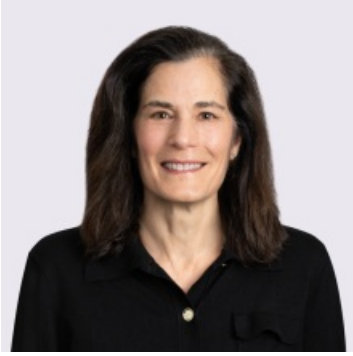
Podcast

ESG: How Data Privacy Relates to Good Governance Practices

By Susan M. Corcoran & Damon W. Silver

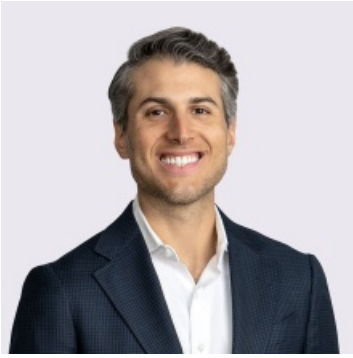
March 19, 2024

Meet the Authors



Susan M. Corcoran

(She/Her)
Principal
(914) 872-6871
Susan.Corcoran@jacksonlewis.com



Damon W. Silver

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

Related Services

Environmental, Social and Governance (ESG)
Privacy, Data and Cybersecurity

Details

March 19, 2024

Organizations implementing ESG strategies are focused on managing their companies in ways that are ethical, transparent and responsible to stakeholders. Equally important is implementing good governance practices, including managing privacy compliance and risk.

Jackson Lewis P.C. · ESG: How Data Privacy Relates to Good Governance Practices

Listen on Spotify
Listen on Soundcloud
Listen on Apple Podcasts
YouTube

Transcript

Alitia Faccone:

Welcome to Jackson Lewis' podcast, We Get Work. Focused solely on workplace issues, it is our job to help employers develop proactive strategies, strong policies, and business-oriented solutions to cultivate an engaged, stable and inclusive workforce. Our podcast identifies issues that influence and impact the workplace, and its continuing evolution and helps answer the question on every employer's mind, how will my business be impacted?

Organizations implementing ESG strategies are focused on managing their companies in ways that are ethical, transparent, and responsible to stakeholders. Equally important is implementing good governance practices, including managing privacy, compliance, and risk. On this episode of We Get Work, we discuss the data privacy implications of website tracking technologies and the impact on an organization's governance practices. While website tracking technologies can provide value, they may also cause customers, clients, stakeholders, and employees to be uncomfortable, while unintentionally exposing the organization to significant litigation and regulatory risk.

Today's hosts are Susan Corcoran and Damon Silver, principals in the White Plains and New York City offices of Jackson Lewis and members of the ESG Group. Susan is an experienced employment counselor and litigator, a corporate governance and internal investigations group member and co-editor of its blog.

Susan provides legal advice to organizations and boards relating to risk and strategy. Damon, a core member of the firm's privacy, data and cybersecurity group helps clients navigate the treacherous data privacy and security landscape by leading complex projects to assess and mitigate their compliance risk under various frameworks, guiding them through investigation of and responses to data breaches and providing day-to-day counseling on the data privacy and security implications of various business practices.

Susan and Damon, the question on everyone's mind today is how can organizations ensure good governance practices while safely leveraging the benefits of website tracking technologies and how does that impact my organization?

Susan Corcoran:

Welcome. Thank you Damon, for letting me join you. As we talk about the G in ESG as it relates to data privacy and related technology concerns, we certainly are continuing to hear a lot about ESG reporting and how privacy and data privacy governance are part of that mix these days. And certainly with respect to G, the governance aspect of ESG, we're hearing a lot about how organizations are trying to manage new technologies and the issues that are arising out of that.

So I'm certainly excited today about having a conversation with you about trends and how we're dealing with the different types of issues that are arising out of new technology and how we can create best practices to help organizations manage those trends. And also from a governance perspective, how we can provide an organization clear direction while taking steps to reduce risks and perhaps costs associated with unfortunate times may be poor decision making or not being prepared for risks that may be associated with new technology.

Damon, maybe if you can start off by just telling us what are you seeing as some of the trends out there with respect to things that are getting a lot of attention these days?

Damon Silver:

Yeah, thanks Susan. I appreciate you taking the time to chat today. So one significant trend we've been seeing is the rise in risks related to the use of website tracking technologies. We're really seeing that organizations across the spectrum are increasingly using these technologies to track what website visitors click on, what videos they view, what searches they run, and what they say when they're communicating with chatbots.

Now, these technologies serve a number of functions that most of us would consider legitimate, like showing us similar content we may be interested in or remembering items that we put in our shopping carts, but they're also used in ways that increasingly make people kind of uncomfortable, for instance, when they caused the shoes that we looked at or sometimes it seems even just thought about to start appearing in ads all over the web wherever we go. And this discomfort is further heightened if we substitute shoes for something more sensitive like prescription medication or medical devices.

