Podcast

We Get Privacy for Work — Episode 6: The Potential Privacy Risks Inherent to Mergers and Acquisitions

By Joseph J. Lazzarotti & Damon W. Silver

July 24, 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

Related Services

Privacy, Data and Cybersecurity

Details

July 24, 2025

To say mergers and acquisitions present significant risk is an understatement; however, additional vulnerabilities are being exposed as bad actors threaten to exploit privacy and data security leaks during the transition.

YouTube

Listen on Apple Podcasts

Transcript

INTRO

To say mergers and acquisitions present significant risk is an understatement; however, additional vulnerabilities are being exposed as bad actors threaten to exploit privacy and data security leaks during the transition.

On this episode of We get privacy for work, we discuss what employers can do to protect client and employee data as they expand their company.

Today's hosts are Damon Silver and Joe Lazzarotti, co-leaders of the firm's Privacy, Data and Cybersecurity Group and principals, respectively, in the firm's New York City and Tampa offices.

Damon and Joe, the question on everyone's mind today is: What steps should employers take before, during and after an acquisition to minimize cybersecurity risks, and how does that impact my organization?

CONTENT

Joseph Lazzarotti
Principal, Tampa

Welcome to the We get privacy for work podcast. I am Joe Lazzarotti, and I'm joined by my co-host, Damon Silver. Damon and I co-lead the Privacy, Data and Cybersecurity Group here at Jackson Lewis. In that role, we get a variety of questions every day from our clients, all of which boil down to a core question—how do we handle our data safely? In other words, how do we leverage all the great things data can do for our organizations, but avoid running into a wall of legal risk? How do we manage that risk without unnecessarily hindering our business operations?

Damon Silver
Principal, New York City

On each episode of the podcast, Joe and I are going to talk through a common question that we're getting from our clients. We're going to talk through it in the same way that we would with our clients, meaning with a focus on the practical. What are the legal risks? What options are available to manage those risks? What should we be mindful of from an execution perspective?

Joe, our question for today is, what are some of the data privacy and security concerns that come up if we, as a business, are thinking about acquiring another company?

Lazzarotti

There is really a lot to think about there because you have to think about this from the standpoint of what kind of data we anticipate the target will have. We have to think about what industry we are in, where there might be some regulatory requirements. We might think about what type of information we want to have and don't want to have. We have to think about, and we can dive into a lot of these issues, but if we're going to purchase equipment from the target as part of the transactions, or part of the assets, if it's an asset deal. We can get rid of some assets and take some assets – what's the status of those? Certainly, you don't want to buy a data breach, and want to understand if it's out of date; what would it cost to get it up to the standard that the company is at? Just understanding that, and really thinking through and making an assessment of the risks in those and other areas, is something that during the due diligence process we would want to assess pretty carefully.

Silver

Absolutely, Joe. You touched on this. Maybe we can dive into it a little deeper, but there are some key questions that you want to ask to try and get your handle on the data privacy and security risk you're potentially assuming. You mentioned one for sure: getting an understanding of the types of data, what legal obligations may attach to that data, and what contractual obligations may attach to that data.

An important one is getting an understanding of the target's record retention practices. Do they have, for example, data in all of their email boxes going back 20 years? If that's the case, you probably do want to get a pretty quick understanding of what might be in those mailboxes. Probably, you want to get a process in place to do some archiving and purging. We have seen quite a few breaches where there was an acquisition, and then some of the data, at least, coming over in connection with the acquisition, was kept in a legacy system that wasn't actively being used. They perhaps had some accounts with administrative privileges, and no one was monitoring those accounts. They weren't running their normal endpoint detection solution on that environment. It was a field day for the bad actors. They just got to go in there and took everything they wanted, completely undetected until they released ransomware or took some other action that finally tipped people off that this breach was happening. In doing the investigation and talking to clients, a lot of times it turns out that there wasn't really even a need to continue to maintain

that data or most of it. It was just there, and something that no one really wanted to spend the time to dig through. It was this massive source of liability just sitting out there.

Joe, maybe you can talk about some of the other dormant liabilities you could run into. Data breach is definitely one of them, but on the privacy side and from some other standpoints, there could be other types of risks that you're not aware of until you've really dug into what the data says and what systems you've required.

Lazzarotti

To give a couple of examples that come to mind, sometimes employees might get copied on an email or save in a shared file, a spreadsheet that has all kinds of information that may not be necessarily relevant to the business. In one case in connection with an acquisition, it was learned after the acquisition that one of the employees of the acquired company had been running their personal tax business out of the company's systems. Then, the company realized that they had tax returns of people. They were like, what is this tax return? What's going on here? They didn't know that. To some degree, it may be difficult to find those hidden treasures that you wind up with, but something like that, perhaps, there's a service. We've worked with some that can run some type of scan to identify data that might be unusual or create some unnecessary risks. That's certainly one thing.

Even in the employment context, we've run into this where the buyer will want to see what the status of the employees is, like, who do we want to hire, what's someone's work history, how many leaves of absence and workers' comp costs do they have? Now, we're talking about the purchase, but from the seller's perspective, they may want to say, well, wait a second, we don't want to provide that, certainly not until the transaction closes. What if we do want to exchange some information during that time? If you decide to share that information, one question is, what are you sharing? Can you disclose that information in the due diligence process? Then, if you do, what exactly are you sharing? A lot of people talk about, well, we'll give you the personnel file. If you haven't had good data practices and kept files separate that ought to be kept separate, you might be sharing medical information, for example, with a party that doesn't have any authority to have that. In effect, you may technically create a breach or a violation of maybe the ADA or even HIPAA. That is a dormant issue in the process of what might be considered a normal exchange of data in anticipation of a deal; you wind up doing that.

