Podcast

Tech Tools + Privacy Considerations

By Joseph J. Lazzarotti & Damon W. Silver

January 16, 2025

Meet the Authors

Joseph J. Lazzarotti

Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com

Damon W. Silver

Principal
(212) 545-4063
Damon.Silver@jacksonlewis.com

Details

January 16, 2025

"It's this constant sense of governance — risk and compliance processes that should take place whenever you're dealing with these technologies. If there was one goal I would recommend for next year, that would be more collaboration between the stakeholders [IT, legal, HR, the business area deploying the tech] when rolling out these kinds of tools."

Listen on Apple Podcasts

YouTube

Transcript

INTRO

Welcome to We get work® and the Year Ahead 2025 podcast series. This year, our special report and corresponding podcast series are created to help you move forward steadily, seamlessly, and successfully in a workplace law environment in persistent flux. Jackson Lewis invites you and others at your organization to experience the report's legislative, regulatory, and litigation insights in full at our website, JacksonLewis.com or listen to the podcast series on whichever platform you turn to for compelling content.

CONTENT

Damon W. Silver
Principal, New York City

Hi, everyone. Thanks for joining us. My name is Damon Silver. I'm a co-leader of the Privacy Data and Cybersecurity Group here at Jackson Lewis. I'm here today with Joe Lazzarotti, the other co-leader of the group. What we wanted to do today was quickly run through some of the key trends that we saw in 2024, and then gear up for 2025 with a focus on various areas where we expect to see new developments in the new year.

Joe, for starters, as we take a look back at the year that we're wrapping up right now, one of the things we saw a lot of was an increased focus on litigation. Do you want to talk a bit about some of the key trends that we've been seeing?

Joseph J. Lazzarotti
Principal, Tampa

Sure. First, it's good to be here with you, Damon, in New York. I haven't been to the New York office in a while, so it's good to be here.

We definitely have seen, from a standpoint of privacy and data security litigation, a significant uptick. There was a while there where we weren't seeing class action data breach cases unless the number of people affected was in the six or seven figures. That number has come down, and the number of suits, as a result, has pretty dramatically increased. In some cases, some numbers they've quadrupled between 2021 and 2023. We don't see any signs of that slowing.

There's also been a significant uptick, as those who are watching this stuff have been seeing, which is these website tracking pixel-type claims that have been brought under a range of theories, including the CIPA statute in California, the Video Privacy Protection Act, and a whole host of others, including in Florida and certain other states. That has remained strong with a lot of novel theories like 'Trap and Trace' and others that we've seen. Then, of course, some of the decisions that have been handed down have been pretty interesting to follow.

The other area that we've seen that continues to be strong, even with a pretty significant decision that has helped companies that collect biometric information, is the Biometric Information Privacy Act in Illinois. The decision held that we're not having to count violations at the per instance that the biometric information is collected but per individual, which keeps the potential damages pretty low. Those claims are continuing along with another type of privacy statute in Illinois, which many of you may not have heard so much about, which is the Genetic Information Privacy Act. That's a little bit more nuanced, but it has very much the same type of damage opportunities for plaintiffs with more dollars in the amount that can be recovered than we see under BIPA.

That's what I'm seeing, Damon, but any thoughts there?

Silver

It's interesting, Joe because you mentioned that on the data breach class action front, we weren't generally seeing a lot of cases brought unless a huge number of potential plaintiffs were impacted, and that has drastically changed. We have some cases now where as few as a thousand people were impacted.

On the privacy front, as an organization trying to assess risk, you really were more concerned about potential regulatory investigation than litigation risk, and that seems to be changing as well. Even though some of the new state privacy laws that we're about to talk about, Joe, don't necessarily create a private right of action in most instances. What we're seeing is that the plaintiff's bar has become very creative in taking laws that weren't necessarily intended to regulate privacy and security and leveraging them for that purpose.