Without taking us too far into the weeds, there are a couple types of tracking

activities that have driven a lot of the litigation and enforcement activity that we've seen thus far. So the first is a website owner allowing third parties to collect or access information about visitors' website activity for use in serving those visitors targeted ads. And then the second is allowing a third party to access visitors communications with chatbots. Based on these types of uses of these technologies among others, we've started to see a variety of legal claims asserted. For instance, wiretap laws may be triggered if communications with chatbots or with other features on a website like a web forum or a search bar are "intercepted" by a third party without proper consent from the site visitor. Those interceptions, along with the tracking of other website activity, can also form the basis for invasion of privacy claims, particularly if the visitor's interaction with the site reveal arguably sensitive information.

So this could be something like the visitor's medical condition if we're talking about a hospital website, their sexual orientation or their religious or political affiliations. If the tracking activity on a site is inconsistent with the disclosures that the site owner makes in their privacy policy or terms of use, that inconsistency can also form the basis for breach of contract claims or violations of the FTC Act's prohibition on unfair or deceptive acts or practices.

And then if we're talking about a site where there is video content, the disclosure of the site visitors' preferences around the videos they view or the videos they like to some outside party without their consent could be a violation of the video Privacy Protection Act. In addition to this litigation risk, it also seems like there's a lot of regulatory agency attention on this area in particular from the FTC, the Department of Health and Human Services, and then over in the EU from the various agencies that enforce the GDPR.

Susan Corcoran:

Damon, this is really an incredibly challenging area for a lot of us, particularly me who grew up in an era where we were not dealing with a lot of these types of issues. And one thing I'd like to talk a little bit further about is website tracking type of issues because not only is there a litigation risk, and certainly with a lot of the topics that you just talked about, there's a reputational risk downside that could affect perception by stakeholders and have an impact on an organization.

So with that said, when we talk about website tracking issues, can you talk a little bit more about what we could do to perhaps be in a better posture to maybe prevent or maybe what are some of the defenses in those types of cases?

Damon Silver:

Yeah, absolutely, Susan. So along with procedural defenses like lack of personal jurisdiction or standing, the key substantive defense is establishing that the site visitor provided informed consent to the collection of their personal information by the site's tracking technologies. To bolster this defense, the site owner needs to be mindful of a couple things. The first is timing, and the second is whether the consent was adequately informed. In a somewhat recent decision from 2022, the Ninth Circuit held that site owners must collect consent prior to tracking visitors' activities. So if you're a site owner and you're intending to rely on disclosures in

your privacy policy, which is linked at the bottom of your home page, or you're going to have the site visitor provide consent as they're checking out, as they're completing their transaction, that may not be viable consent because by the time the individual receives that notice and arguably their consent is collected, quite a bit of tracking activity may already have happened, and that tracking activity would be beyond the scope of the consent they provided.

As for whether the consent was adequately informed, there really isn't unfortunately a clear standard on that point yet. And looking at some of the decisions, some of the limited decisions that have analyzed the issue, it seems like courts are viewing this as a very fact-specific determination. So at least for the time being erring on the side of detailed disclosure, for instance, with respect to what categories of tracking technologies are used, what categories of personal information are collected and what categories of third parties that information is disclosed to is going to be the prudent approach.

Susan Corcoran:

And thinking about what steps to take and what might be the most prudent approach, what type of resources should a company be thinking about to obtain now, look to in the future to be able to put them in the best position to handle whether these situations or to prevent one of these situations?

Damon Silver:

Yeah, so the mitigation strategy we recommend can be broken into three phases. The first is to essentially start by zooming out before addressing mitigation strategy specific to website tracking technologies. It can be helpful to take a look at website risks more broadly, in particular to take stock of the now 12 states, starting with California, that have passed comprehensive privacy laws. These new laws have very broad definitions of personal information or personal data. The term used varies depending on the statute. And these laws cover information that might be collected via website tracking technologies. And if that information's covered, there are a wide array of obligations that the website owner potentially needs to address in order to be in compliance.

The second phase, once the site owner has sort of taken in stock of the broader considerations is to do some homework, to really drill down on what tracking technologies are currently in use on their sites, what information they're collecting through those technologies, and whether and to whom that information is disclosed. We've worked with quite a few organizations that are unpleasantly surprised to learn that due to acquisitions, turnover in their marketing and website development teams and a variety of other factors, they may have a whole bunch of tracking technologies running on their sites without their knowledge, and in some instances, without delivering much of any ROI.

