Point Two Workplace Privacy Podcast Series: Biometric Privacy Risks in the Modern Workplace

(This transcript was generated through AI technology.)

Karla Grossenbacher
Hello everyone, and welcome to the Workplace Privacy Podcast, where we discuss employee facing privacy issues that arise at the intersection of technology and employment law. I'm your host, Karla Grossenbacher, and I'm the head of Seyfarth's National Workplace Privacy and Biometrics team. I'm here today with Paul Yovanic. Paul is one of our rock star litigators at Seyfarth who specializes in litigation under, among other things, Illinois' Biometric Information Privacy Act, otherwise known as BIPA. Paul, welcome to the podcast.

Paul Yovanic
Great. Karla, thank you for having me.

Karla Grossenbacher
I'm excited to have this conversation with you, because you and I have worked together over the years on various compliance matters for biometric privacy but I want to talk with you about what you're seeing in biometric privacy litigation. But I guess I feel like we can't have a conversation on a workplace privacy podcast that's debuting in June 2025 without talking about the new law that's coming online in Colorado on July 1. So I guess the headline on that one is that employers who collect biometrics from workers in Colorado are going to have to have a written policy and get consent prior to collection. So Paul, what's your take on the new law in Colorado? I know you've been keeping your eye on it.

Paul Yovanic
Yeah. So, so, I think, to start, I think, you know, the good thing here is that the policy and the consent can be as a condition of employment. So we can start advising clients to start getting that in place and having it as the condition of employment. It's going to be a very interesting law that, as Karla, you said it, it'd be effective July 1. There's a lot of questions. There's a lot of things still up in the air, of, how is this going to be enforced? What magnitude - the statute does not have a private right of action, so the plaintiff's bar is not going to be as focused on it as they are, for example, the Illinois biometric Information Privacy Act. And so where we kind of see is we're not going to have our companies ignore biometric privacy laws that don't have a private right of action, because we still don't want to be sideways with various Attorney General's Offices.
But we have to kind of start figuring out - this might take some time. What does the Colorado Attorney General's office, who is going to be enforcing this addition to the Colorado privacy law, what are they focusing on? You know, for example, Texas has a biometric privacy law that's enforced by the Attorney General's Office. And as far as we're aware, they have not gone after businesses using, for example,

biometric time clocks. We have seen them go after the Googles, the Facebooks, for various biometric information that's being captured collected some facial recognition stuff. I think back in 2022 Facebook and Instagram disabled their, like, dog face features and all that, because that captured biometric information. Obviously, that was because there was the big target by the Texas Attorney General's Office. And therefore would that be similar to what we're going to see in Colorado? So we'll have to see.

Karla Grossenbacher
Right. Yeah. I mean, it looks very much like the Texas AGs office is going after the big headline companies, make big splashy press releases and things like that. So hard to say whether Colorado is going to approach it the same way or be more rigorous about protecting employee privacy in particular, or maybe just going after business targets like the AGs office. And, yeah, obviously no private right of action. But of course, you're right there in Illinois, where we do have a private right of action.
For those listeners who don't have all the background, there's just a handful of states who have biometric privacy laws, by which I mean a law that comprehensively regulates how you collect and store biometrics, and Illinois is the only one that has a private right of action. So Paul's been in the thick of it there, litigating, and I know that until now, most of those lawsuits have been about sort of gotcha action saying, hey, you forgot to get consent, written consent before you collected the biometrics, which is surprising, because the law has been around since 2008 so why didn't everyone know about it? But obviously I would think people know about the consent piece by now. So where do you see litigation under BIPA shifting, given that most employers have those consents in place now.

Paul Yovanic
Yeah, so, you know, I think, Karla, as you point out the statue was enacted in 2008 in Illinois, and we didn't see much activity in it until 2016, 2017 and really the best way to describe how BIPA has been weaponized, I will say, is an old statue on new technology. In 2008, there was never this expectation, at least, and not, in my view, that it was to safeguard against employers using biometric time clocks. In fact, BIPA was enacted in 2008 following the bankruptcy of a company called Pay By Touch, which, at the time, allowed consumers to link their finger scan to their credit card. Well, when Pay By Touch filed bankruptcy, Pay By Touch listed as one of its assets a database containing the biometric information of its users.

Karla Grossenbacher
That's crazy.

