



Podcast Transcript

2023 DSIR Report Deeper Dive: U.S. Employee Privacy

Date: September 13, 2023

Guests: Jennifer Mitchell and Justin Yedor, **Host:** Amy Kattman

Run Time: 10:54

For questions and comments contact:



Jennifer L. Mitchell

Partner
Los Angeles
T: +1.310.442.8865 | jlmitchell@bakerlaw.com



Justin T. Yedor

Partner
Los Angeles
T: +1.310.979.8405 | jyedor@bakerlaw.com

Kattman: Managing digital assets requires the efforts of the whole enterprise. The 2023 issue of the Data Security Incident Response Report, or the DSIR, includes more content than ever regarding the data ecosystem and how companies can best manage their digital assets as they move through the life cycle of data. The DSIR dives deep into the annual incident response trends and analytics our clients and friends depend on. It also covers topics such as global privacy, ad tech, the increase in litigation, healthcare privacy and compliance, and the latest in emerging technology. I'm Amy Kattman, and you're listening to BakerHosts.

We're back today with a Deeper Dive series covering key topics in this year's DSIR. On today's episode, we take a deep dive into the U.S. employee privacy

developments. Our guests today are Jen Mitchell and Justin Yedor, partners on our Privacy, Governance, and Technology Transactions team. Welcome to the show, Jen and Justin.

Mitchell: Thanks for having us.

Yedor: Yeah, glad to be here.

Kattman: Jen, I'd like to begin with you. Now that the CPRA has taken effect, can you tell us what types of changes you're seeing and how companies approach employee privacy compliance?

Mitchell: Yes, absolutely. So, we saw a lot of change late last year leading up to the CPRA operative date, and companies are still adopting to the law in preparation for the law's enforcement date of July 1, which is just around the corner. Under the CPRA, employers subject to the law must now provide all CCPA rights to their California workers, including current and former workers, as well as job candidates. And we've worked with many companies who've been very focused on these compliance efforts and who are now in the process of maintaining this arm of their privacy compliance program.

For example, many employers took the CPRA as an opportunity to update their data maps to include HR data processing activities and specifically, to identify where and why sensitive personal information is being processed, how long data is retained, and to what entities data is shared. We're also seeing employers continue to prepare for and react to the receipt of consumer rights requests from employees and job applicants, and this includes the right to know, the right to delete, the right to correct, the right to limit certain uses of sensitive personal information, and less commonly in the employee context, the right to opt out of sales and sharing of personal information.

And finally, the new contractual agreements for HR vendors has really been burdensome for a lot of employers. The CCPA requires a written agreement, including specific privacy terms when personal information is transferred outside of the company, and to meet this requirement in the employment context, businesses should continue to review and update agreements with HR vendors, recruiting vendors, and all other entities that handle employee and applicant personal information.

Kattman: Thanks, Jen. What are some of the key challenges you've helped clients work through under the CPRA as it relates to employees and job applicants, Jen?

Mitchell: Sure. From my perspective, I think the biggest challenge is going to be responding to employee privacy rights under the CCPA. From my perspective, we haven't seen a high volume of these requests to our clients yet, but each request will be time-consuming, and responses require some sensitivity given the HR context. And I think one of the top challenges in this area is that there is still some ambiguity in how these requests should be handled in the employee context, because implementing regs to the law are really consumer focused.

Also, any response to employee privacy rights should be coordinated with privacy counsel and employment counsel because an employee's standard employee rights may be confused with a privacy request, and also because sometimes there is an underlying employment dispute that prompted that CCPA request. Justin, curious what your thoughts are.

Yedor: I agree with everything you said, Jen. The CCPA, as applied to employees, job applicants, other workers, really is a square peg trying to be fit into a round hole. So, beyond the challenge of mapping and thoroughly understanding a pool of data that was previously an unknown for many businesses, there is a real challenge when it comes to trying to apply the consumer-focused privacy rights from this law to workers.