Joe, this would be a good time to jump into some of these state privacy laws, because we do have several that came online in 2024. We had seven states whose laws went into effect in 2024. We have a whole bunch more coming online in 2025. We are seeing a mixture of both regulatory enforcements. Also, we anticipate various claims being brought by the plaintiff's bar based on laws that they are repurposing to try and get redress in this area.

Lazzarotti

You're right about a lot of the state privacy laws that do not have a private right of action.

Then, we go back to looking at some of the litigations brought under HIPAA, for example, where it also doesn't have a private right of action. However, some cases have held that you can still use the standard of what's required under HIPAA as a basis for basic negligence claims, implied contract claims or others. What you're required to do, from a compliance perspective, even though there's not a private right of action, if you violate those rules, could still be framed in litigation that might result in some liability. Of course, there are other hurdles that a potential plaintiff would have to get through, but you certainly still have some litigation risk as well as, you were mentioning, Damon.

Thinking about HIPAA for a minute, in the last few weeks, there were several pretty substantial penalties that were announced by the Office for Civil Rights relating to breaches that had happened involving protected health information. So, you're getting it from both ends. You're getting the litigation risk, but also the regulatory enforcement risk.

Thinking about these state privacy laws, there are now about 20 or so states that have them. The states are going to begin to get their legs underneath them in terms of how to regulate and what to enforce. As we're seeing, like for example, Damon, I think it's a big issue for a lot of our clients. I know we've talked to several of them about this whole idea of data minimization, something that comes from the GDPR. It's also just a general common-sense part of the safeguards and practices that organizations should be thinking about but maybe talk about that a little bit.

Silver

Absolutely, Joe.

The CPPA is the newly created agency that enforces the CCPA. Its very first enforcement advisory focused on this issue of data minimization, which essentially means that you need to be cognizant and thoughtful about what data you collect in the first instance and how you use that data, whether you disclose that data, how long you retain it. The trend had been before there were these new privacy laws in the last five years or so, to assume that it was always good to have more data, to collect more data, to hold on to more data because you just didn't know what uses you might put it to. Now, with the widespread adoption of AI, that mentality, at least from the business standpoint, might hold even more true because now there are ways to analyze these huge data sets and potentially leverage benefits from them.

But from a data privacy and security perspective, both because of this new requirement under the CCPA and GDPR and other laws to be focused on data minimization, but also from the standpoint of managing your data breach risk, we've been talking with a lot of our clients about whether they need to do some type of data mapping exercise to get their arms around the data that they have, where it's coming from, what they're doing with it, how long they're keeping it and, in many instances, start to take purposeful action to try and minimize their

footprint. It's not unusual for Joe and I and other members of our team to be helping a client with a breach where the data that's impacted, much of it hasn't been used for any purpose in quite a while. Sometimes, it goes back 10 or 20 years. The client didn't even realize they had the data. Meanwhile, under data breach notification laws, it doesn't matter that you haven't been doing anything with the data. You are still maintaining it and you still have an obligation potentially to notify people and report.

To Joe's point about these laws serving as the standard for handling of data, given a data minimization requirement. If you are now in litigation because you had a data breach, even if you perhaps had a decent argument that you had some reasonable safeguards in place from the standpoint of endpoint detection and response, data backups, encryption and stuff like that but it comes out through discovery that you just were collecting and maintaining way more data than was appropriate for disclosed purposes. That could be a place where in looking at whether you complied with the standard of care, you could lose out even though you've made this huge investment in your cybersecurity.

This segues into the next point I wanted to talk about, sort of an offshoot of data minimization, or at least a component of data minimization, is not just looking at the data that you are maintaining in your own systems but also looking at the whole ecosystem of data that the various vendors you engage to collect and process data for you are holding onto. Because we've seen a number of ways how not having a tight handle on that vendor risk piece can end up thwarting otherwise best-laid data protection plans.

Lazzarotti

That's exactly right. It ties in also to the idea of what trends are we seeing in the market in how businesses are conducting certain operations, both on the commercial side and the employment side.

