Podcast

Workplace Law After 'Loper': Will Organizations Face a Wider Regulatory Gap Between Conflicting Data Privacy and Security Laws?

By Melissa Pascualini &

October 17, 2024

Meet the Authors

Melissa Pascualini
Associate
631-247-4676
Melissa.Pascualini@jacksonlewis.com

Related Services

Artificial Intelligence & Automation
Privacy, Data and Cybersecurity
Workplace Law After 'Loper'
Workplace Law After 'Loper' Audio Guide

Details

October 17, 2024

The *Loper Bright* decision could challenge Congress in passing particular and forward-thinking data privacy and security laws.

Listen on Spotify
YouTube
Listen on Apple Podcasts

Transcript

INTRO

The United States Supreme Court's recent decision to end the Chevron doctrine in the Loper Bright case exposed a governmental fault line, which may have far-reaching implications for many entrenched U.S. federal agency regulations that have existed for decades and, consequently, for employers.

The Loper Bright decision could make it difficult for Congress to pass specific and forward-thinking data privacy and security laws to close the current gap in the regulatory landscape. In this episode of our podcast series, Workplace Law After Loper, we discuss how employers can remain aware of current and often conflicting requirements and ongoing challenges for compliance.

Today's hosts are Melissa Pascualini and Rob Yang, associates in the Long Island and San Francisco offices, respectively, and members of the Privacy, Data and Cybersecurity Group.

Melissa and Rob, the question on everyone's mind today is: How does the U.S. Supreme Court's decision in Loper Bright affect employers' need to comply with a patchwork of data privacy and security laws, and how does that impact my business?

CONTENT

Melissa Pascualini
Associate

Hello everyone, my name is Melissa Pascualini. I'm an associate in the Long Island Office of Jackson Lewis. As part of my involvement in the firm's data privacy and security group, I advise on various privacy and cybersecurity-related issues. Here with me today is my colleague Rob Yang. How are you, Rob?

Robert Yang
Associate and Certified Information Privacy Professional (CIPP/US)

I'm doing pretty good, Melissa. Hi everyone. I'm an attorney at the firm’s San Francisco office. As part of my practice, I also focus on issues relating to data security and privacy.

However, I have more of a litigation bent to it, so I also deal with lot of CIPA [California Invasion of Privacy Act] litigation, data-breach litigation, and things of that nature.

Pascualini

Great. So, Rob, we're here today to talk about the Supreme Court’s recent*Loper Bright* decision, which effectively ended *Chevron* deference, and about how that impacts the world of data privacy and security, including regulation and enforcement of related issues.

Yang

Yes. Before we dive into any details, let's talk through some context first.*Chevron* deference is a legal doctrine that came out of the *Chevron USA v. Natural Resources Defense Council* case back in 1984. Since then, the doctrine has been used to allow courts to defer to a federal agency's interpretation of ambiguous statutes that the agencies are responsible for administrating so long as the interpretation is deemed “reasonable.”

For decades, *Chevron* deference has been given to agencies like the FTC, the FDA, and all the other federal agencies, giving them a great latitude interpreting laws related to what they do. But what would happen if this principle is weakened or eliminated? What happens to AI governance when the agencies are no longer given this wide latitude to interpret these kinds of laws that Congress promulgates?

That's what we're really going to talk about today: the recent Supreme Court case that came out this year, *Loper Bright Enterprises v. Raimondo*, which basically overturned the principal of *Chevron* deference and shifted more of the regulatory decision-making to the courts. So, now, with this kind of crazy wild, wild West, what do you think is going to happen, Melissa?

Pascualini

That's a great point. There's such a glaring lack of regulation when it comes to data privacy and security-related matters. There's no one organization that really spearheads either the creation or the interpretation or the management of these regulations. So, now, due to this change, Congress is really tasked with a pretty difficult task at hand, which is to pass laws and regulations that are extremely specific and have, you know, incredible foresight and accuracy, which could really result in the regulation of data privacy and security matters being either exceptionally slow or even underdeveloped generally.

With this reverted deference, interpretation of legislation now relies on the review of the trier of fact to make a final determination. As a result of that, the data privacy and security-related regulation is going to suffer from quite a few things:

- We’re going to have a lack of understanding in evolving technologies, especially when it comes to things like AI and the general knowledge around AI tools and things of that nature.
- There's going to be a lack of a controlling federal agency.
- There's certainly now a shift in the burden on Congress to enact extremely specific legislation, like I mentioned.
- I would imagine — and this is definitely more in your realm — there's going to be a flood of litigation that's going to come out of this.
- And there's definitely going to be a shift towards regulation by the states.

Just taking a step back and really thinking about AI generally, because I think that that's a big one when it comes to the impact that this decision is going to have just on the data privacy and security realm generally. It's not just me who thinks that. Several justices brought up the topic of AI during oral arguments. Justine Kagan even included reference in her dissenting opinion about it.

