Health-ISAC Weekly Blog -- Hacking Healthcare®

Hacking Healthcare® | TLP:WHITE | Alert ID : a4dc9314 | Jul 18, 2024, 08:17 AM

In reversing a prior decision the Supreme Court of the United States (SCOTUS) made decades ago, the current SCOTUS has primed the United States (U.S.) federal regulatory landscape for widespread legal challenges. This edition of Hacking Healthcare®[i] explores what Health-ISAC members should know about how the SCOTUS decision in *Loper Bright Enterprises v. Raimondo* could significantly alter the cybersecurity and privacy regulatory landscape in the U.S.

Welcome back to Hacking Healthcare®

U.S. Supreme Court Decision Likely to Impact Cybersecurity Regulations

On June 28, SCOTUS released its decision on *Loper Bright Enterprises v. Raimondo* that reversed an earlier SCOTUS ruling in *Chevron v. Natural Resources Defense Council*.[ii] The result of this decision will likely have momentous effects on the federal regulatory landscape for years to come and may invalidate or require the revision of existing cybersecurity and privacy regulations that affect the Healthcare and Public Health (HPH) sector.

Before we begin, please note that the authors of Hacking Healthcare® are not lawyers and that a detailed legal analysis is beyond the scope of this newsletter. For our purposes, the brief overview of the two cases provided below focuses on the legal precedent that was set after the *Chevron* decision in 1984, and the generally accepted understanding of what the *Loper Bright Enterprises* case means for challenges to federal regulations.

Why was "*Chevron* Deference" Important?

The SCOTUS decision in *Chevron v Natural Resources Defense Council* established which became known as "*Chevron* deference" or the "*Chevron* doctrine."

This deference meant that when U.S. courts heard legal challenges to federal agency regulations or enforcement actions, the courts were required to "defer" to the agency's interpretation of a statute (i.e., a law passed by Congress) as long as the agency's interpretation was "permissible." As a result, when congressionally passed laws are ambiguous, and the agency interpretation was reasonable, a federal

agency had considerable discretion to determine the scope of its authority under the law to establish and enforce regulations.

For regulatory agencies within each presidential administration, this meant they were often able to pursue policy aims through creative but plausible interpretations of the law. For Congress, this meant that they did not necessarily need to be subject matter experts and could pass laws that were not overly prescriptive, relying on agencies to fill in the details. For industry or advocacy groups litigating federal regulations, it meant a more difficult time overturning or modifying regulations and enforcement decisions in court.

SCOTUS Ends *Chevron* Deference

The recent SCOTUS decision in *Loper Bright Enterprises v. Raimondo* essentially puts an end to *Chevron* deference and ushers in a new paradigm where the courts will have greater say in how ambiguous laws should be interpreted. As the Center for Cybersecurity Policy and Law describes it "The ruling will be used by courts in deciding cases that challenge whether a regulation exceeds Congressional authority" and that "[t]he ruling applies to both existing and future regulations."[iii]

Action & Analysis

Included with Health-ISAC Membership

[i] Hacking Healthcare is officially registered in the U.S. Patent and Trademark Office to the Health-ISAC

[ii] Background and professional legal analysis of the specifics of these court cases is beyond the scope of this newsletter. However, for those interested, the SCOTUS opinions for *Loper Bright Enterprises v. Raimondo* & *Chevron v. Natural Resources Defense Council* can be found at https://www.supremecourt.gov/opinions/23pdf/22-451_7m58.pdf & https://www.law.cornell.edu/supremecourt/text/467/837. Furthermore, a brief legal analysis can be found at https://www.venable.com/insights/publications/2024/chevron-decision/supreme-court-chevron-deference-decision

[iii] https://www.centerforcybersecuritypolicy.org/insights-and-research/chevron-pattern-disrupted-the-impact-on-cybersecurity-regulations

Report Source(s)

Health-ISAC

Release Date

Jul 18, 2024, 11:59 PM

Reference | References

supremecourt
cornell
centerforcybersecuritypolicy
venable

Tags

Regulations, Chevron, SCOTUS, Regulatory, CIRCIA, Hacking Healthcare, Supreme Court of the United States, CISA, United States

---

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare®:

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Councils efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Councils Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISACs annual Hobby Exercise and provides legal and regulatory updates for the Health-ISACs monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Threat Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).