Paul Yovanic
Yeah, it really is. And so what we're looking at is now fast forward 10 years after its enactment, and all of a sudden, there's a more widespread availability of biometric time clocks, not something you saw available, readily available or affordable in 2008 the way it was in 2017, the way it is today. Very affordable for businesses to manage their time, keeping systems that way. And so, as you know Karla, it was very easy for a lot of the plaintiffs' bar to go after these cases where there was no notice, no policy, companies didn't even know about it. Fast forward to 2025, unless you're living under a rock, you're aware of BIPA's requirements in Illinois, and you're aware that it requires a policy, a written consent.

Now I think where we're going to start seeing the shifts is in two different ways. I think in the first bucket, it's going to be the sufficiency of the notice and consent. The consent requires you, or the notice requires you, to disclose how this information is being captured and collected, for what purposes, how it's being stored, in what manner it's being stored. You don't want to find out that you just put all this in to check boxes under BIPA, and that you're not storing it the right way, that you're not- that you're disclosing it to a time clock vendor, for example, is where we see some of these lawsuits, or we see some of these issues arise. And so what it's a key from a compliance perspective, whatever you're saying, you're doing in the policy, whatever you're saying when you're asking for a written consent, you're actually doing it.

Karla Grossenbacher
Yeah, and I think when we talk about all of the requirements that go in the policy that you're saying people have to, you know, make sure they're living up to… I talk to clients even outside of the states that have biometric privacy laws, outside of Illinois, where you're required to have that policy, and I say, look, even if there's no law, there's such a thing as invasion of privacy and collecting someone's biometric information without their consent, I think would be a good claim of invasion of privacy. And what I also tell people is, if you are going to get someone's consent again, even in these states without a law, you've got to provide all this information about what you're collecting, what you're doing with it, how long you're going to keep it, because that's the only way you're getting informed consent. If you don't tell people all of that stuff, you know, the consent, in my view, isn't really worth the paper that it's written on. Do you agree?

Paul Yovanic
Well, yeah, absolutely. You're going to have a tough time convincing a trier of fact that someone knew what they were giving up their you know, biometrics for if you're not disclosing it. So, I mean, if you're not disclosing the purposes, and BIPA in Illinois requires that. And again, you know, when we advise clients on how to be compliant with BIPA, I mean a lot of times we're saying, Hey, we put this in your draft consent forms. Are you actually doing it? If you are, let's make sure. And sometimes you get clients that will say, well, that's actually a good question. Let us go back and just confirm. Because again, don't want to find out that we have this consent form, and then the question is the sufficiency, and then you find out you've been deceiving employees by not doing what you're saying you're going to do. It's absolutely a concern. And I think until now, it was very low hanging fruit for the plantiffs' bar to go after just companies that did not have a policy and a consent in place. I mean, it's very easy, absent various exemptions under the statute. If you don't qualify for one of those, it's hard to argue that you're not liable. And so, but, but obviously I think the plaintiffs bar is going to want to keep BIPA up and going, and so it's going to be the sufficiency in one, in one instance be the sufficiency of the of the consent form.

Karla Grossenbacher
And tell our listeners a little bit about those exceptions, especially ones that might be available to employers.

Paul Yovanic

Sure. So there's various exemptions that fall under BIPA including a healthcare exemption, where if biometric information is used for healthcare purposes. That was a recent decision by the Illinois Supreme Court in *Mosby vs Ingles Memorial Hospital* in 2023 came down that if you're using in furtherance of healthcare operations, it is exempt from BIPA. Now that case solely focused on the use of on the cell or a Pixis machine, a medication dispensary system. The court there expressly said we're not making decisions beyond that, and you can read between the lines. It meant we're not saying whether or not health care time clocks in hospital settings is exempt. They didn't close the door to it, but they were only analyzing it based on certified questions to the Illinois appellate court, and then ultimately the Supreme Court, related to those medication dispensary systems. So that's an exemption. We have financial institutions exemption, if you are subject to certain reporting under the Gramm-Leach-Bliley act. We also have state contractor exemption, where, if you are a state contractor providing services pursuant to a contract you are exempt, that is subject to certain issues on appeal currently. But those are exemptions that we always look at on top of also union preemption under the LMRA. That was recent decisions over the last few years from the Illinois Supreme Court and the Seventh Circuit US Court of Appeals. And so generally, when we're looking at cases, and we're taking cases in, we do look at all of these exemptions to see where can our clients and prospective clients fall under these exemptions, because it helps with the fights against these cases, where sometimes there might not be a policy, sometimes there might not be a consent, or sometimes the consent form on its face isn't even sufficient. We need those abilities to fight back, otherwise it can be an uphill battle.

