

Podcast

# ESG: Promoting Racial Equity

By Damon W. Silver & Michael D. Thomas

May 16, 2023

## Meet the Authors



### Damon W. Silver

Principal

(212) 545-4063

Damon.Silver@jacksonlewis.com



### Michael D. Thomas

Principal

(949) 885-5240

Michael.Thomas@jacksonlewis.com

## Related Services

Corporate Diversity Counseling

Environmental, Social and  
Governance (ESG)

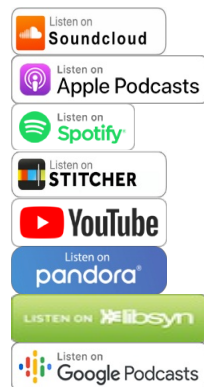
ESG Audio Guide

## Details

May 16, 2023

As more corporate shareholders demand that companies assess their progress in environmental, social, and governance areas, businesses are considering the proactive step of performing a racial equity audit. These audits help to create accountability for values-based outcomes.

Jackson Lewis P.C. · ESG: Promoting Racial Equity



## 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? As more corporate shareholders demand that companies assess their progress in environmental, social, and governance areas, businesses are considering the proactive step of performing a racial equity audit. These audits help to create accountability for values-based outcomes.

On this episode of We get work™, two members of the Jackson Lewis ESG group discuss tips for conducting a racial equity audit while avoiding privacy related legal traps. Our hosts today are Damon Silver and Michael Thomas, principals in the New York City and Orange County offices of Jackson Lewis. Damon partners with clients on setting, reaching, and monitoring their ESG related goals. Michael assists with the full spectrum of workplace diversity and inclusion related issues, including conducting trainings on unconscious bias and microaggressions, creating inclusive cultures and behaviors, employee engagement and developing, leveraging and implementing diversity and inclusion initiatives. Michael regularly speaks and publishes on diversity related topics. Damon and Michael, the question on

everyone's mind today is why should I conduct a racial equity audit and how does that impact my business?

**Damon Silver:**

Welcome everyone. My name is Damon Silver. Thank you all for joining us today. As we work with clients to develop and manage their ESG programs, one of the issues that arises is whether they should conduct racial equity audits and if they should, what does that process look like and what are the legal risks they need to be mindful of in particular with respect to employee privacy. In the time we have together today, Michael and I are going to talk through these considerations a little bit at a high level. Michael, to get us started, could you just give us some context? So what is a racial equity audit?

**Michael Thomas:**

Thanks, Damon, and thanks for everyone that's listening to this podcast. And so a racial equity audit really is an evaluation, so it's usually conducted by an external organization, often a law firm, and it's of an employer's policies, procedures, and practices to identify and address any systemic bias and discrimination. So it shows where the employer might be falling short in efforts to build a more diverse, equitable and inclusive workplace. And so the auditors may analyze recruiting, hiring, promotion, retention, training, social media messages, and even algorithms used in operations, and they ultimately make some recommendations. And the recommendations could include things like training employees, adjusting corporate policies, even analyzing pay equity or conducting a corporate climate survey. And so ultimately, an effective audit holds up a mirror to an organization to examine what its values are and whether it's actually living up to those values.

**Damon Silver:**

Thanks, Michael. That's very helpful. You touched on this a little bit, but I'm wondering if you can expand on why companies are conducting racial equity audits. What's the driving force behind that trend we're seeing?

**Michael Thomas:**

Thanks Damon and that's also a great question. And so over the last couple of years, we've seen a significant increase in the number of companies, government entities, and even nonprofits conducting internal and external racial equity or sometimes called civil rights audits. And so the demand for audits come from proxy demands to public traded companies, investors, the government, employees, consumers, and even the public at large sometimes. And in general, there seems to be a greater expectation that employers evaluate their environmental, social and governance, so your ESG impact and that includes looking at the impact on communities of color and that maybe change might be warranted.

And so a lot of companies do not conduct in a racial equity audit because they have not heard a lot of complaints about racial bias or they might think that if bias does exist, it's really just an isolated issue. And so the truth is that often racial bias goes unreported, and that can be for a variety of reasons. It can be because the targets are afraid that they won't be believed that they say something. Sometimes people

don't report racial bias because they don't believe their supervisor or the company will actually do anything to fix the problem, or sometimes they're actually even worried that reporting might negatively impact their career. And so again, there's a lot of driving forces, but ultimately that effective audit holds up a mirror to the organization.

