Podcast

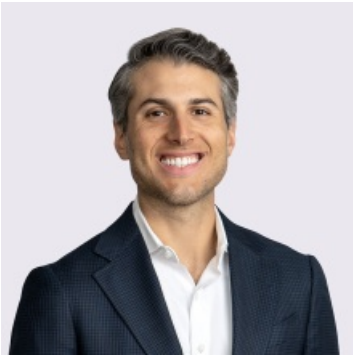
2023 Mid-Year Report: Data Privacy

By Mary T. Costigan & Damon W. Silver

July 24, 2023

Meet the Authors

Mary T. Costigan
Principal
908-795-5135
Mary.Costigan@jacksonlewis.com



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

Related Services

Privacy, Data and Cybersecurity

Details

July 24, 2023

Jackson Lewis P.C. · 2023 Mid-Year Report: Data Privacy Update

Listen on Soundcloud
Listen on Apple Podcasts
Listen on Spotify
Listen on pandora
Listen on Google Podcasts
LISTEN ON libsyn
Listen on STITCHER

Transcript

Alitia Faccone:

No matter the month or year, employers can count on one thing, changes in workplace law. Having reached the midway point of the year, 2023 does not look to be an exception. What follows is one of a collection of concise programs, as We Get Work™ the podcast provides the accompanying voice of the Jackson Lewis 2023 Mid-Year Report. Bringing you up-to-date legislative, regulatory, and litigation insights that have shaped the year thus far and will continue to do so. We invite you and others at your organization to experience the report in full on JacksonLewis.com, or listen to the podcast series on whichever streaming platform you turn to for compelling content. Thank you for joining us.

Damon Silver:

Thanks for joining our midyear podcast on key data privacy and security issues. My name is Damon Silver and I'm a principal and the firm's New York City office and a member of the firm's privacy Data and cybersecurity group. I'm joined today by my colleague Mary Costigan from our Berkeley Heights office, who's another member of our core group.

Data Privacy and Security is a wide-ranging and fast moving area, and Mary and I spend much of our time working with clients to develop strategies that enable them to continue pursuing their business objectives without assuming unacceptable levels of data privacy and security risk. To give our listeners a sense of the areas that are of greatest concern to our clients, both in the near term as well as in the longer term, Mary and I are going to talk through four of the most frequently asked questions that we've been receiving. The first of those questions, Mary, is we're seeing a lot of

states passing new privacy laws. I think we're up to 10 states now that have comprehensive privacy laws on their books. How do we as an organization figure out if we're subject to some or many of these laws, and what are our best options for coming into compliance efficiently and effectively?

Mary Costigan:

Hey Damon, so you're right. This is a frequent question that we're hearing from clients. Since the CCPA was enacted, the California Consumer Privacy Act, for those of you who aren't familiar with the CCPA, a at least 10 other states have enacted comprehensive consumer data protection laws, and that number continues to grow. So the good news for employers is that these laws, unlike the CCPA, don't apply to applicant or employee data, but for those companies that still need to know whether these laws apply to their consumer data, well, the test is a little different from the test for the CCPA. The test for companies doing business in these states is not revenue, but the number of residents from whom they collect personal information. So to be subject to these state laws, you have to collect the personal information of state residents in excess of a certain amount.

Depending on the state, this may be the data of 50,000, 75,000 or even a hundred thousand residents, but if you sell the PI or the personal information of residents, a different test will likely apply. So aside from this test, these laws are otherwise very similar to the CCPA. They all require providing notice of your data collection activities, including data protection language and your vendor agreements, performing data protection impact assessments, and also providing consumers with rights to access or even control use of their data. There are a lot of new consumer data protection laws out there, but the good news is there is a significant overlapping in terms of compliance. So clients should be able to leverage their data mapping, their notices, their policies, and even practices for compliance across these state laws with some targeted tweaking. So Damon, I have a question for you. What's the deal with all these class action lawsuits we're seeing that relate to website tracking technologies and how does this relate to data protection?

Damon Silver:

Yeah, great question, Mary. So for advertising, marketing, site maintenance and a variety of other purposes, many organizations are using technologies on their websites that track what pages users visit, what they click on, what they search for, what videos they watch, and what they say in chats and using other communications tools. In a lot of cases, with a lot of the clients we've spoken to, they don't even necessarily realize that some of these technologies are in use. For example, they may have been installed by a vendor or a marketing director years ago and are still on the client site even though no one is actively using the information collected or they're not aware that they're using the information collected by these tools in any event, and we're also seeing a lot of instances where our clients may be aware that they have certain tracking technologies in use in their site, but they're not familiar with the full capabilities and functionalities of these tools.

Particularly, they may not be aware that some of these tools are not only collecting data from users, but also disclosing that data to third parties, such as firms that provide targeted advertising services. Somewhat cleverly the plaintiff's bar has

picked up on the fact that the use of these technologies may violate federal and state wiretap laws, which for those not familiar, prohibit intercepting communications without consent, and that these technologies may also violate protections against invasion of privacy and disclosure of sensitive information. As a result of all this, over the past year or so, we've seen an explosion in website tracking class actions, and it seems by all indications that this trend is gaining momentum.

