RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: LAW-M05

“Hacker” Law After the Supreme Court Ruling: Insider Threats, Research & CFAA

Leonard Bailey

Head of Cybersecurity Unit/Special Counsel
for National Security
Department of Justice

Harley Geiger

Senior Director for Public Policy
Rapid7
@Harley Geiger

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

What the CFAA does

- Prohibits—
  - Unauthorized access to a “protected computer”
  - Exceeding authorized access to a protected computer
  - Intentionally damaging a protected computer without authorization
  - Trafficking in passwords through which a computer may be accessed without authorization
  - Accessing a protected computer without or in excess of authorized access to commit fraud
  - An “access” violation is a misdemeanor if it causes less than $5000 of damage but is otherwise a felony
- Criminal and civil penalties

CFAA in context with hacking laws

- Federal:
  - Digital Millennium Copyright Act, Sec. 1201 (with exemption!)
  - Wiretap Act/Stored Communications Act
  - Defend Trade Secrets Act
  - Unauthorized disclosure of classified information

- State computer crime laws
  - Similar formula to CFAA, but with important differences
  - WA, MO, MD

CFAA – used against security researchers?

- The CFAA has rarely been used to prosecute security researchers.

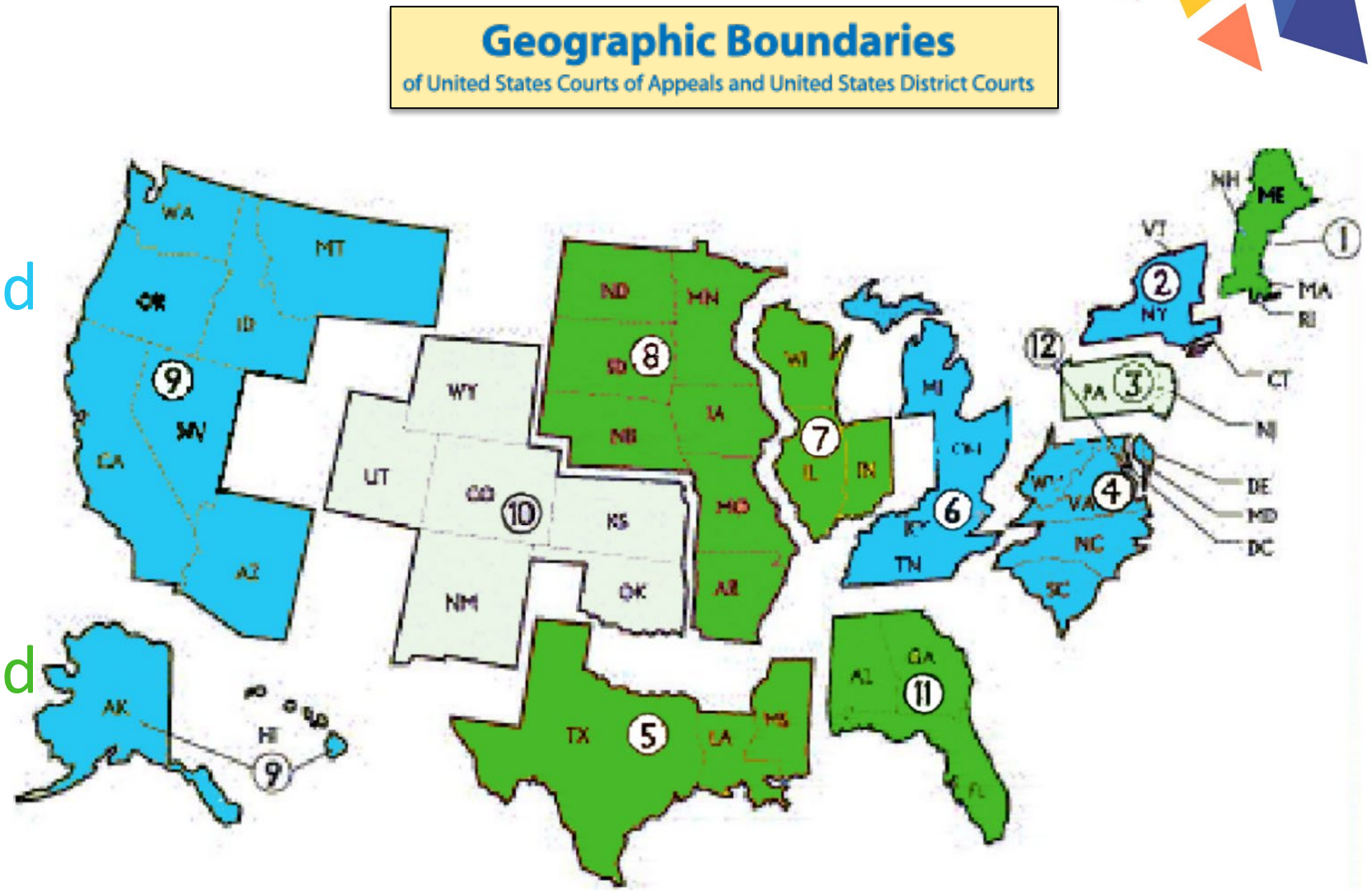
  "[I]t is important to note that prosecutions against security researchers-qua-security researchers are extremely rare."