Damon Silver:

Thanks, Michael. And what is the purpose of doing the audit? What can a company that's considering this hope to accomplish?

**Michael Thomas:**

Yeah, and so the purpose or really the goals of a racial equity audit, they're going to be different for each company, and that just makes sense. Each company has different values and things like that, but the goals might include things like informing shareholders about their investments, helping to establish baseline metrics, measuring performance in terms of achieving social justice and diversity, equity and inclusion goals, and ideally even using the audit to show the business case for DEI or ESG. So using an audit to show that it does actually increase profits and that investing in DEI and ESG actually does create a competitive advantage for the company. So the goals can vary in a variety of different ways, but ultimately the goal should be for the company to hold itself accountable for the findings, including being willing to take necessary action based on the recommendations from that external partner, often ideally done under attorney-client privilege, but be honest with the audit and its results because a big part of accountability is transparency and transparency for organizations is critical to build both trust and psychological safety for your employees and even for your external stakeholders.

And it's okay for their organization to acknowledge that it might have work to do, stakeholders respect that kind of transparency and it builds trust. And so one of the questions that does come up for a lot of our clients, when they're doing these audits, are the privacy risk. And so Damon, if you could really help the audience to really kind of think about what are some privacy risk employers should consider conducting that racial equity audit?

**Damon Silver:**

Yeah, absolutely. From a US perspective, the most significant privacy consideration is going to be compliance with the California Consumer Privacy Act or CCPA, which was recently amended by the California Privacy Rights Act or CPRA. Due to those CPRA amendments, which took effect earlier this year on January 1st, personal information about employees or applicants in California, which is very broadly defined and would likely include information that's collected in connection with racial equity audits is now fully in scope. What that means for employers with employees and applicants in California is that they need to navigate a number of CCPA compliance obligations when conducting those audits. For instance, employers need to ensure that they limit their collection and processing of personal information to only what's necessary in order to conduct the audit, and they also need to be thoughtful about how long they retain that information.

In other words, employers need to be prepared to articulate exactly why they're

collecting the information that they did. They need to think about how they're using that information and whether it's consistent with the purpose of conducting the audit, and they also need to think about what criteria they're using to determine how long they're going to keep that information. Another thing employers need to think about is making sure that they provided requisite disclosures to employees and applicants. The two main disclosures being a, what's called a [inaudible 00:08:28] collection, which advises employees and applicants what categories of their personal information are being collected, the purposes for which that information's used and how long it's being retained. And then the other of those disclosure documents and the more detailed one is a privacy policy, and many of our listeners have probably seen privacy policies on companies websites for disclosures to their consumers.

They now need to do the same thing in effect for their employees and for their applicants. They need to have a privacy policy on their site. It needs to disclose the sources of the personal information they collect. It needs to disclose the third parties that information's being disclosed to and the purposes of those disclosures. And also, and this is going to be something we'll focus on a bit here, the policy needs to disclose what rights employees and applicants now have with respect to that information. Another thing that companies need to think about as they're doing a racial equity audit and collecting personal information related to it is whether they have any vendors or consultants that are assisting them with that process and specifically any vendors or consultants that are going to have access to the personal information that is being collected from employees and applicants because the CCPA says that if you have some outside party that has access to your personal information, there's specific provisions that you need to have in your contracts with those parties.

Another important consideration, which I mentioned a minute ago, is how to deal with the requests that are now going to start coming in from employees and applicants to exercise their CCPA rights. The CCPA grants data subjects now meaning employees and applicants as well as commercial consumers, an array of rights including the right to access their personal information to request it be corrected or deleted, and then to request in certain instances that their employer limit the way that that information is used and disclosed. One of the key challenges for employers in responding to these types of requests is ensuring that they are consistent and mindful of timing. The CCPA prohibits discriminating against data subjects for exercising their rights. So as is very often the case in the employment context, employers will need to develop thoughtful processes to avoid treating certain employees and applicants differently than others unless they have some justification for that different treatment.

