaint and the controlling law. So, for instance, multiple courts have held that HIPAA-required privacy notices cannot form the basis of plaintiffs' claims. Rather, these are notices that are just merely provided to patients in order to comply with federal law.

Another argument to consider is whether plaintiffs have alleged specific contract provisions that a hospital defendant allegedly breached. And these related considerations can also impact arguments like, is there mutual assent? Is there consideration? Things like that. And also consent. So, have plaintiffs consented to the alleged analytics practices? For instance, just one Ninth Circuit decision has affirmed dismissal of plaintiffs' claims on the ground that plaintiffs' consent to those analytics and data disclosure practices barred their statutory and common law privacy claims. And courts have also dismissed intrusion upon seclusion privacy claims, finding that plaintiffs have failed to allege that hospital defendants obtained any patient data.

Other defenses may depend on the precise statutes involved and the facts alleged. For instance, courts have rejected statutory claims requiring disclosure of medical information where none was actually identified. And additionally, courts have dismissed state consumer protection act claims for failure to identify damages sufficient to state and identifiable laws.

As for statutory wiretap-related claims, and those are very common in these types of cases, and depending on the precise wiretap act at issue, whether it is federal or a particular state wiretap act, hospital defendants have been successful in defeating these claims by arguing that, for example, if it is a one-party consent statute, as parties to the communications hospitals cannot be held liable for interception. The wiretap acts' criminal or tortuous conduct exceptions do not apply. Some statutes do not have a private right of action.

Some successful arguments have involved hospitals not being, quote, electronic communication service providers because hospitals provide healthcare services to the public. They are not necessarily in the business of providing an electronic communication service. And plaintiffs have also failed to establish that the

contents of any communications were transmitted. And lastly, that any interception occurred or that any interception occurred in transit. That is the holding of an important case within the Ninth Circuit.

Lastly, hospital defendants may find that plaintiffs' claims are subject to binding arbitration and/or class action waivers, and this may also form the basis of the successful motion to compel arbitration and/or a motion to strike class allegations.

Bilancini: Alex, some might say that these cases all deal with the same third-party source code, and thus it is the same facts and the same legal issues. Is that the case?

Vitruk: In theory, perhaps, but in practice it is a totally different beast, so to speak. So, like I said earlier, key differences can involve, is it just patients, or is it users of the website? Is it just the public website, or is it the patient portal? What are the claims involved? What is the jurisdiction? Who is the opposing counsel? Who is the judge? Both procedurally, administratively, and legally on the merits, all of these cases can really significantly differ from one another, and those distinctions may be really important in successfully litigating a case.

And then finally, before I hand it over to Melissa to discuss class certification and motion for summary judgment, plaintiffs have also brought motions for preliminary injunction at the outset. And these motions have been mostly unsuccessful because plaintiffs can always disable the collection of their data through various opt-out tools, or they can refrain from using the hospital website at issue. So now, I'll flip it over to Melissa to discuss class certification and motion for summary judgment.

Bilancini: Thanks, Alex. So, class certification is a critical stage in class action litigation in general and that is no different in these cases. When opposing class certification, hospitals can raise a number of arguments to support a conclusion that issues are too individualized to support class treatment. For example, the way that class members use hospital websites can vary. They might visit for different reasons. I might be on there to make an appointment for my daughter or for myself. They might visit different pages. Their browser settings and device settings might be set differently. For instance, I might only use VPN, but you, Alex, maybe you accept every cookie, and you never delete any of them. So, all of that can play a role in what information is shared and who the actual class member is.

Hospitals may also argue that plaintiffs' damages theories are unreliable. Hospitals may argue that theories of damages don't reflect the economic realities of users' interactions with websites or that damages theories don't fit within the plaintiffs' class-wide claims. Additionally, depending on what is learned during discovery, hospitals might be able to argue that the named plaintiffs do not actually represent the class because their claims are subject to unique defenses.

As I mentioned before, we're only aware of two healthcare Pixel class certifications to date. For the decision that denied class certification, the court found these types of arguments to be persuasive and how the individual issues

predominated over common issues of law. The court also held that the plaintiffs were raising novel questions under state law, and so their claims were not suited for class certification.

Motions for summary judgment are also a very important tool that defendants can have. As noted, we're not aware yet of any summary judgments or summary adjudication rulings in hospital website Pixel cases. But from a merits standpoint, hospitals might consider arguing whether patients consented to the use of analytics technology and to what extent. Whether that technology was deployed within the online patient portal, as opposed to just on the public-facing website, because that is not often the case, and it can also be case-dispositive.

Hospitals might also want to consider arguing whether state law prohibits the disclosure of specific information that was allegedly disclosed, and they could also consider arguing the precise information that was disclosed and to whom, among other considerations.

Vitruk: So, Melissa, should litigants consider whether to move for summary judgment at the same time as opposing class certification?

Bilancini: Absolutely. As you know, motions to dismiss are based on the plaintiffs' allegations. So, until either class certification or summary judgment, the court does not necessarily have a clear understanding of the underlying facts. So, summary judgment can be a way for hospitals to educate the court about the use of third-party source code.

Also, these cases have not yet resolved on their merits, so there are many questions regarding what a trial would look like, competing perspectives on what the technology is and does. And given the legal burdens, we think that it would be prudent to consider moving for a summary judgment at the same time as class certification, because it gives you an opportunity to dispose of the case in multiple ways and to give the court the grounds to do so.

Kattman: Alex, as my final question, what do companies and hospitals need to know in order to mitigate the risk of these lawsuits?

Vitruk: Absolutely. So, often the best litigation strategy is to mitigate the risk of litigation in the first place. And some examples of how that can be done in these cases or to prevent these cases is, for instance, to conduct an investigation into the use of any analytics technologies on the website, first and foremost. So, are the technologies being used at all? What types of technologies in particular? On what portion of the website, if any? Is it on the secure patient portal? To what extent? Questions like that will be very important to have a full understanding of what is actually going on.

Evaluating the privacy policy or the notices in place, as well as any consent mechanisms, is also very, very important because as we know, these cases will often either reference or even rely on the language in certain policies or notices or even terms and conditions on the website. And so even though virtually all

hospitals have these notices and these terms in place, the allegations basically focus on, are they sufficient? What is the particular language? Is the consent mechanism clear? And so being able to look at that comprehensively is very important.

And then finally, receiving advice on the best compliance practices in light of the law and the litigation landscape. That may involve hiring competent counsel, basically to understand what is really going on as developments in the law happen on a lightning-fast basis, and it would definitely be prudent to stay apprised of the most recent developments in the law.

Kattman: Alex and Melissa, thanks so much for joining us today.

Vitruk: Thank you very much. We appreciate it.

Bilancini: Thanks very much for your time.

Kattman: Thank you, Alex and Melissa. If you have any questions for Melissa and Alex, their contact information is in the show notes. As always, thanks for listening to BakerHosts.