Regardless, businesses rely on third-party vendors. That may not necessarily be a Social Security number, but it can be a name and an email address. It can be a name and a biometric. It can be a name and activity on a dash cam. Or it can be a performance management platform that a business is using to see which applications is an employee going in and out of. Which for CCPA purposes, that still is personal information, typically. The question becomes how do you figure out where all that data is? Who's responsible for it? What kind of obligations has the company pushed onto its vendors to say, hey, if we reach out to you, we need to know what data you have, how it's going to be maintained, why is it being maintained, and if it's not for a legitimate purpose anymore, if we don't have a need for it?

There may very well be a good need to retain data, but if not, there's a good reason to try to begin to think about how do we have a process in place to get rid of that data and only retain what you need? That’s a challenge, but it's something that I think we're going to probably see more of as we go into these expanded data privacy frameworks that now many, many state legislatures have pushed through.

It does tie into a lot of the AI tools that we're seeing on these performance

management platforms. We're seeing in some of these same use cases, the use of employees' and customers' image and likeness, and the technology that enables that to happen comes with some risk of misuse. That trend of using image, sound, voice and voice recognition in some ways can be a benefit when it comes to advertising, promotion and authentication. But it also enables bad actors to use those things to commit crimes and to hurt organizations. We're seeing a lot of use as deep fakes to hurt organizations. We're seeing companies trying to figure out how do we balance the need to advertise, to promote their services, to help get more customer outreach with their websites, but without running into claims that they haven't made the proper disclosures, haven't gotten the right consents?

How are you seeing your clients work with their marketing people? Because I see a lot of silos. I don't know if you see that, but sometimes one group in the company may not be sure about what the company did on its website. So, they then have to figure that out.

Silver

That's a great point. The class action litigations and the demand letters we're seeing alleging these violations of CIPA and the Video Privacy Protection Act and other claims based on the use of various website tracking technologies have forced an internal discussion for a lot of organizations around the communication between legal, compliance and marketing. For a long period of time, there wasn't really enough of an impetus to have that discussion. Similar to the point we were discussing earlier with data minimization, there was a tendency to say, yeah, if we can add more trackers to this site, we can get a better understanding of what people are doing on the site, where they're spending their time and where they came in from. That's just going to help us with our marketing efforts. We're going to be able to be more targeted. Here in the U.S., there was not, in the way that there was in the EU, this framework in place to require stuff like getting a cookie banner up and making detailed disclosures about what you were doing.

But because so many of these website-tracking-based claims have been brought, all of sudden, many organizations, especially those that are doing pretty active digital marketing, have to start looking at the costs out of the equation, too. Because if you are doing tracking, particularly using trackers that result in disclosures to many of the third-party digital marketing vendors, and you haven't gone through the process of creating a detailed cookie policy and getting your banner up, you're a sitting duck. When you get these demand letters from some of the key plaintiff firms in the space, they really know they've got you. You don't have a defense, and it's just a matter of how much you're going to pay to make them go away. You might be able to make that particular plaintiff and firm go away for a little while, but there are many others out there.

What we're seeing a lot more in our discussions with clients is a more collaborative approach where there is recognition of the fact that these tools serve a lot of value. No one's advocating for getting rid of them altogether, but there are thoughtful programs that can be put in place to help keep track of what's being collected, make sure what you're collecting is actually serving you, and then making sure, from a legal compliance standpoint, that you're making the

disclosures and you're offering the rights that you should be offering.

Joe, as we turn the calendar to 2025, one of the things that you and I have discussed is an interesting development, is the increased compliance burden that a lot of HR departments are going to be facing.

