RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **LAW-M06**

What Have the Courts Done Now? Explaining the Impact of Recent Cyber Cases

Rick Aldrich
Lead Cybersecurity Policy & Compliance Analyst
Booz | Allen | Hamilton
@AldrichRick, Aldrich_Richard@bah.com

Julie Bowen
Senior VP, GC, and Corp. Sec'y
Mitre Corporation
jbowen@mitre.org

Disclaimer and Legal Caveat

- This presentation is designed to raise awareness of general legal principles raised in several recent domestic and foreign cyber-related cases
- This session, and any information contained in this presentation, should not be construed as legal advice*
- The views and opinions expressed in this presentation are those of the authors and do not necessarily reflect the policy, opinion, or position of their employers or any other entity.

* **Disclaimer:** Information contained herein, and in this briefing, is for informational purposes and general guidance on matters of interest only and should not be considered legal advice or a recommendation. The application and impact of laws can vary widely based on specific facts and jurisdictions. Given the changing nature of laws, rules and regulations, there may be omissions or inaccuracies in the information contained in this presentation. Nothing by the presenters or moderator, or the information presented herein, is intended for, nor should it be construed as, rendering legal advice or services. This should not be a substitute for consultation with professional legal advisers.

Theme: Transform

- Goal of this Session
  - Identify emerging legal cases in which the courts are attempting to address transforming technologies
  - Provide takeaways to assist in anticipating or recovering from evolving changes in the law

Transform:
"to change completely the character or appearance of something in order to improve it"

-- Cambridge Dictionary

Why is this session important?

- Failure to keep up with evolving laws and court decisions can be very expensive and slow down an organization's ability to transform and evolve in the future
  - Facebook settled a biometrics case for $650 million
  - Poly Networks lost $600 million via a "smart contract"
  - Firms have been denied $100 million+ in insurance claims for cyber losses due to four key words—do you know what they are?

Key Cases

- Computer Fraud & Abuse Act
- Cyber Insurance
- Privacy
- Biometrics
- Evidence preservation
- Blockchain

Computer Fraud & Abuse Act

Van Buren v. United States, 593 U.S. __, 141 S. Ct. 1648 (2021)

- Facts of the case
- Issue: Whether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the Computer Fraud and Abuse Act if he accesses the same information for an improper purpose.

Court Holding

- Supreme Court: No (6-3). Hinged on the meaning of "so" in "so to obtain." Much discussion of privacy concerns, feds ability to prosecute such conduct, and S/C was uneasy with potential breadth of this statue based on an "improper purpose."
- Court adopted a "gates-up-or-down" approach that indicated either one was entitled to access the information or not, rejecting a circumstance-based approach.
- Resolved a circuit split: 2nd, 4th, and 9th reject the improper purpose approach ("parade of horribles"); 1st, 5th, 7th, 11th held contra
- Reversed 11th Cir. which had reaffirmed *US v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (holding a SSA employee who searched a SSA database for birth dates and home addresses of 17 people violated the law as it exceeded his authorized scope.)
- Takeaway: Pursue other means for suing insiders gone bad. Create contractual or regulatory terms to cover conduct. DoJ's new charging guidance addresses "parade of horribles" and "good faith" security research.

Cyber Insurance

Merck v. Ace American Insurance, No. L-002682-18 (N.J. Super. Ct., Jan. 13, 2022)

- Facts of the case
- Issue: Is collateral damage from NotPetya excluded under an "act of war" exclusion from insurance coverage?

Court Holding

- Super. Ct.: No—in a summary judgment holding
- Insurers relied on US and other countries' public claim that Russia was behind it, and that this was fallout from hostilities with Ukraine.
- Held that "reasonable understanding" of the exclusion would involve "armed forces." Contracts have not changed their language so expanded meaning not reasonable.
- What of SolarWinds? MS Exchange exploits?
- Takeaway: While insurer lost here, *Mondelez* and others are still pending, may go opposite way.
- US Office of Foreign Assets Control (OFAC) guidance: Beware of ransomware payments to certain entities. Strict liability for victim, insurer, and forensic company
- Consider also whether work-from-home environments prompted by COVID impacts insurance policy attestations regarding the covered network.

Privacy

C-311/18, DPC v. Facebook Ireland and Schrems (Schrems II), (2020)

- Facts of the case
- Issue: Was Facebook's transfer of Schrems' data from the EU to US sufficiently protected under the EU-US Privacy Shield?

Court Holding

- No. US national security laws and surveillance powers do not adequately protect EU citizens, invalidating protection under the EU-US Privacy Shield.
- Alternate protections also questioned
  - Standard Contract Clauses
  - Binding Corporate Rules
- Takeaway: For corporations: Carefully assess basis for data transfers. (Max penalty is 4% of annual global turnover.) Also, China's vague Personal Information Protection Law (PIPL) took effect on 1 Nov 2021. Many other countries and US states have various laws making compliance complex and mistakes costly. For government: Could impact Five Eyes intelligence sharing. Catch is that the GDPR expressly exempts EU's intelligence activities—but not those of non-EU countries.
- French and Austrian decisions that EU websites could not use Google Analytics due to *Schrems* II further undermines EU-US data transfers.
- Irish decision regarding Meta may require Facebook and Instagram to close down in Europe.
- On 25 Mar 2022 the EU and US announced an "agreement in principle" on Privacy Shield 2.0.
- *FBI v. Fazaga*, No. 20-828 (U.S. Mar. 4, 2022), may complicate the agreement in principle.

Biometrics

United States v. Wright, 431 F. Supp. 3d 1175 (D. Nev. 2020) aff'd No. 20-10303 (9th Cir. Jan. 6, 2022)

- Facts of the case
- Issue: Did warrantless, non-consensual use of W's biometric info violate 4th or 5th Amend? If so, does it justify suppression of tablet data?