So one of the things we've been doing with a lot of our clients to try and get out ahead of this litigation risk is we've partnered with a data analytics firm that can scan the client's site to identify what tracking technologies are in use and what those technologies are doing, and then we can work with the client to analyze the associated legal risks and start to develop strategies to better manage that risk. So Mary, sticking with the topic of tracking technologies, a question we get from a lot of clients is that they're interested in using various tracking technologies to track their employees physical locations, the websites they visit, the searches, they run what they're saying in emails. And so I was wondering if you could talk a bit about how these technologies are being used and what are the legal risks that we're working with our clients to navigate?

Mary Costigan:

Sure. So this is an area where we recommend that clients proceed with caution. As you noted, there's a growing interest in monitoring employees, especially with the remote workforce. We're seeing clients use a variety of technologies to do this monitoring. It could be keystroke loggers, screen capture and browser monitoring, GPS, CCTV, and even smart cards. And that's just a small representation of the types of technologies that now can monitor. More often than not, the companies have legitimate interests or needs for doing this monetary, but as I noted before, it comes with significant risks. So proceed with caution, some of that risk. For example, we see a growing number of states enacting laws that regulate employee monitoring. What makes this compliance challenging is if you have employees across a number of states. These state laws vary. They vary by the type of monitoring that they cover.

They vary by the type of notice to provide and how to provide, and also on whether or not consent is required. In addition to state laws, you can have monitoring activities that can create risk if the monitoring actually results in inadvertent access to sensitive information such as an employee's personal email, their sensitive personal information such as a financial or health data, privileged communications with their attorney or even private photos.

So all of this type of access could potentially lead to invasion of privacy claims or even discrimination claims against the company. So you have the state laws that you want to be monitoring. You also have certain monitoring activities that could result in violations of the Electronic Communications Privacy Act. And also if you're monitoring employees communications, this might run a foul of the National Labor Relations Act, and that NLRA protects an employee's ability to exercise certain rights, including engaging in protected conversations about unionization. So there is several factors to be considered very carefully before initiating a monitoring program.

Damon, another topic generating a lot of questions we're experiencing we're

receiving right now is AI. What are the key AI related risks we need to be mindful of?

Damon Silver:

Yeah, so Mary, this is an expansive topic and certainly one that's evolving rapidly. Our AI group, which Mary and I are both members of, has been closely monitoring legal developments in this space. And there are two areas that are coming into focus from an employment perspective. First is use of automated decision making tools to make or assist in making decisions about which employees to hire and to promote. And the second is how to regulate employee use of generative AI tools like Chat GPT. On the first topic under a new New York City law, employers utilizing an AEDT or an automated employment decision tool need to ensure that those tools have undergone bias audits in the past year. They need to publish the results of those audits, and they need to provide advanced notice to applicants employees regarding their use of those tools and also the employers related data privacy and security practices.

We've seen that a number of other jurisdictions are considering similar legislation, and the EEC has made the role of AI and perpetuating workplace biases, one of its focal points. With respect to employee use of generative AI. Some of the key issues we've been discussing with clients are, one, preventing employees from inadvertently disclosing confidential information by entering it into a tool like Chat GPT. Another is employee reliance on information from one of these tools that looks very polished and sounds very credible, but maybe totally false, and there are a variety of intellectual property considerations. And then of course, as with the first issue I just touched on, there's concern about hidden biases in these tools and what that could mean for businesses whose employees are relying on these tools for various work-related functions.

For listeners interested in a deeper dive on these topics, the co-leaders of our AI group, Joe Lazzarotti and Eric Felsberg, recorded a mid-year podcast on this topic, which we encourage you to check out.

Mary Costigan:

Thanks, Damon. So a few thoughts to wrap up. As Damon mentioned earlier, data protection has become such an active space, both in terms of enacted law and litigation. We're hearing constantly from clients about how hard it is to keep up with new developments on top of their daily responsibilities. So we wanted to take this time to help answer some common questions that we think you might have. But we also wanted to let you know that our Jackson Lewis Privacy and Cybersecurity Practice Group, well, we blog frequently about new data protection laws, compliance, best practices, and also trending litigation issues. So please feel free to check out our Workplace Privacy blog. It's on the Jackson Lewis website, or reach out to us. We're always happy to help. Damon, it's always a pleasure catching up with you.

Damon Silver:

Same with you, Mary.

Alitia Faccone:

Thank you for joining us on We Get Work™. Please tune into our next program where we will continue to tell you not only what's legal, but what is effective. We Get Work™ is available to stream and subscribe on Apple Podcasts, Google Podcasts, Libsyn, Pandora, SoundCloud, Spotify, Stitcher, and YouTube. For more information on today's topic, our presenters, and other Jackson Lewis resources, visit JacksonLewis.com. As a reminder, this material is provided for informational purposes only. It is not intended to constitute legal advice, nor does it create a client lawyer relationship between Jackson Lewis and any recipient.