Just by the way, for those exchanges of data that do make sense and aren't going to trigger those kinds of things, you still may want to have a due diligence agreement that covers the responsibilities for that data. It's certainly conceivable in the course of carrying out a deal, you may have a data breach. Who's responsible for that? If the deal doesn't go through, what happens to the data? Those are just a couple of examples of some dormant issues that I've run into.

Silver

Those are important ones, and I did want to just drill down on one. It's really a

question to ask in a litmus test in some ways. It's a topic that we talked about on a previous podcast episode, and that's data mapping. If you were going to be acquiring this company, something you want to ask about is, are there data maps? One, if they don't have them, they've never done data mapping. They have no idea what that is, and that definitely tells you something about their data practices. It suggests they do not have a very mature program. If they do have them, you can get, hopefully, a preview of some of these issues that we've been talking about. You can see what type of data assets they've been using to process data and what types of data elements are being maintained by those various assets. You can see some of the safeguards that are in place. You may be able to get some information about retention practices. That could be a very helpful starting point to try and get a better understanding. You will never have a perfect understanding, and there's always going to be some chance for surprise. In looking at data maps and asking about data maps, you at least give yourself the lay of the land and have put yourself in a better position to ask additional questions and to start getting a real handle on what the risk profile is of the acquisition from a data privacy and security standpoint.

Lazzarotti

You talked about sophistication and trying to understand what the target company's approach to data privacy and security is as an indicator of what the risk is. That's really important.

Taking that to a different level, I run into situations, just to use one industry as an example, like in healthcare. If you're a hospital system and you're acquiring a practice of physicians, you may acquire them in whatever form that takes. The physician practice group may just be used to practicing in, let's call it, a less secure environment without some controls that may be viewed as inhibiting the ability to practice efficiently, but in fact may provide better safeguards for patient and employee data. After the transaction closes, and they're now a subsidiary or a wholly owned sub of the acquiring company, how do you now integrate them and avoid creating additional risk? Should there be some compromise down the road because they've dragged their feet in taking steps to secure their environment in a way that's consistent with the overall enterprise? Thinking about that in the deal and trying to do what you can to get some assurances that will take place might be a good thing.

There have been some situations, not just in healthcare, but in others, where the target, after the transaction, now becomes a pretty big liability for the company overall. Understanding the overall sophistication and how to integrate the new company into the organization can come with some challenges, not just at the transaction stage, but even afterwards.

Silver

One other thing to consider, Joe, is that most organizations at this point are using a variety of vendors to process their data. It's not just the systems of the target you need to think about. You also need to get an understanding of what other parties out there are processing data that you, as the acquirer, are now going to be the owner of. There may be a variety of different software providers, contractors and

others who may have either access to or may even be maintaining data that you are now going to own. It's helpful to get a sense of what vetting was done of those parties. Are there data processing agreements in place with them? What kind of risk are you inheriting if you acquire this company?

Tangentially related to that, an issue that I've seen come up a couple of times is that one of the assets the acquirer will acquire is a website. That website might be running all types of tracking technologies, like cookies, pixels, et cetera, that, potentially, if efforts haven't been made to provide proper notice and collect consent, could expose the acquiring company to claims of wiretap violations and invasion of privacy violations. It may be a type of situation where the acquiring company has done some work on its own sites. It has an understanding of what's being run, and a pretty good program in place to address compliance. That may not necessarily be the case for the new website. I've certainly seen situations where there was a lag in taking a look at risk related to the new website, or there's just no plan to even do that – it just wasn't something on the checklist. Particularly since over the last two years, we've seen so many of these website tracking claims being brought. That's another item I think is important to try and take a look at. Since the website is public-facing, it's something that the acquiring company could even do on their own as part of diligence. They can run scans, see what's running on the site and take a look at the site. Is there a cookie banner? How does the privacy policy look? There are some self-help type steps that could be taken to get a general feel for what type of website compliance-related risks might be assumed.

Lazzarotti

You don't think you can just copy and paste the acquiring company's privacy policy and put it on target companies if they remain an entity?

Silver

I don’t think that's the best practice. Now, Joe, you don't recommend that.

Lazzarotti

That’s a great point. Even if there are no tracking technologies and pixels on the site, you're exactly right to be looking at that. Even the internal practices that now these comprehensive privacy laws that you're referring to are obligating companies to really delve into, like what are you collecting and disclosing to whom? What are the sources of the data, and what are your rights? That can get pretty confusing pretty quickly when two organizations come together and have pretty different practices as it relates to that. That’s a really good point.

In any transactions, attorneys’ toolboxes probably may not deal with these issues all the time. They may want to have some specific counsel, whether it's internal at the company or otherwise to really dig into this. Even for a lot of vendor contracts and some of the deal documents we've looked at, the data privacy and security provisions have gotten a lot longer and a lot more complex and it really is a lot to dig into. We've just scratched the surface here.

Damon, did you have any other things to raise, at least at a high level here?

Silver

That's a really good place for us to wrap up. We want to thank everyone for joining us on this episode of the We get privacy podcast. As always, if you have any suggestions for topics we can talk about or any feedback on this episode, please reach out to us at privacy@JacksonLewis.com.

OUTRO

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 to on Apple Podcasts and YouTube. For more information on today's topic, our presenters and other Jackson Lewis resources, visit jacksonlewis.com.