Podcast Transcript

2023 DSIR Deeper Dive: Plaintiffs' Attorneys Are Trying to Assert a New Cause of Action Against Universities Based on an Old Law Regulating Videotape Service Providers

Date: October 24, 2023

Guest: Ben Wanger and Joel Griswold

Host: Amy Kattman

Run Time: 16:34

For questions and comments contact:

Ben Wanger

Counsel
Philadelphia
T: 215.564.1601 | bwanger@bakerlaw.com

Joel Griswold

Partner
Chicago
T: 312.416.6238 | jcgriswold@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're back with the Deeper Dive series covering key topics in this year's DSIR. On today's episode, we discuss recent litigation targeting the Higher Ed industry, specifically privacy litigation and the VPPA. Our guests are Ben Wanger, counsel with the Digital Risk Advisory and Cyber Security team, and Joel Griswold, partner with the Privacy and Digital Risk Class Action and Litigation team. Welcome to the show, Ben and Joel.

Griswold: Thanks. Excited to be here.

Wanger: Thanks for having us. I'm happy to be here.

Kattman: Ben, let's start with you. Could you tell us what are the current trends that you're noticing in the Higher Ed industry regarding incidents that include privacy litigation and data breaches?

Wanger: Sure. There is three current trends that we're really seeing. The first is that ransomware is, as always, a big issue that affects Higher Education. I think one of the things about ransomware and Higher Education that is different than a lot of industries is whereas personal information is important and it is something that would trigger notice, I think what is really worrisome to Higher Education and to these universities is their research data, and they have a lot of sensitive data that really they, could cause a lot of problems if that data gets out in the public, and their ability to operate. If the university goes down, the effects of that could go very deep and a lot of people could be affected. Another current trend we're seeing are laws related to ransomware. One state, North Carolina, has issued a law banning all state entities, including public universities, from even negotiating or paying ransoms. So, whereas that is really limited to North Carolina now. Florida has a similar law, but that law carves out universities. But I think the bigger take-away is, is that laws like this are being considered. So at least for public universities, there is a trend where they are needing to focus more on putting themselves in a position where they wouldn't need to pay a ransom in the future because their ability to pay a ransom could be somewhat questionable. And the third trend is with litigation. We are seeing a large increase in litigation arising from data breaches and especially where there is a university that is kind of a big name, that will pique the interest of plaintiff lawyers, and we are seeing much more litigation than we saw in the past.

Kattman: Ben, where are the universities struggling?

Wanger: So, I think there are three issues, or three areas where universities are struggling in the instance of data breaches. The first one, and a lot of companies have this issue, is knowing exactly what data they have, and where the crown jewels are located. In Higher Education, especially in research universities, data is often spread out, meaning not everybody knows what everybody else is researching.

So, in the event of an incident, there is a lot of scrambling to find out where the important data is and how it was protected. So, one of the things that we always encourage universities to do is, as best they can, start trying to figure out exactly where they are most vulnerable, where their pressure points are, and where their important data is, and by knowing that, they can take steps to protect that data. So, hopefully they won't be in a situation where that data is getting out.

And another area where universities are always facing tension is in messaging. Universities generally pride themselves in transparency and communicating as much as possible but oftentimes in ransomware or data breaches, communication is not always beneficial. Frankly, first of all, if you're negotiating a ransom, sometimes you can give leverage to the threat actors if you're communicating too much. And second of all, it takes time to get all the information. We don't have all the answers right away. And that is often contrary to a university's way of thinking of they want to overcommunicate. So, a lot of times we find ourselves working with universities to balance that need for transparency with making sure that they're not overcommunicating too early and risking saying something that may not turn out to be accurate.

And the last area that I see some universities struggling is in the process and decision-making in the event of these incidents. Often times there are so many people with co-equal authority that there are questions about who is responsible for deciding certain things. So, I think, making sure that they can nail down that process in advance is very helpful for universities. So, in the event that an incident occurs, they know exactly who is responsible for what decisions.

Kattman: Ben, why do you think this industry, in particular, has been target?

Wanger: So, I'm not sure that they're being targeted, per se. In 2022, as we wrote in our DSIR, Higher Education matters accounted for about nine percent of the cyber security incidents that we saw. I think that number will go up significantly in 2023. But I think the reason that we see a lot of universities that are falling victim to these incidents is universities, by design, have an open infrastructure. If you liken a computer network to a house, they have a lot of windows and doors because they have a lot of different people who are accessing the network. And I think it is not surprising that they're more likely to have one of those windows and doors cracked open, which allows a threat actor to get into their environment. And also, these universities have a lot of data. So, when the threat actor gets in, there is a lot of data that, to be taken, and a lot of it is sensitive data. So, I think that makes them attractive to these threat actors. And then finally, universities have a lot of stakeholders. There are a lot of people who notice when something is wrong in the university, whether the systems are down or when the university is sending out a notice letter. And I think that makes them, it makes their pain points much more obvious to threat actors, which I think, once they get into the system it makes them eager to exploit those pain points.

Kattman: Thanks, Ben. Joel, will you provide our listeners with an overview of privacy litigation, specifically the VPPA?