  Center for Democracy & Technology, *"The Cyber:" Hard Questions in the World of Cybersecurity Research* (2017)

- However, companies sometimes invoke the CFAA companies to discourage research involving their products and security researchers are sometimes investigated for their activities that might implicate the CFAA.

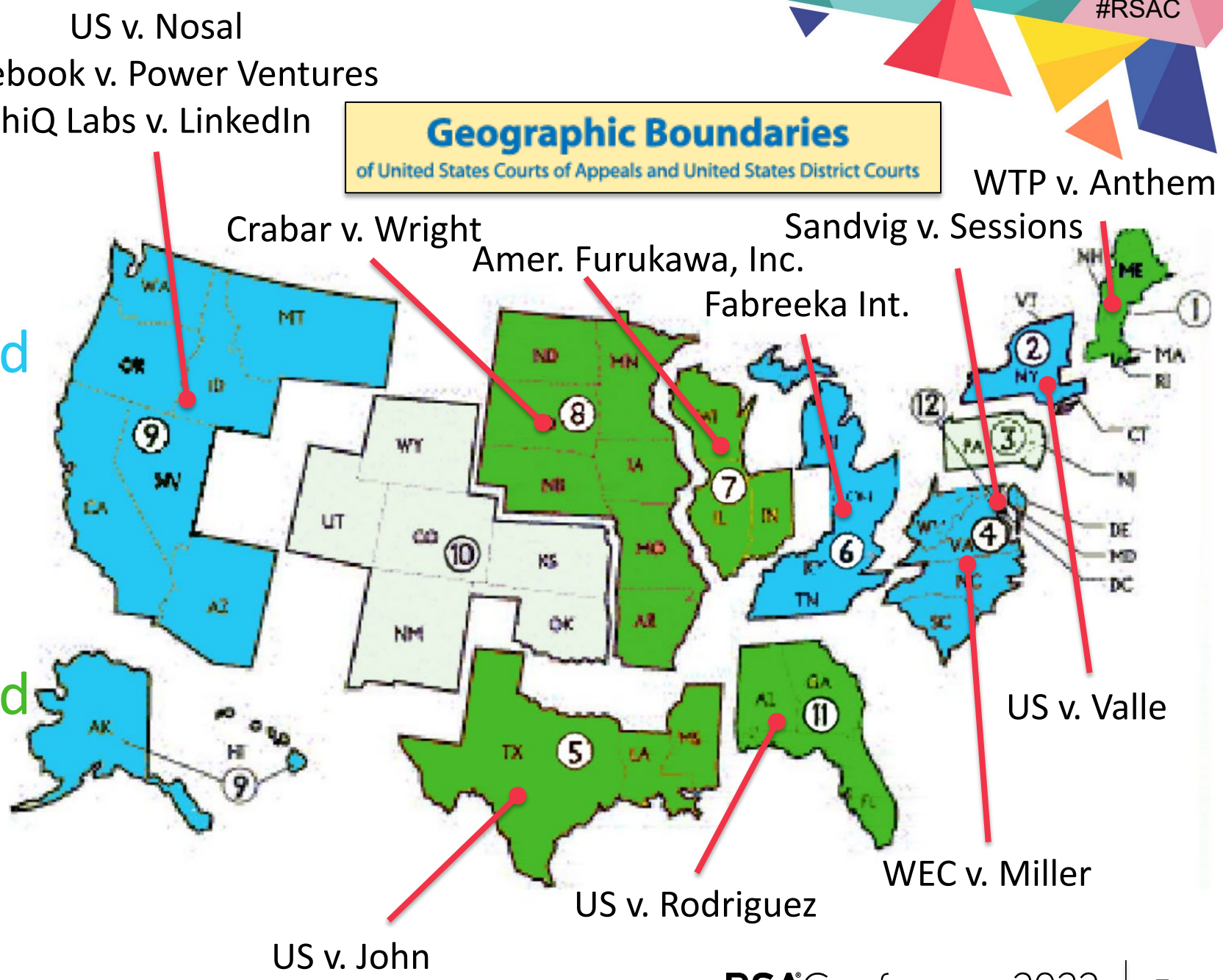
Circuit Split!