Karla Grossenbacher
And you were saying earlier about how employers could be, you know, accused of deceiving their employees if they're not accurately describing what the technology is doing, like the time clock. But I find when I talk to clients, it's not really - like deceiving, you know, would have an intent to it. A lot of them, I think, just don't fully understand the technology that the vendor is providing them. Do you see that on the litigation side?

Paul Yovanic
Yeah, I think there's, there's often a time where they just expect that based on what a, for example, like a time clock vendor gives them that, you know, everything's compliant, just as it's received. I think there's always been those exceptions or expectations, and I think we're starting to see more communication from time clock vendors and everything to make sure that there's compliance in place, which is why you're not seeing the mass number of filings that we've seen in five years prior in BIPA litigation under time clocks. Now, I think the other thing, though, the component is there are other things than time clocks that are covered under BIPA, especially in the employment context. I think we get into different types of technologies.
So I think, you know, it's different types of technologies. You know, I think the misconception for a lot of clients is that BIPA only relates to time clocks, because 95 plus percent of BIPA cases are time clock cases. So when you start thinking all of a sudden like, oh, driver facing cameras that track distracted driving, well, how is it doing that? Arguably, it's capturing some facial geometry that is capturing whether or not someone is drowsy, whether or not someone's looking off the off the road, and those can arguably be issues to consider under BIPA.
There's also issues of voice, voice command and voice print. Sometimes security features where we have computers are opened through voice print. We have, you know, headsets that are operated and

controlling things via voice print. And so I think that those are things that we always want to triage with clients of, okay, you're using this but - and sometimes in specific areas, in industries, logistics industries, for example, use a ton of driver facing cameras. And so anytime we're talking with a logistics company, it's, what are you doing inside the driver's cab? Do you have any of these features? And sometimes it's, oh, yeah, we are using something, or we're going to use something like this. And then we have the conversation about, well, until someone's going to show me otherwise, I think that there's some facial geometry that's being analyzed here. And facial geometry is a buzzword in Illinois' BIPA, and so we do have to have those conversations. And so anytime you're using someone's voice, face, iris, you know, hand, palm, anything that can identify them based on a feature, and it's a unique feature, you should be thinking about, does this come under one of the biometric privacy laws, especially Illinois' BIPA, with a private right of action. And if it does, we need to have those discussions.

Karla Grossenbacher
Right. And you know, facial geometry is an identifier listed in the other biometric privacy laws certainly would come up under common law invasion of privacy. I was actually talking to my kids last night about biometrics, and one of them was asking me to explain to them, like, what is a biometric identifier? How would someone operate and get your voice. And when you mentioned driver facing cameras, I often have people calling me about driver facing camera to talk about just the GPS aspect, like, is it okay to track people by GPS, which almost it is if it's a fleet vehicle. But they're not even thinking about, Oh, my goodness, it's actually capturing the facial geometry of the driver. And we need to have a discussion about biometrics. And they're like, What do you mean? I'm not collecting biometrics, just our face and camera.

Paul Yovanic
Yeah. I mean, you have a lot of clients that are in tune with the geo tracking, with the tracking of GPS, and just, you know that they're on top of that, and they're great, they feel great about that. But then it's like, okay, but what else does this technology, Is this technology doing? Oh, it'll tell us that a driver is drowsy, right? Well, how do we think it could be doing that? And so then all of a sudden, you see the, you see the questions of, well, maybe we should look into this technology a little bit more beyond the tracking softwares and technologies that are in the cab. So I think it's just more of, if there's one takeaway is, with other areas of biometric privacy, is just keep an open mind of if it's capturing and detecting something on your body, you should be mindful, or at least have an initial reach out of, hey, is this something I should be concerned about, or is this something that I don't have to worry about? We see it every day. We're always advising on various different technologies. And new technologies are coming up, new ways of accessing systems, secure systems, secure entryways, driver safety, all sorts of stuff, aside from just the time clocks that we've been dealing with for the last five, six years now.

Karla Grossenbacher
Absolutely. Yeah, it's a brave new world, Paul, that's what it is. Well, listen, it's been an absolute pleasure having you on the podcast today. Thank you so much for being here. I know our listeners have learned so much from you today. So thank you very much.

Paul Yovanic
Oh, I really appreciate it. I look forward to the next podcast and what you come up with next, Karla.

Karla Grossenbacher
Great. Thanks, Paul.