Supplementary Segment

Navigating Cyber Governance Post-Chevron Deference Ruling

Jack Freund

Cyber Risk Officer, Kovrr

There has been a lot of hand-waving of late about the end of cyber regulations in the United States in the aftermath of the Relentless, Inc. v. Department of Commerce and Loper Bright Enterprises v. Raimondo cases. These cases overruled 40 years of administrative law based on the finding in the 1984 Chevron U.S.A. v. Natural Res. Def. Council case (called Chevron Deference). In the original ruling, the courts were ordered to give deference to the executive branch agencies in order to determine whether they could make rules based on unambiguous legislation. Now, the courts must take a much more literal reading of legislation when hearing and deciding challenges.

When evaluating these impacts, it's helpful to return to US Civics 101 and the branches of government. This will reveal where action may occur and what the major players would do in response. The US government is divided into three equal branches: the Executive (the President and the administrative agencies), the bicameral legislature (Congress, comprised of the House and Senate), and the Judiciary (courts). The original US states were effectively “countries” and have also retained a significant amount of historical power.

It will come as a surprise to no one that the Congressional branch of the US government has had difficulty effectuating its powers, but this is not a recent phenomenon. What started as good intentions in Chevron Deference has enabled the Legislative branch to delegate a lot of its powers to the Executive branch in a win-win situation. It’s far easier to get elected if the difficult decision-making happens outside the legislative function. They don’t have to go on record with a potentially unpopular opinion but get the credit for “doing something” in an area of concern, for example, writing a cybersecurity bill without hammering out any details on the specifics. Further, outside of the President and Vice-President, those in the executive branch don’t have to face the electorate and can make tough decisions in their areas of expertise with relatively little consequence.

The legislative branch has full power to make very specific laws—it always has and always will. Whether they wish to exercise that power is still to be determined. Congress can revise laws and write new ones with any granularity level. This is the most direct way that existing cybersecurity practices can be codified.

The courts now have a more significant role in judging challenges to these vague laws that don't have the specifics the executive branch agencies say they do. This doesn’t automatically mean that they are all overturned; it is simply that some interpretations may be more correct than others. This will mean lots of chaos in the near term as the exact operating environment is likely unknown, even though we know what good cyber governance looks like without needing regulatory tools to enforce good behavior. However, it should be noted that challenges to government regulations are common. This just portends even more of it in the near term.

The States retain a significant amount of power that can still be exercised. State-level regulatory agencies can fill gaps in federal laws if they choose. States are given broad latitude to govern when not limited by federal preemption. Congress, the courts, and the States could effectuate big changes in the cyber landscape. Below are a set of predictions about where and how things may play out:

- Congress will pass (some) specific laws about how to regulate cybersecurity. We’re likely to see some progress in the realm of critical infrastructure/operational technology and disclosure laws (perhaps an amendment to CIRCIA).
- Some non-zero amount of current cybersecurity rulemaking won’t be challenged. The SEC already requires that firms disclose material events and cyber can cause material events. However…
- Some rulemaking will be challenged, either as a whole or in part. For example, the SEC breach disclosure window will be challenged and perhaps overturned, but a CIRCIA amendment would dull the impact of this. Some of these challenges will take a long time to play out in the courts, so in the meantime there will be a requirement to adhere to them.
- However, we may find injunctions against these regulations that immediately put a halt to them.
- States could fill in the gaps and make all sorts of laws (except for where it doesn't have jurisdiction like inter-state commerce). A good example of this is the New York Department of Financial Services (NYDFS)—which does this all the time. The bad part of this is that it creates a patchwork of regulations that may conflict and make it harder to comply without burdens on companies.
- The market will regulate itself to a certain degree. Proclamations about how no one knows what will happen or what to do are alarmist doomsday predictions. We know how to manage cybersecurity, and we can refer to countless good practice frameworks.
- Communicating publicly about breaches is now so commonplace it's a de facto standard even if rules about it are later invalidated. Many organizations will continue to follow the rulemaking because it has become a part of good governance. Security and credit rating agencies could push this as well.

The English aphorism “keep calm and carry on” is on point here as organizations grapple with all these changes. Having a solid process for managing control posture, governing cyber risk, proactively engaging with regulators, and keeping the investor community in sync with your security program is as important now as ever. As we navigate these evolving regulatory landscapes, resilience and adaptability will be key. Organizations that remain vigilant and proactive will not only weather these changes but potentially emerge stronger and more secure.

Jack Freund, Ph.D., is the Chief Risk Officer for Kovrr where he oversees corporate risk and compliance, and strategy and governance of the firm’s cyber risk products. He is also the co-author of the foundational cyber risk quantification (CRQ) book using the FAIR standard, which was inducted into the Cybersecurity Canon in 2016. Jack was awarded a Ph.D. in Information Systems after his research in disaster informatics and cyber resilience at Nova Southeastern University and a post-doc certificate in International Law. He was named an ISSA Distinguished Fellow, FAIR Institute Fellow, IAPP Fellow of Information Privacy, ISC2 2020 Global Achievement Awardee, and ISACA’s 2018 John W. Lainhart IV Common Body of Knowledge Award recipient. Jack also serves on the board of the ISSA Education Foundation.