So, there's certainly concerns about the long-term workability and having courts or Congress generally decide very highly technical statutory questions, especially when it comes to things like AI.

Let's talk about that for a minute. What are you really seeing, Rob, when it comes to AI — the different types of tools that are being used and how it's being used in the workplace?

Yang

For sure. So, broadly, AI as a field is basically computers trying to mimic human intelligence and, from a workforce perspective, I'm seeing a lot of clients using or wanting to use AI to see, understand and respond to natural language. They analyze that data.

For us in the Wage and Hour Class Action Group, it's very important for some way to efficiently analyze all of that kind of data from payroll, timekeeping, etc. And clients would really like to use that kind of data to make recommendations and to make decisions.

Right now, we're seeing more of an emphasis on employers using traditional AI to process and interpret data. But now with the onset of generative AI like Chat GPT, it's now come to the point where AI is being used to generate new content.

And to be sure, employers are using AI to perform tasks traditionally performed by humans, especially in the HR space. Like recently, I'm sure everyone's been hearing more and more about how AI is being used in making hiring decisions, identifying internal talent, and predicting attrition.

However, a lot of employers should be mindful of the pitfalls that come with that kind of power. For example, you might inadvertently just have some kind of bias programmed into your AI in which you're screening out applicants under a protected class. With those kinds of issues going out there, the lack of understanding on not just the employers' part but the courts' part is going to lead to a lot of gray areas. It's good for us as attorneys, but it's bad for everyone else who needs to spend the money to try to get an AI governance model in place.

Pascualini

I couldn't agree more. I think that there's definitely potential that AI regulation is going to suffer from this lack of understanding by various key decision makers in general. Now, the onus is on the courts, it's on Congress, it's on judges and lawmakers to specialize in the interpretation and even creation of new laws.

Even the most technical, savvy lawmaker doesn't really understand what AI is, for various reasons. The biggest one is mostly due to its ever-changing nature. But it's such a highly technical area. It's a very technical field. The lawmakers and judges have to rely on information generally provided by specialists in the field to be able to understand the complexities that would result.

Even with such reliance, we still need somebody to distill this information. We need someone to be able to bring this down to a level where lawmakers and judges can really understand it. And there's going to be levels to that. Because, as with any other subject matter, there's a degree in which individuals understand things. The complexity of how AI tools work is definitely unlikely to translate very clearly. There's going to be a lot of questions in terms of having these individuals themselves, whether it's the judges or the lawmakers, decipher what these tools can do and how to regulate them.

But also, what about the fact that the attempts to better understand AI from a legislative or even an enforcement perspective — it's not something that's new; there have been agencies and lawmakers that have already attempted to clarify misunderstandings — have been unable to even come up with one definition of what constitutes AI: Like what is artificial intelligence?

Because it varies and it's super complicated. It's very complex. There's a lot of technicalities to it. So, because of that vast complexity, it's going to be very unlikely that lawmakers are going to jump to create new legislation. And I think that that's definitely something that is going to halt legislation in terms of data privacy realm and AI just generally.

Yang

For sure. I just want to make a contrast to what you just said: In Europe, they have the AI Act and the GDPR. There's already a very clear set of rules as to what is AI and how it's being used. They, in the European Union, are moving forward with developing AI in a more predictable regulatory environment.

On the flip side, here in the United States, a lot of the regulation that we have is actually being based on existing laws and guidelines. There's no real federal agency that's taking charge of AI regulations. And even if there are, we got this whole problem of being in a post-*Chevron* deference world. This is probably going to lead to something like what we have in California where I practice. We are seeing a lot like meta pixel claims being brought under the California Invasion of Privacy Act, which was passed back in 1967. This was well before the data of the internet and was meant for phone calls.

Can you imagine how hard it is trying to adapt a law from 1967 in 2024 when you're applying technologies that didn't exist at the time? What are your thoughts on that?

Pascualini

Yes, we've seen that in a lot of what we do. I wouldn't call them stale laws, but they're things that were developed at a time where nobody could even conceptualize what was going to happen in five years, let alone 20 plus years to come. In that instance, oftentimes we've relied on agencies. We've relied on individuals that are a lot closer to this, individuals that have experience working in that field to be able to regulate. So now the thought of not having that . . . it's definitely something that many individuals, many business owners should really think about.

Yang

To follow up on your point: Here, in California, we have a pretty good example of what would happen in a regulatory landscape where things are very unclear. We have the CCPA [California Consumer Privacy Act] here in California, but that's not universal, one-size-fits-all, even within California. The CCPA, for example, won't go back and try to interpret how the CIPA, that I was talking about earlier, is not going to really dovetail into that. And you're just going to have this Frankenstein patchwork of laws, even within the same state, trying to figure out how this is going to tie back to AI.