For a long time, employee data didn't need to be safeguarded. There were some restrictions around, say, the collection and use of medical information in connection with administering leave or accommodations. But a lot of the new privacy laws we were seeing, with the exception of the CCPA in California, had this carve-out for employment data. So, a lot of HR professionals and employment counsel were not necessarily feeling the need to dig deeply into a lot of the new privacy laws. The CCPA, as I mentioned, did change that calculus to some degree because the exemption for employment information sunset at the end of 2022.

But now with some of the new AI laws we're seeing, there's the Local Law 144 here in New York. Illinois has issued some new guidance and amendments around the use of employment information and HR tools. Colorado has an AI act, the E.U. has an AI act. It seems like one area where this is going to be felt in a way that some of these other privacy laws have not been is in the HR space because of all the information that companies are collecting about their employees and the various ways that they want to use it to make consequential decisions about the people that will potentially work for them or do work for them now.

So, you want to speak a little bit to that, Joe?

Lazzarotti

It's funny; I mentioned I am in the New York office today with you, Damon. Before we came to your office, I passed by and saw Cliff Atlas. We were talking about some of the stuff that he's doing in his group. A lot of great work on restrictive covenants and non-competes. We just got to talking about how crazy it is when an employee leaves the company and, in the process, takes a whole bunch of data. A lot of times, there's not a lot of time to figure it out. You don't know exactly what they took. Oftentimes there's a belief that it doesn't include personal information. It really was just a bunch of business data. Years ago, the whole idea of data breach notification used to be, and it really still is largely, largely, but not entirely, an issue of unauthorized access or acquisition of personal information.

Well, since that time, we've seen statutes, regulations, contractual obligations, like the reporting obligations under the SEC, which says, hey, look, if you've had a material breach. Some of the insurance rules came from the model cybersecurity law from NAIC, which says if some breach of data affects your systems or your ability to operate. Some of these situations where employees take a lot of data or deleted a lot of data could trigger some of those obligations. They also could trigger contractual obligations that a business may have with customers. In the employment context of trying to deal with that restrictive covenant issue, you may still have data privacy issues.

Not only HR departments, but organizations as a whole realize how critical managing human capital is in an organization and all of the data that employees

have access to. Whether you're talking about the data collection that's needed for AI to be effective, trying to figure out how do we comply with CCPA and how employees use these tools. Whether we think about what the processes are and how employees are affected or employee or commercial data in the business of minimizing that data of customers. There's this whole range of things that have to be thought through when employees are charged with managing what is becoming and has been, I suppose for a long time, big data and how important data is in an organization. So, the HR function really has to be mindful, not just of, hey, this is your benefit enrollment information, and it's really sensitive. It's how do we get our workforces to be more in tune to the importance of managing this important and critical asset of the organization, namely data information.

That's where I'm seeing, Damon, a lot more of a bigger role in the years ahead for HR departments to help minimize company risk as well as to manage better HR compliance.

Silver

I'm seeing the same thing, Joe. In part because the New York City law was one of the first to come online, and also because it has this more limited focus that people are more able to more easily wrap their heads around using the tool in connection with hiring or promotion decisions. Some organizations are still getting up to speed with the fact that making employment decisions with these tools is only one piece, and probably the smaller piece, of the puzzle.

The bigger piece is employees are going to be using these tools in lots of different ways. They're going to be using the tools whether an employer introduces certain approved tools, which is certainly the approach we'd recommend. Even for organizations that don't think they have introduced tools proactively to their workforces, people are still going to find them. They're going to use ChatGPT. They're going to use Claude. Even just doing a Google search now triggers Google's AI functionality.

One of the things that we've been talking to clients a lot about is how, as with the website tracking technologies, to leverage the benefits of this new technology that's not going anywhere. It would be a fool's errand to try to avoid it altogether and prohibit employees from using it. How to leverage it in a thoughtful way that is not going to create huge exposure. We are regularly having conversations with clients who are seeing all these unintended pitfalls of the use of AI without Guardrails.