For instance, the CCPA establishes numerous exemptions that enable employers in certain circumstances to deny an employee or applicant's request or at least deny it in part. These exemptions are of course welcome news to employers in many respects since they're going to provide a shield against complying with really expensive and burdensome requests in some instances. But by the same token, the exemptions also create risk, in particular if an employer is not prepared to explain why it relied on in an exemption or applied in an exemption a certain way with respect to one employee's request, but not another. Employers also need to be

mindful of timing. If you have an employee that recently made a CCPA request, you're going to want to really carefully assess your potential CCPA retaliation liability if you take adverse action against that employee close in time to receipt of their request.

Moving beyond the CCPA, employers will also want take a close look at whether they have adequate safeguards in place to protect the information that they collect in connection with conducting a racial equity audit. Although this information probably is not going to qualify as personally identifiable information or PII, which is helpful because it means that it's probably not subject to a statutory obligation to protect it, and it may not trigger notification or reporting obligations. If it's breached, there's still going to be benefit to treating racial equity audit information as if it were PII. Employees understandably are going to view this information as being very sensitive and they're going to expect their employers to handle it accordingly. To that end, employers should be thoughtful about who... This could be both internal personnel as well as any outside party that they may involve in the process, it should be thoughtful about who is going to have access to the information related to a racial equity audit, and they're going to want to make sure that they've implemented technical safeguards to limit access to only those who really need it.

Employers should also ensure that the information they're collecting in connection with an audit is transmitted via secure channels and is stored in secure locations. So for example, it's likely going to be best to use something like a portal or a secure file transfer protocol rather than just regular email to collect, transmit and store this information. As I mentioned with respect to the CCPA, employers should also take note of what vendors or consultants have access to the racial equity audit information because they're going to want to ensure that their service agreements with those vendors include appropriate data privacy and security provisions beyond those that they're already going to have to include for CCPA purposes. So for instance, you're going to want to have those vendors and consultants agree by contract that they are going to securely store and transmit your information. They're only going to use your information for purposes of providing whatever service you've engaged them to provide related to the audit, and you're going to want them to promptly notify you in the event that there is a breach of that information.

Employers will also want to think about whether they need to provide additional training to whatever members of their workforce are going to be involved in conducting the racial equity audit on how to appropriately handle the associated information. Implementing thoughtful policies and procedures is always going to be an important and necessary first step, but oftentimes absent in an effective training program, many of those policies and procedures are not going to be complied with in the way that an employer may hope. The last item I wanted to mention is that our focus here is on US privacy law, but for some of our clients who have operations elsewhere, for example, in the EU, there may be a number of additional considerations that you'll have to contend with. For instance, under the EU data protection law, the GDPR, you'll also likely need to be able to articulate a lawful basis for collecting and processing personal information related to a racial equity audit, and you'll also need to deal with the sometimes onerous and confusing

restrictions on how you transfer that data across borders.

**Michael Thomas:**

Thanks. Super helpful. A lot of information there, and I think one of the things you highlight is that employers can approach these racial equity audits with just really good intentions, but there's a lot to navigate here and a lot of potential legal risk for employers to really consider. And so maybe one of the things you could do is kind of help some of our listeners really understand what are some common missteps that employers may make in kind of managing this personal identifiable data like race?

**Damon Silver:**

So one issue we're seeing is that employers don't necessarily realize that the CCPA applies to them or that their obligations under the CCPA have significantly expanded since the CPRA took effect earlier this year. The CCPA scope is very broad, and its application to employment information has kind of been in flux since the CCPA was first passed in 2020. So for the first couple years after the law was passed, it basically exempted employment information from most of the CCPA's requirements, and there was an expectation by many that exemption would be extended at least for another year or two. All of a sudden, late last year, it became clear that the exemption wasn't going to be extended, and now all of a sudden many businesses that hadn't really thought a whole lot about the CCPA are trying to tackle this pretty significant compliance challenge.

Another challenge for employers is figuring out what data they have, how they're using it, who they're disclosing it to, and how long they're keeping it. Again, this is something that employers haven't really had to do, at least many have not had to do in the past, and until recently, they didn't really have a structure in place to try and tackle this challenge.

**Michael Thomas:**

Thanks, Damon, that that's really helpful. And as you mentioned, this is a pretty significant compliance challenge, and so in your experience, what do you recommend?