Pascualini

Yes. Lawmakers are definitely going to now be tasked with having to use incredible foresight and wisdom in terms of creating regulation. We can no longer rely on these federal agencies to help provide guidance and technical knowledge. The burden has now shifted. We used to be able to place the reliance on these technically savvy agencies, and now the burden's shifting to lawmakers in Congress who arguably are not as technical or savvy when it comes to the world of data privacy and security. Before, generally, lawmakers could create a vague law that really allowed for specific interpretation from agencies that were much closer and more familiar with these subject areas. We don't have that anymore. Now we have lawmakers that are forced to create laws with much more specificity.

The real issue here is it doesn't matter how much foresight a lawmaker really holds. Unfortunately, they likely won't maintain or they won't even be able to get to establish the technical expertise that a lot of these agencies hold. This gap in knowledge is certainly further accentuated due to the constant developments and new technical innovations that are created in the data privacy and security realm. These lawmakers are having a difficult time trying to create proper legislation that properly regulates all these different areas, these newly developing areas, without either misapplying definitions of certain things — like bringing us back to the inability to create one actual definition of AI to be used across the board — or even the intentions behind it. It's definitely going to be particularly difficult.

I can see this really play out in two ways:

- Either the data privacy and the security regulation is going to be overstated and inhibiting. It could cause an over-regulation in the field, which I think would end up leading to an inhibition in terms of technological innovation. It might ultimately end up with halting US AI growth to a stop. If there's no clarity in terms of how to regulate this or if there's an over-regulation, it can definitely stunt any advances that we make.
- In the inverse of the fear of over-regulating, the lawmakers could create too little regulation. And under-regulation could be just as damaging. It could potentially lead to extreme violations of privacy for individuals or realms of AI where we didn't even conceptualize that these violations could have come up.

Yang

Inevitably, this is going to lead to a flood of litigation when there's going to be legislation that governs AI. Obviously, Congress isn't going to be able to address every nuance, and they're going to want to rely on agencies to interpret those kinds of laws. But without that, we're going to just see challenges in court. Judges don't have all the technical knowledge that these agencies do, they don't have all the staff with the proper training. And it's going to lead to a whole bunch of reasonable people differing in opinion about what the reasonable interpretation of these laws are.

Without a real clear picture of how we're supposed to deal with these things — we've got lawyers with one interpretation, judges with another interpretation, industry experts with yet another interpretation — what do you think is going to really happen in this post-*Chevron* world?

Pascualini

I think that there's definitely going to be a shift towards regulation by the states. We've seen it happen with consumer data privacy laws across the country. Due to the federal government's inability to create one comprehensive data privacy law, it's resulted in, at least by my last count, 18 separate state-specific ones. And that number just seems to continue to increase. Week by week, we see a new jurisdiction that's passing through legislation a new comprehensive consumer data privacy law.

From a business operations standpoint, a potential increase in regulation in states certainly can be overwhelmingly challenging to keep up with, especially for businesses that are operating nationally. You're no longer required to keep up with one law. You now have to think about an intertwined 18, at my last count, like I said, different jurisdictions with different state specific requirements; all due to the fact that the federal government, as much as it seems that it's tried to do, has failed to really create a comprehensive consumer data privacy law.

There were a lot of federal agencies that were able to regulate and things like that to provide at least a little bit of a background for Congress or for any individuals that were involved in any data privacy or AI-related lawmaking. And now we're not going to have that. So where do we go from here?

In terms of business owners and just business operations generally, I think many businesses might find this *Loper Bright* decision as something somewhat relieving. It's relieving them of any compliance or enforcement risks from federal agencies. But one thing to think about is that we're not really out of the woods here as a business owner. Yes, we might not be as regulated from the federal agencies on these issues, but that could definitely lead us to the potential of having additional challenges from either state legislatures or either state-specific enforcement agencies or authorities. What do you think about that, Rob?

Yang

For sure. You practice in New York. I'm here in California. Coast to coast, there's going to be vast, crazy differences in how things are being interpreted and even enforced. Now with this post-*Chevron* deference world, we have a lot of risks, a lot of opportunities for AI governance.

On the one hand, we've been talking about how this is going to create legal uncertainty and potential litigation. It could also spur Congress to act and bring some much-needed clarity to AI laws. Maybe they'll finally get their things together, maybe they'll create another agency which will be dedicated strictly to AI and tie in with all the other regulators out there. But, ultimately, it'll be up to a combination of policymakers, courts and, of course, the AI community to navigate this transition.

Pascualini

I couldn't agree more.

Yang

All right, Melissa, that was fun chatting with you about AI and how we're going to try to figure things out together.

For everyone else out there, if you enjoyed the discussion, don't forget to subscribe to our podcast and share this episode with your coworkers and friends. Hopefully we'll see you back soon to listen to more insights about what we have on the future of AI law.

Pascualini

Thanks, Rob. To our listeners, I just want to add, please feel free to reach out to us or to any other Jackson Lewis attorney with whom you regularly work if you need any other assistance. Thanks.

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, Libsyn, SoundCloud, Spotify 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.

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.