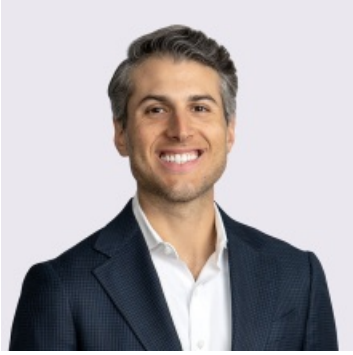
Podcast

We Get Privacy for Work — Episode 5: The Privacy Pitfalls of a Remote Workforce

By Damon W. Silver & Joseph J. Lazzarotti

July 10, 2025

Meet the Authors



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

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

Related Services

Privacy, Data and Cybersecurity

Details

August 1, 2025

Remote work has given employers and employees pathbreaking flexibility, but it has also raised a host of data and employee privacy concerns.

YouTube

Listen on Apple Podcasts

Transcript

INTRO

Remote work has given employers and employees pathbreaking flexibility, but it has also raised a host of data and employee privacy concerns.

On this episode of We get Privacy for work, we discuss what employers must consider when crafting policies and practices for remote workers.

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 can employers do to effectively protect their data and employees from the cyber-related privacy concerns associated with remote work, and how does that impact my organization?

CONTENT

Damon Silver
Principal, New York City

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

Joseph Lazzarotti
Principal, Tampa

On each episode of the podcast, Damon and I are going to talk through a common question that we're getting from our clients. We're going to talk it through the same way we would talk it through with our clients. What this means is that we're going to focus on what's practical. We're going to think about what the legal risks are, what options they have to manage those risks, and what we should be mindful of from an execution perspective.

Damon, our question for the day is, what are some of the strategies for minimizing cyber privacy-related risks for organizations that have a significant remote workforce?

Silver

A good place to start is taking a look at how your remote employees are doing their work. In other words, have you issued all of them a company-owned laptop? Have you issued them company devices? If you are allowing them to use personal devices, do you have some type of mobile device management solution for those devices, because there are a number of risks we can talk about with respect to remote workforces? A lot of them boil down to getting that understanding of the equipment and the technology that those employees are going to use, and what types of safeguards you can put around those uses.

Joe, do you want to jump into it, tackling either the BYOD component or the company-issued device component and talk through some of the key areas of focus?

Lazzarotti

Certainly, when you have employees using their own devices, it raises a lot of issues. Companies, for a while, have gone to a BYOD approach, which makes some sense. You allow the employee to use their own device, and they sign on to that by having a policy that governs how they use the device for company purposes. You might have something that they sign, a policy or some application that they download onto their device, which is where they're able to access company email, calendar and perhaps some other things. That seems to be a fairly typical way of managing that activity, if you have it set up that way.

Even if you have company devices for people working remotely, one of the issues that's come up, just as an example, is that companies supply a company laptop and a company printer or one of these printer-scanner type devices. The employee winds up terminating employment and says, hey, would you mind if I kept the printer, since it is really probably worth nothing? The company's like, sure, no big deal, and they go their separate ways. Then, all of a sudden, you realize that the scanner and the printer have a hard drive and a lot of the documents that were scanned with that device are saved on that device. In other words, even if it's company equipment, you could run into some of these issues. To your point, Damon, thinking about how you safeguard that and what approach to take, whether it's company equipment or employee personal equipment. You run into those things with a remote workforce.

Another issue with this from a privacy perspective is that we're focused on the

privacy and security of the data that's being managed by the employee remotely, but there's also the privacy of the employee. A lot of the struggle is with the fact that people are not in front of you, and there's no face time. All of a sudden, you're wondering, is that person out working in the yard, are they at the beach or are they doing something else and not being active? There are apps that make your mouse move to make the employer think you are actually doing work.

Maybe you can talk a little bit about these productivity platforms and how that plays into the process of managing this remote workforce.

Silver

Absolutely. I have one quick point I want to add on to the last issue we were discussing around the equipment and applications that employees are using. You're absolutely right, even if it's company-issued, you can still run into issues. A lot of those issues center around the degree of control that you continue to have over your data and your data environment.