So as one example, we've spent a lot of time working with businesses to try to figure out what data remain in scope in response to something like a right to delete or the right to limit use of sensitive personal information. As I think probably many of our listeners are aware, there are some pretty broad exceptions to those rights as well as other rights under the CCPA, but the exceptions are phrased in terms of a consumer law. They talk about things like providing goods or services, which of course most businesses are not primarily engaged in doing with respect to their employees. So, there are some somewhat thorny interpretive questions that have to be answered in order to figure out exactly what is in scope.

And of course, we're still waiting to see if and when we might receive regulations from the California Privacy Protection Agency that could clarify some of these topics and to help businesses to understand exactly where the agency sees privacy rights applied in the employment context. Beyond this, there are also some real challenges with some of the more technical requirements under the CCPA. Those who have reviewed the law know how detailed it is, and it talks about things like home page links, recognition of browser signals for opt outs, and many other specifics that can be a real challenge to implement in the employment context, again, because they're ultimately targeted to consumers. So, those are a few of the things that I've noted as additional challenges.

Kattman: Justin, will other states follow California in regulating employee privacy in this way?

Yedor: It is a good question, Amy, and I think it is probably somewhat unlikely. There are now 11 states that have passed comprehensive privacy laws that, in many ways, are similar to the CCPA. However, as we sit here today, of all the laws that have passed, only California has extended its law to cover employees, job applicants, and other workers.

So, while we can never predict the future with certainty and at any given time, there are dozens of bills pending in state legislatures that, any one of which could be amended or could propose to cover these types of workers. It seems really unlikely at this point just given that there hasn't been much interest, or ultimately,

when the laws have passed in other states, they've been narrowed to really focus on the consumer context.

Kattman: Jen, moving across the country, what are you seeing in New York in regard to employee privacy?

Mitchell: Yeah, we have a few updates in New York as well. So last year, a new law took effect in New York State that requires employers that monitor employees' use of telephones, emails, Internet, other communications, to provide prior written notice of those monitoring activities to employees and also to obtain acknowledgment of receipt of the notice. And this law is similar to existing state laws in Connecticut and Delaware relating to employee monitoring.

More recently, on July 5 of this year, New York City will begin enforcing its local law, Local Law 144, which regulates the use of AI in the employment context and specifically the use of automated employment decision tools. And this law requires employers to provide notices, undertake audits, to identify potential bias associated with the use of those tools. And just recently, the New York City Department of Consumer and Worker Protection held a roundtable about the law to address open questions and try to resolve some ambiguity relating to the law, such as the applicability of the law to remote jobs and also how the notice should be provided. So still a bit of confusion, but again, that enforcement date of July 5 is just around the corner.

Kattman: As my final question for each of you, what trends do you see in U.S. employee privacy following us into 2023 and beyond? Justin, let's hear from you first.

Yedor: Sure. Picking up on Jen's answer to the last question, I think that the trend of regulating specific practices such as automated decision making or employee monitoring or biometrics will certainly continue. There's been intense interest in these issues both among state legislators but also among citizens in general, and so with that interest in these topics, I would not expect for the regulations to slow down anytime soon.

Kattman: And what about you, Jen?

Mitchell: I completely agree, and I think following our comments on the New York City law, I think how the use of AI in the employment context is regulated is going to be a really hot topic. And we know the topic of AI, of course, extends much beyond the employment world. But we've seen other states attempt to pass laws similar to the New York City law. California, for example, hasn't been successful yet, but California is busy conducting informational hearings. And we know that the EEOC has recently released a document focused on assessing the impacts of AI and in particular, the potential adverse impacts of AI in the employment context, with the view that employers' use of certain tools can violate civil rights of their employees. So, I think this is an area that we're still trying to wrap our arms around and keep up with the potential impact of this great new technology.

Kattman: Thank you so much, Jen and Justin.

Yedor: Thanks, Amy.

Mitchell: Thanks, Amy.

Kattman: If you have any questions for Jen or Justin, their contact information is in the show notes. As always, thanks for listening to BakerHosts.

Comments heard on BakerHosts are for informational purposes and should not be construed as legal advice regarding any specific facts or circumstances. Listeners should not act upon the information provided on BakerHosts without first consulting with a lawyer directly. The opinions expressed on BakerHosts are those of participants appearing on the program and do not necessarily reflect those of the firm. For more information about our practices and experience, please visit bakerlaw.com.