Griswold: Sure. So, what we've been witnessing really over the last year and a half, two years, has been pretty much an all-out, full-scale war on the Internet that's been waged by the plaintiffs' bar. What they're essentially doing is trying to take old statutes and old theories of tort law and apply it to new technology that clearly wasn't contemplated when statutes or common law causes of action were originally recognized. And specifically, what they're doing is taking a look at what pixels are being used by various companies on their websites and what information is being allegedly transmitted to ad tech companies or ad companies like the various large social media companies that are out there, for instance.

So, the Video Privacy Protection Act, or the VPPA, is one of these battles that is being waged. And the VPPA was a statute that was passed back in 1988 and really, in response to Judge Bork having his family's video rental history being obtained and then disclosed by a media outlet in an attempt to, I guess, embarrass him or vet him during his Supreme Court confirmation hearings. So, in that context, it was clear this statute was really meant to apply to brick-and-mortar traditional video rental chains that we all, I think, remember fondly and have since ceased to become a major industry. The statute itself applies to videotape service providers and that basically means, or is defined to mean, any person engaged in the business in or affecting interstate or foreign commerce of the rental, sale, or delivery of prerecorded video cassette tapes or similar audio-visual materials.

Now, we've seen a wide range of defendants being sued under the VPPA, everything from restaurants to retail to not-for-profits. Really, it's been a pretty broad range of industries that's been hit. And the case law recently has been kind of, I think, trying to clarify what it means to be a videotape service provider. And at least one case has acknowledged that it is, you really need to be a business that is centered, tailored, or focused around providing and delivering audio-visual content as opposed to just having video that is part of your brand-awareness campaign and is included a website.

But again, plans are continuing to try to push the theory that unless notice and consent has been given separate and apart from anything in a policy or terms and conditions, and the defendant has pixel on their website in a way that communicates information about the subject matter or the title of the video to any ad tech company, then that company is allegedly in violation of VPPA. That is theory that they're continuing to pursue, and it hasn't just been against Higher Ed, we've seen some Higher Ed institutions sued, but we've seen a, really, a broad spectrum.

Kattman: Joel, what outcomes have you seen recently in VPPA cases?

Griswold: Well, I think at the outset of these, this pixel theory of liability, we saw a fair number of courts denying motions to dismiss, and really denying them on the basis that defendants have been challenging what was being disclosed or whether it was being disclosed, and in support of those arguments, have been attaching declarations and information that was extraneous to the complaint. So, courts were reluctant to grant motions to dismiss at the outset, opting rather to let

these cases proceed to discovery and then maybe summary judgment. But what we've seen recently has been some courts willing to dismiss cases based on a couple of different theories.

One is that the defendant isn't truly a videotape service provider as defined in the statute. And two, is that the plaintiff isn't really a consumer as defined in the statute. And consumer means basically any renter, purchaser, or subscriber of goods or services from a videotape service provider. And courts have basically said, hey, it is not enough to be a subscriber or, for instance, a rewards member of a company where your subscription or membership doesn't afford you access to video content above and beyond what a member of the general public would be entitled to. So, it has to be consumption of video by virtue of your subscription, not just, I'm a subscriber or rewards member and I've consumed a good from this company that is completely separate and apart from any video that they may have watched just as a member of the general public. The courts have not gotten into the more factual issue about whether what is being disclosed is PII or whether it is even being disclosed by the companies at all, or whether, in fact, it is being disclosed by the plaintiff's own browser settings. Those are, again, issues that we're waiting to see rulings on, but I expect in the next year we're going to start to see those trickle in.

Kattman: Thanks, Joel. As a final question for you, Ben, how can universities exercise best practices moving forward?

Wanger: So, I think there is three things they can do. The first one is work on knowing where their vulnerabilities are, and where their pain points are. And that entails, again, knowing what your crown jewel data is. Where is your most important data? And again, that is much easier said than done. But I think by taking inventory of that you're helping yourselves immensely. First of all, once you identify the most important and sensitive data you have, you can take additional steps to protect that data. Also, you can put yourself in a position where in the event of any incident, you know where to look to make sure that certain data is or is not involved. And I think along the line of what Joel said with the VPPA is knowing what data you're getting. Making sure that if you are collecting data from websites that you know you're doing that because whether that is something you should or shouldn't do, I think making sure that you know what you are collecting will help you. So otherwise, you're apt to be surprised.

I think another thing that universities can do is start developing a messaging strategy in the event of these incidents. Because, like I said, that is a difficult area for them because it is so important to universities to be transparent with their communities. So, I think, thinking about how you are going to message in the event of an incident would save a lot of headaches on the back end.

And finally, just working on the process, making sure you develop an incident response plan that really calls out who is in charge of what and what steps need to be taken in the event of an incident would prevent and alleviate a lot of that early chaos that occurs once you find out something is wrong. And one of the best ways once you have that plan is I would say practice it. Practice it with

tabletop exercises, because I think once you start developing that muscle memory, the process becomes much less chaotic and tends to go much more smoothly.

Kattman: Thanks so much for joining us today, Ben and Joel.

Griswold: It was a pleasure. Thank you.

Wanger: Yep, thanks for having us.

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