Court Holding

- Ct.: Yes, it is testimonial and therefore violates the 5th Amendment. Court avoids ruling on 4th Amendment based on above. Ct said:
  1. Biometric is functionally the same as a passcode. Since telling a passcode would be testimonial, harvesting a biometric is too.
  2. Unlocking a phone equates to testimony you have unlocked it before, showing control over the device, which is very important in a child porn possession case
- Court suppresses evidence from phone, but not tablet, smartwatch.
- Courts are split on this, though above analysis is an outlier.
- What if faceprint was lifted from public images?
- Takeaway: Case law is unclear on this issue, but organizations may wish to consider whether policies are necessary to mandate a passcode vice a biometric until the law is clarified.

Evidence Preservation

Edwards v. Junior State of America Found., 2021 WL 1600282 (E.D. Tex. Apr. 23, 2021)

- Facts of the case
- Issue: Are images of offensive Facebook Messenger messages legally sufficient, or must plaintiff produce messages in original HTML or JSON format?

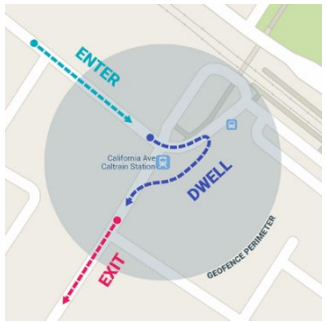
Court Holding

- Ct: Defendant's motion to dismiss granted in part. Key evidence was excluded on the basis of F.R.C.P. 37(c), failing to provide information required in initial disclosure.
  1. Preservation of .jpeg images of a part of a screen ruled incomplete. Needed to provide html or json versions to permit the defense to authenticate the images.
  2. Plaintiff's act of permanently deleting his Facebook account destroyed the alleged messages.
- *Brown* court distinguished between account deactivation (potentially recoverable) and deletion (permanently lost)
- Takeaway: As organizations deal increasingly with a dispersed workforce, due to the pandemic, with employees using a wide variety of collaboration tools, organizations should ensure data necessary for litigation is appropriately preserved, in an appropriate format.

Geofence Warrants

United States v. Chatrie, No. 3:19-cr-130 (E.D. Va, Mar. 3, 2022)

- Facts of the case
- Issue: Does obtaining 2 hours of Google "location history" under a geofence warrant violate the constitution as a "general warrant"?



Court Holding

- Ct: Yes, but Defendant's motion to suppress denied. Ct held this geofence warrant plainly unconstitutional, but upheld under the good faith exception.
- Geofenced area included a major road, restaurant, hotel, and church during rush hour. As such, it is a general warrant seeking dragnet information on a large number of innocent people.
- US: (1) Def. had no REOP in 2 hours of location history, not a search, consented to collection, (2) Warrant satisfied 4th Amend., (3) Good faith
- Google: Location history is more accurate than data in Carpenter, but is collected via "consent" of user.
- Still unclear this is a "search" (though court treated it as one since Google required a warrant). Ct seemed to erroneously require individualized PC for all in geofence.
- Takeaway: While highly critical of geofence warrants, the court's analysis failed to clearly answer many complex questions leaving still more questions.

Cases and Issues to Watch

- Blockchain Smart contracts: "code is law"
  - Smart contracts are based on code that self-executes upon the satisfaction of certain conditions. Jurisdictions grappling with how to deal with these. The UK has deemed they can be valid contracts.
  - As code they can be hacked. Poly Networks lost $600 million via a hacked smart contract. Pressure and pleas got some of the money back.
- *Apple v. NSO Group, 2021 WL 5490649*
  - Apple alleges violations of CFAA, Calif. Bus. & Prof. Code § 17200, breach of contract (iCloud terms), and unjust enrichment.
  - Some claims appear to be based on CFAA violations by NSO Group against Apple's users (vice against Apple)

Cases and Issues to Watch

- Cyber insurance
  - *Mondelez Int'l v. Zurich American Insurance*, No. 2018L011008 (Ill. Cir. Ct.) still pending based on denial of $100 million NotPetya claim
  - Will court follow *Merck* court's analysis? How will insurers respond?
  - Exclusion for "hostile or warlike acts" was based on attribution of NotPetya to Russia (Will 2022 Russia/Ukraine hostilities create new fallout?)
  - What of SolarWinds, MS Exchange hack, Pulse Secure?
- Takeaway: Companies seeking cyber insurance should be wary of war exclusions, broad recission clauses, and "similar quality" / "betterment" clauses.
- US Office of Foreign Assets Control (OFAC) guidance: Beware of ransomware payments to certain entities. Strict liability for victim, insurer, and forensic company

"Apply" Slide

- Next week you should:
  - Take actions to update your organization's policies to minimize risk with regards to the use of biometric data; ensure your evidence preservation policy mandates original format or is cleared by your legal team
- Within three months you should:
  - Review your organization's exposure to GDPR or CCPA-related suits and start preparing for CPRA, Virginia's, NY's, and CO's related laws
- Within six months you should:
  - Take actions to update your organization's policies to minimize risk with regards to insurance providers; review and update compliance programs and ransom policies to mitigate sanctions risks

RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **LAW-M06**

What Have the Courts Done Now? Explaining the Impact of Recent Cyber Cases

Rick Aldrich
Lead Cybersecurity Policy & Compliance Analyst
Booz | Allen | Hamilton
@AldrichRick, Aldrich_Richard@bah.com

Julie Bowen
Senior VP, GC, and Corp. Sec'y
Mitre Corporation
jbowen@mitre.org