To help clients get a handle on this kind of expansive area of risk, and to be able to make informed decisions about how their use of technologies is affecting their risk mitigation strategies. We've collaborated with an AI-powered data analytics firm called SecondSight to offer a website compliance assessment. The way this works is we engage SecondSight on the client's behalf under privilege to scan its designated

websites for cookies, pixels, and similar tracking technologies. We then perform a high-level review of the site owner's websites to identify legal compliance risks stemming from some of the data privacy laws I mentioned and other regulatory requirements that may be applicable. And then we share our findings with the client and develop an action plan to mitigate its website tracking risk. The specifics of that plan are going to vary depending on the organization's situation, but in most cases, they'll involve some combination of adjusting how the site owner is using website tracking technologies, updating their privacy policies and notices, and ensuring their service agreements with website tracking vendors include requisite data protection provisions.

So Susan, as we start to wrap up here, what are your thoughts around best practice governance strategies that our listeners should be mindful of as they're considering everything that we've talked about today?

Susan Corcoran:

Sure. Before we get to that too, Damon, you and I have talked before about what type of industries might be most susceptible to website tracking type of liability. Can you tell us what industries have been hit the hardest in this regard?

Damon Silver:

Yeah, absolutely. Absolutely. So the heaviest concentration of these website tracking lawsuits has been against organizations in the healthcare space, but we have seen increasingly that the plaintiffs' bar is also starting to target various other industries, some of which include retail insurance, real estate, tax preparation, aviation, and automotive as well.

Susan Corcoran:

Thank you. And then you provided us with a lot of great information. And also too, when we think about the governance side of things in terms of putting in some best practices, one thing that you said that was really step one is undertake a assessment. And we talked about a legal compliance assessment to understand any areas requiring corrective action. And I can't recite all the number of things that you included, although I was thinking of pixel and I was thinking of that term and so many other technical terms that would fall underneath that assessment and review and resources that you would use to undertake such an assessment.

And then two, as a result of that assessment, create some type of plan and part and parcel. There might be some immediate action parts of that plan versus what might be an ongoing plan to review policies, processes, and standards to ensure that they meet any legal requirements and certainly address any type of other company strategies and potential reputational risk concerns as well.

And then three, bring in the resources that you need, whether legal IT or other experts to create a solution that works for a particular organization in a particular industry because, as you noted, different organizations may have different needs. So those would be the top three things for a roadmap from a governance perspective.

Is there anything else that you want to share with us today, thinking about what you may need to do in 2024 with respect to privacy and data governance?

Damon Silver:

So one other thing I did want to flag Susan, and this is not necessarily a new development, but it's a continuing development, and that's just that we continue to see very large volume of data breaches. And there was a dip at some point. In ransomware cases, they seem to have returned with Vigor. We're seeing a lot of business email compromise type attacks as well, a lot of misdirected wire cases, and then also good old-fashioned mistakes or wrongdoing by insiders, by employees and others that result in data incidents. And while it used to be the case that when we had one of these incidents, we would notify the affected individuals, report to government agencies, sometimes those agencies would open investigations. Increasingly now, unless the incident affected a very small number of people, we're also seeing a lot of class action litigation.

And so there's nothing you can do truthfully as an organization to completely prevent data breaches. But this puts a lot of onus on organizations to make sure that they have a really well crafted and well executed plan in place to make sure that they are securely handling their data to reduce the likelihood of one of these incidents. And then perhaps as importantly, if they do have one to be in a position to defend their program as having included reasonable safeguards, which it's not always the easiest thing to do, but there are a number of steps that can be taken that really do go a long way towards putting you in a better position to make that type of defense.

Susan Corcoran:

And certainly from a governance standpoint too, there's potential disclosure requirements these days, also with respect to data breaches as well for certain organizations. And one of the things that I was thinking to kind of wrap up our discussion here is, so how does one organization sort of measure their success in this area, which ends up being very, very difficult. It's not necessarily that I have not been subject to any of these. It's more what kind of plan do they have in place to be able to successfully manage what lies ahead? Because this is going to be a tremendously busy area for us in the future just because of the growing regulations, rules, and litigation that is going to continue to expand because of the number of issues that are going to continue to populate in this particular area. Would you agree?

Damon Silver:

Yeah, I absolutely agree. And I think you make a great point about not focusing on the outcomes, not focusing on whether you did or didn't have the breach or did or didn't have a regulatory investigation, and focusing more instead on the process, specifically looking to certain benchmarks. There are some good benchmarks out there now for what qualifies as reasonable safeguards in the data security context, what would qualify as having a reasonable compliance program in place for something like CCPA or GDPR. And so I think in trying to measure success and measure progress, that's really the place to focus, identify what those benchmarks

are, and then evaluate your progress towards meeting them.

Susan Corcoran:

One of the things that I have to do, and I had a reminder today, is I have to complete my training for security purposes at Jackson Lewis. And I think that's a first step and a second step and a third step and so on to ensuring that an organization has the right steps in place for a preventive type of program. And there are certainly many other things. And so I want to thank you, Damon, for your time, and this has been a terrific educational experience in terms of learning what has happened in the past and what we all have to do in the future to put us on the right road for success.

Damon Silver:

Thank you. Great talking to you, Susan.

Susan Corcoran:

Take care. Bye-bye.

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.