Blockbuster SCOTUS Ruling Will Push Privacy and AI Laws Into the Hands of the States: Your Post-Chevron Game Plan

Insights
7.31.24

The Supreme Court's recent landmark ruling that gives employers a powerful tool to fight back against regulatory overreach will have a broad impact on just about every area of workplace law. We're looking at the specific federal agency rules and positions most susceptible to attack now that SCOTUS ditched the decades-old *Chevron* doctrine. This edition will focus on how the new standard will affect the way federal agencies – particularly the Federal Trade Commission – attempt to regulate privacy and artificial intelligence.

What Happened?

Forty years ago, the Supreme Court laid out a legal standard forcing courts to give "considerable weight" to an agency's interpretation of a statute as long as the interpretation is not contrary to "the unambiguously expressed intent of Congress." This doctrine – known as the *Chevron* doctrine (so-named after one of the parties to the case) – allowed agencies to fill in gaps where a statute was silent or resolve ambiguous. It also gave federal agencies a tremendous amount of power to shape the law in ways they believed appropriate.

Three days after its fortieth birthday, however, the Supreme Court overruled the *Chevron* doctrine, holding that courts need not defer to an agency's interpretation of the law. This signifies a major shift, putting much more oversight and accountability in the hands of judges. You can read all about it here, including all the different ways that the workplace law landscape may soon change.

So, how will the areas of workplace privacy and artificial intelligence be impacted?

Federal Agencies Will Lose the Ability to Adapt to a Fast-Changing Technology

Privacy issues tend to be swiftly moving, and laws need to be nimbly crafted to be able to adapt to the changing technological landscape. At the federal level, the United States does not have an overarching general privacy statute. However, one (but not the only) agency that has played a large role in enforcing such laws is the Federal Trade Commission (FTC).

The demise of *Chevron* will make it harder for agencies such as the FTC to promulgate regulations which catch laws up to rapidly evolving technology. The end result is that, on the federal level, we

are likely to see a lot more uncertainty and a lot more challenges to regulations. Some specific examples include:

- ***Federal Trade Commission Act (FTC Act)*:** While the FTC Act does not mention privacy per se, it does provide the Federal Trade Commission with the authority to address "unfair or deceptive acts or practices" and to draft rules that define specific unfair or deceptive practices. Given the potential ambiguity in terms such as "unfair" or "deceptive," regulations seeking to address data security or privacy issues may face court challenges upon approval. While some Congressional leaders unveiled a bipartisan federal data privacy law earlier this year, it seems unlikely to pass due to fundamental differences in what its supporters believe should be covered in the bill.
- ***Gramm-Leach-Bliley Act (GLBA)*:** The GLBA authorizes the FTC to "prescribe such regulations as may be necessary to carry out the purposes" of the GLBA. Earlier this year, amendments to the GLBA "Safeguards Rule" – which established new notification requirements for financial services institutions – belatedly went into effect. These amendments affected big banks to auto dealerships which provided financing. These amendments may now be open to challenge as to whether they are "necessary" to carry out the purpose of the law.
- ***Children's Online Privacy Protection Act (COPPA)*:** Recently, the FTC published a notice of proposed rulemaking to strengthen COPPA. The proposed changes would provide additional factors to determine whether a website or online service is directed to children, increase data security requirements, and limit data retention. While some of the changes appear to fall squarely within the delegated regulatory authority of the FTC under COPPA, others may push the bounds of what is permissible.

Federal Agencies Will Be Hindered in Attempts to Regulate Artificial Intelligence

In April 2023, four government agencies – the Consumer Financial Protection Bureau (CFPB), the Department of Justice (DOJ), the Equal Opportunity Employment Commission (EEOC), and the FTC issued a Joint Statement on enforcement efforts against discrimination and bias in automated systems. While the Joint Statement itself is not a rule and therefore would not have been subject to *Chevron*, this may have been a prelude to rulemaking by one or more agencies.

Without *Chevron*, agencies will having a tougher time attempting to regulate AI. The FTC, the Federal Communications Commission (FCC), and the Health and Human Services Department have all issued rules surrounding AI. To the extent that agencies are trying to fit AI into frameworks that predate the existence of AI, this opens questions of whether such laws even contemplated AI – and meant to delegate authority on AI to those agencies.

States Will Continue to Lead in Crafting Laws and Regulations

While this may seem to create more of an open market for businesses, much of privacy and artificial intelligence regulations have been driven at the state level in lieu of overarching national laws – as many businesses are well aware. Over the last several years, the charge on privacy laws has been

led by the states, with 19 states having passed consumer privacy legislation. The existence of these laws (and the need to comply with them) is unaffected by demise of *Chevron*.

In the absence of any federal law, we can expect to see a patchwork of state laws filling the space. Indeed, that has already happened on the privacy side. While many of the consumer privacy laws are similar, they all have enough differences among them that one-size-fits-all compliance with them all is difficult. We expect to see a similar movement with AI laws, with differences state-to-state creating

Your Next Steps:

1. **Continue to Comply with Federal Regulations and Agency Interpretations of Statutes.** Unless and until a court overturns a federal regulation, you still need to comply with it. Even though federal regulations are more at-risk with the end of *Chevron* deference, that does not guarantee that they will be stricken down. Any outcome could be dependent on where a suit challenging a regulation is filed, and even a ruling against regulations may apply only to specific jurisdictions or in specific cases.
2. **Stay on Top of and Comply with State Laws.** As noted above, this recent Supreme Court decision does not negate state laws on privacy and AI. The bulk of the privacy regulation, to date, has come from the states. With agencies on a tighter leash as to AI, we can expect states to also take the lead on AI.
3. **Be Prepared to Devote More Resources to Privacy and AI.** Because agencies will be hamstrung in creating a national baseline for privacy and AI, we can expect ever more states to throw their hats into the ring to regulate these areas. While that might result in some states having few if any laws on these topics, expect states to lead the way. This past year, Colorado and Utah have already each signed into law a bill relating to AI. California, Illinois, Massachusetts, and Ohio also have bills working through the legislative process.
4. **Stay Alert.** Given the upheaval on the federal side coupled with active legislating on the state side, your business should expect to see a changing landscape over the next few years.

Conclusion

The best way to stay alert is to make sure you are subscribed to Fisher Phillips' Insight System. We will provide the most up-to-date information on data security and the workplace and AI-related developments directly to your inbox. If you have questions, contact your Fisher Phillips attorney, the author of this Insight, or any attorney in our Privacy and Cyber Group or AI, Data, and Analytics Practice Group.

Related People

Darcey M. Groden, CIPP/US
Associate
858.597.9627
Email

Service Focus

AI, Data, and Analytics

Government Relations

Litigation and Trials

Privacy and Cyber