For example, Joe, I recently was talking to a client who had some employees who were using an AI note taking tool. The AI bot would join every meeting that they held over Teams or Zoom. It seemed great. It would take a transcript of the meeting. It would send out action items afterward to everyone who was invited to the meeting. The problem was this tool, just by default, starts recording the second that the meeting is started by anyone. So, there was a situation where a couple of the first people to join the meeting were just chatting. One of the things they were chatting about was the frustrations they were having with another member of the company who was one of the other invitees to the meeting, but who wasn't on the call yet. The meeting then officially starts and goes forward. No

one thinks anything more about it. Then, when the meeting ends, a transcript, including that first part where they're bad-mouthing their colleague, gets sent to everyone. There's like 10 people who get this. Obviously, that creates all kinds of employee relations headaches. You can certainly imagine a situation where instead of trashing their coworker, they were talking about their recent medical procedure, or they were talking about something related to their religious beliefs or their sexual orientation. There are all kinds of extraneous information that could be collected through the use of these and other tools.

Also, from a litigation standpoint, the cost of ESI when you have to go through all these transcripts that are now being created or all the chats that an employee is having with a bot during the course of working on a project. There are lots of different second-order-effect impacts of the use of these tools by employees if the company hasn't been thoughtful about how to structure that use and how to maintain the resulting information.

It's something to think about. It's not going away. There are lots of new tools. An interesting discussion to have is what features the tools offer. Do you want to allow employees to use all those features? Are there safeguards built in audit logins so that you can see who accesses certain documents through their use of an AI tool? It's an interesting puzzle for a lot of organizations to put together. How do we get the benefits from these tools, but do it in a way where we're not creating huge problems for ourselves down the line that we're unprepared for?

Lazzarotti

Well, I think we could probably sit here all day and talk about this, right? I totally agree with you. The AI note-taker is a great example. We had a similar issue with an employee using a notetaker, and the call was intended to be privileged. We had to then begin to think about if we save that transcript somewhere other people can access it, does that undermine the attorney-client privilege for that conversation? So that's just one other type of thing.

But to your point, being thoughtful about the implementation, many times these technologies, like many others, including performance management platforms, dash cams and cameras and recording of phone calls, all of those things sometimes often get left to the IT department without really having the benefit of the expertise of the legal department or the HR department to identify these issues.

If I were to say, what's one thing we can really do to look ahead in 2025 for employers is to say, look, let's get people together to talk about these issues. Before we roll out this technology, let's start thinking about some of this stuff and say, look, it's a great tool, but let's make sure we're using it in a way that doesn't shoot ourselves in the foot. That means also doing that on an ongoing basis. What I see a lot of times as a company will do that, that is they'll do the due diligence on the front end when they first get the tool. Then it'll get rolled out and then everybody goes back to their day job, so to speak. Six months later, the IT department will get a call from the vendor saying, hey, we have this new functionality, so let's roll it out. It seems like it makes sense for the company. But the same conversation doesn't happen about, well, what are the implications? How is it used? Where do

we store the data? It just gets rolled out. It's this constant sense of governance, risk and compliance processes that should take place whenever you're dealing with these technologies.

If there was one goal I would recommend for next year, that would be more collaboration between the stakeholders when rolling out these kinds of tools.

Damon, it was great presenting with you as always. Good to be here in the New York office. Hope everybody had a wonderful holiday season, and we look forward to everything that's going to come in 2025.

Silver

Great seeing you, Joe.

OUTRO

Thank you for joining us for The Year Ahead 2025 special edition podcast series. Please tune to future episodes, where we will continue to tell you not only what's legal, but what is effective.

Our We get work® podcast is available to stream and subscribe on Apple, Spotify, and YouTube, as well as JacksonLewis.com. If you enjoyed these episodes, we encourage you to share any or all of them with your network and leave a review to help others find us.

We would love to hear your suggestions for future topics, or if you're interested in being a guest on our show. Please reach out to us at Wegetwork@JacksonLewis.com.

Thank you for tuning in!

Return to The Year Ahead 2025 Report