**Damon Silver:**

So I have few recommendations for employers. One that's more near term focus and another that's longer term focus. The near term recommendation is to try and build some momentum within their organization by sort of grabbing some of the low hanging fruit that they can address relatively quickly, relatively painlessly. Specifically, they can ensure they're providing requisite privacy notices to employees and applicants. They can update their website privacy policy to include the required CCPA language and correct any inaccuracies. They can identify any vendors and consultants that are processing personal information on their behalf and make sure that they have appropriate language in their agreements. They can develop some user-friendly internal processes to manage requests by employees and applicants to exercise their CCPA rights. And then they can just determine as a threshold issue whether they have a written information security program, and if

they do, they can make sure that the personal information they're collecting in connection with a racial equity audit is going to be covered by that existing program.

Then from a longer term perspective, my recommendation is that employers conduct what's called a data mapping exercise, which is a way to get a better handle on what personal information they're collecting and how they're using and securing it. As might sound like the case, that can be a bit of an onerous process, but I will say that it's a major value add for the clients that we're working with on that exercise because it gives them a level of visibility that allows them to make much more informed decisions about how they want to build out their program. So Michael, turning things back over to you, are there any final thoughts you want to share with the audience on conducting racial equity audits?

**Michael Thomas:**

Yeah, Damon, and thanks so much for all of your information and insights. There's really kind of two main things that I would suggest companies think about. The first is I really would recommend every organization to consider conducting a racial equity audit or often call a civil rights audit, are really regardless of where you are within your DEI or ESG life cycle in terms of how you've developed that program. And so investors and stakeholders, including the government, employees, applicants, and consumers are paying greater attention to environmental, social and governance, so ESG impacts of the company. They're also requesting and sometimes demanding data from companies regarding some of these social justice issues. And so you'll be more prepared to respond to these requests if you have looked at your data before one of these requests actually comes in and you kind of understand what your data shows and you've made some cost decision as to what you're going to do and what you're not going to do.

The second thing that I would say as a final thought is a large part of what we're talking about here is ultimately building trust and creating transparency and accountability. And so what that ultimately means is be sure to follow through with the recommendations and Nick's active steps that come out of the audit. And so effective audits really encourage that real and sometimes difficult self-reflection, that often leads to the need for future work. And so once you have that data, you got to really think constructively and critically about how you're going to use that to potentially change your organization and what that actually means. And change becomes important here, but don't expect meaningful change to happen quickly, it's not really going to occur overnight. So change takes time, which again is why building trust and also psychological safety are really important here. And so Damon, I'll turn it back to you for you to share some final thoughts or insights that you might have.

**Damon Silver:**

Yeah, thanks Michael. So on the privacy front, there are a couple major trends that we, and I imagine many of our listeners have observed. The first is that organizations are collecting more and more data, and the second is that that data is exposing their organizations to more and more risk, both because the area of data privacy and security is becoming more heavily regulated, and there's been a sharp

uptick just in the last year or two years in class action litigation and also because data subjects themselves are becoming increasingly cognizant of and protective of their data rights. There's a concept in data privacy that's called privacy by design, which essentially means that you're thinking about privacy at the front end when you're designing a program rather than trying to plug the holes on the backend, which tends to be a clunkier, more expensive and less effective approach. So for employers listening that are in the process now of developing or revamping their ESG programs, there's a great opportunity here to build privacy into the foundations of your programs, which is sure to yield numerous benefits in the years ahead.

**Michael Thomas:**

Thank you, Damon. This has been really informative and I think super helpful. It's always great to spend time talking with you and learning from you. And I also want to thank all of our listeners for spending some time with us today on this ESG recording.

**Damon Silver:**

Thanks, Michael. Great talking to you as always.

**Michael Thomas:**

We look forward to continuing this conversation.

**Alitia Faccone:**

Thank you for joining us on We get work™. Please tune in to 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](https://www.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.

©2023 Jackson Lewis P.C. 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. Recipients should consult with counsel before taking any actions based on the information contained within this material. This material may be considered attorney advertising in some jurisdictions. Prior results do not guarantee a similar outcome.

Focused on employment and labor law since 1958, Jackson Lewis P.C.'s 1,000+ attorneys located in major cities nationwide consistently identify and respond to new ways workplace law intersects business. We help employers develop proactive strategies, strong policies and business-oriented solutions to cultivate high-functioning workforces that are engaged and stable, and share our clients' goals to emphasize belonging and respect for the contributions of every employee. For more information, visit <https://www.jacksonlewis.com>.