- 2nd, 4th, 6th, 9th, DC Circuits interpreted "exceeding authorized access" narrowly
- 1st 5th, 7th, 8th, 11th Circuits interpreted "exceeding authorized access" broadly



Circuit Split!

- 2nd, 4th, 6th, 9th, DC Circuits interpreted "exceeding authorized access" narrowly
- 1st 5th, 7th, 8th, 11th Circuits interpreted "exceeding authorized access" broadly



Van Buren

- US Supreme Court:

  Not a CFAA violation to obtain or use information on a computer for impermissible purposes, so long as you are authorized to access the information in the first place.

Van Buren v. United States, 141 s. ct. 1648 (2021).

Van Buren - “Gates up or down?”

- CFAA violations do not encompass breach of TOS or contract terms which grant access but limit that access or use based on purpose, intent, or manner of access.
  - *Example*

- But… what establishes “authorization?”
  - Contract/policy-based limits on access?
  - Technological/code-based access limitations?

Van Buren – Cybersecurity implications

- The good news:
  - Clarifies important security research question
  - Settles long-running debate about the CFAA

- The bad news:
  - Limits protections against insider threats
  - Restricts use of a statute that protects privacy
  - Leaves important unresolved questions

- Reminder:
  - Van Buren is limited to CFAA. Other laws still apply.

Applying Van Buren

- Organizations may still restrict authorization to access or use a computer through—
  - Technical means, such as password protection or access privileges
  - Data segregation, such as keeping material on separate networks or protected directories

BUT

- When a user is authorized for one purpose, CFAA is a limited deterrent to unauthorized use of information and restrictions on manner of access.

Applying Van Buren (cont.)

- Examples:
  - Employee accessing unrestricted information on employer computers (and providing it to non-employees).
  - Performing security research on publicly accessible web assets.
  - Using work or school computers for personal purposes.

Applying Van Buren (cont.)

- Van Buren left some uncertainty:

  "For present purposes, we need not address whether this inquiry turns only on technological (or "code-based") limitations on access, or instead also looks to limits contained in contracts or policies."

  - *Van Buren*, fn. 8

- While a contract or employment or workplace policy may not be sufficient to revoke authorization standing alone, it may be a factor that is considered with other limitations on access.

Van Buren Aftermath

- What Van Buren left unexamined
  - "Without authorization"?
  - What are "information located in particular areas of [a] computer—such as files, folders, or databases—that are off limits"?
  - What is a "gate" and when is a gate "up or down"?
- How cases like HiQ might (and might not) provide additional guidance on security research practices
- Other security research practices that might be charged as offenses
- Federal legislation?
  - *International Cybercrime Prevention Act*
- State computer crime laws

Van Buren Aftermath

- Revised DOJ guidance on the CFAA!
  - "The attorney for the government should decline prosecution if the defendant's conduct consisted of, and the defendant intended, good-faith security research."
  - "'[G]ood faith security research' means accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability,
    - where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and
    - where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services."

RSAConference2022

Thank you!

Leonard Bailey

Harley Geiger, @HarleyGeiger