I've had a number of clients who have had situations where they terminated an employee who was working remotely. They sent that employee a prepaid box to send back their laptop, but the employee, for a while, didn't do it, and we ended up having to send demand letters and do this whole thing. Meanwhile, there were a couple of months that sometimes passed between when the employee was terminated and when they returned the device. In a couple of those instances, the client was in a heavily regulated industry like healthcare. The question became, did the employee continue to access PHI that may have been stored locally on their device or even on the company systems if we didn't cut off their access during that period? Both with personal devices and company devices, you do want to think about what would happen if this device were lost. What would happen if the employee refuses to return it to us? Do we have some way of making sure that we're able to remotely wipe that information? Are we able to see the activity, like do we have logging of the activity on that device in the same way that we would if the employee were working from the office? Your obligations related to your data are just as stringent when the employee is in the office as when they're elsewhere. Sometimes what can change is that you have a lot less control.

Jumping to the point you mentioned, Joe, around the privacy rights of the employee, we have seen a huge increase, understandably, in the use of various types of electronic monitoring tools, both for purposes of assessing the productivity of the client's workforce and also to make sure that they're complying with company policies and standards. There are a number of privacy issues that can come up in that context. Some of them, as with the issue of personal vs. company devices, the degree of risk will turn on that factor.

If the electronic monitoring tool results in the monitoring of an employee's activity in their own Facebook account or email account, which could totally happen if the employee is using a personal device or even using a company device, and they log into their personal account. Because there are pretty extensive monitoring tools being run by the employer, they may end up seeing communications or searches that are run. That's definitely something to be mindful of.

You could also run into issues with recording of communications where there might be an obligation to notify to avoid liability under a wiretap law like the California Invasion of Privacy Act, or there are similar laws in eleven or so other states. Those are some of the common issues that come up with the use of these monitoring tools.

Any others that you want to flag, Joe?

Lazzarotti

Well, one is that you have increased the potential for people to work remotely from a lot of different places, and they may be residents of different countries. Now, they have access and maybe store data in those other countries. The question becomes, do you now, in some way or based upon your business, become subject to another law in another country? If so, how does that impact your compliance obligations? Does it trigger a provision in a customer agreement where the customer says we don't want that data stored outside the United States? We look at a lot of agreements. I don't know about you, but I'm seeing, certainly in some industries, businesses are saying, we want to keep that data in the U.S.

Another issue with remote workers is two similar situations where I've seen several clients come. I'm curious, Damon, if you've run into this. A client hires someone, they go through the interview process, they have Zoom meetings and they make the decision to hire the person. Then, six months later, they start to scratch their head and say, I don't think that's the person we hired. It doesn't sound like them, and we wonder who that person is. In a more nefarious case, there have been a lot of reports, and we've been working with some clients on certain nation states that are using this model to infiltrate companies. That's become more of a law enforcement issue, but this idea of trying to identify and know who these people are that we're hiring. Is there some validation and authentication process for when we hire someone and allow them access to our systems, but we're not seeing them every day? They're not at the water cooler; they are just on some screen. Is that who we say we're hiring? Those are a couple of things that I think are really creating some risk for employers.

Silver

One more to add to that, building off the idea that you don't necessarily know where people are, some of these monitoring tools will very precisely track geolocation. You can run into issues where an employee brings their laptop with them to their doctor's appointment, to church or the temple that they go to after work or to another location in which arguably they have some expectation of privacy. They're not thinking necessarily about the fact that their employer will know where they are. That is fortunately something that can be addressed pretty effectively through policies, just making sure there's a clear disclosure of the fact that certain devices or applications are going to track location. Employees who choose to bring a company laptop with them when attending to personal business should not have any expectation of privacy in the places that they choose to visit. That is something to think about as well. It may not even be the intention of the company; they probably don't want to know necessarily where their employees are going off hours. Unless technical controls are put in place and disclosures are

made, that's another area of risk that we've seen come.

Lazzarotti

It is clear, like with a lot of issues we're talking about, this is one of those where you really want to think about what your overall strategy is. From the standpoint of what devices and data are remote workers using, and how are we managing them from a productivity perspective and their privacy rights? How do we manage that expectation, then? How do we know who we're dealing with and validate who they are, among other issues?

Developing a policy and a strategy to deal with that involves HR and IT. Maybe thinking about your vendor agreements and customer agreements to make sure that you're not running into any issues.

Thank you for listening to our We get privacy podcast. Hope this is helpful for you. As always, if you have any questions or suggestions for future episodes, please email us at privacy@JacksonLewis.com. Damon, always a pleasure speaking with you.

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