Emerging Developments in Cyberlaw: 2023

Rick Aldrich, JD, LL.M, CISSP, CIPT, GLEG
Aldrich_Richard@bah.com, 703-545-2329
CSIAC, Aug 2023

Legal Caveat

- Presentation is not legal advice*
- Designed to raise awareness of general legal principles applicable to information assurance and cyber security
- 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.

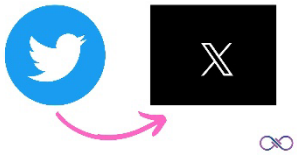
*The information contained in this briefing is for general guidance on matters of interest only. The application and impact of laws can vary widely based on the specific facts involved. Given the changing nature of laws, rules and regulations, there may be omissions or inaccuracies in information contained in this presentation. Accordingly, the information in this presentation is provided with the understanding that the author is not herein engaged in rendering legal advice and services. As such, it should not be used as a substitute for consultation with professional legal advisers.

Agenda

- Recent Supreme Court Cases
- Important Bills
- New Strategies
- Significant Recent Cases

Pending Supreme Court Cases

- *Gonzalez v. Google, No. 21-1333*
  - Facts
    - Father of fatal victim of ISIS terrorists attacks sues Google, et al, for aiding and abetting terrorism by permitting ISIS to post videos on YouTube and via Google's algorithms that suggested such content based on some users' viewing or search history
  - Issue
    - Does Section 230(c)(1) of the Communications Decency Act immunize interactive computer services when they make targeted recommendations of information provided by another information content provider?
  - Ruling: Vacated and remanded in light of *Twitter* case
- *Twitter v. Taamneh, No. 21-1496*
  - Facts (very similar to above)
  - Issues
    - Does an internet platform "knowingly" provide substantial assistance under 18 U.S.C. § 2333 merely because it allegedly could have taken more "meaningful" or "aggressive" action to prevent such use?
    - May an internet platform whose services were not used in connection with the specific "act of international terrorism" that injured the plaintiff still be liable for aiding and abetting under Section 2333?
    - Ruling: Reversed: "Mere creation of" social media platform not culpable.



FISA

- Section 702 of the FISA is set to expire on 31 Dec 2023
- Section 702
  - Provides an exigent circumstances exception to the FISA warrant requirement upon approval of both the AG and DNI
  - Permits foreign intelligence acquisition against persons located outside the US and not believed to be US persons
- Current Administration supports reauthorization based on successes. Some examples include:
  - Identified multiple foreign ransomware attacks aiding in prevention, response, and mitigation
  - Aided in identifying Al Qaeda threats against US troops and targeting its top leader in 2022
  - Aided in thwarting foreign adversaries' effort to obtain weapons of mass destruction
  - Thwarted foreign attempts to recruit spies in the U.S.

FANFSA

Fourth Amendment Is Not For Sale Act

- H.R. 4639 (of 118th Congress)
  - Would prevent law enforcement and intelligence agencies from obtaining subscriber or customer records in exchange for anything of value, to address communications and records in the possession of intermediary internet service providers
  - Aimed at a perceived circumvention of the 4th Amendment, where LE or Intel agencies buy records rather than obtain warrant or court orders to get similar information
  - Would apply to records of persons in the US and US persons outside the US
  - Has bipartisan support
  - May be attached to a must-pass bill

National Cybersecurity Strategy

- Key Takeaways
  - Focus shifted from “cyber” to “cybersecurity”
  - Seeks to rebalance the cybersecurity burden
    - Shift from end users to “most capable and best positioned actors”
    - Begin to shift liability for insecure software to vendors
  - Recognizes DoD’s role in defending against state and non-state sponsored acts that pose strategic-level threats
  - National Cyber Investigative Joint Task Force (NCIJTF) to be expanded
  - Federal cyber insurance backup to be explored

Significant Cases

- "Reverse Warrants"
  - Geofence Warrants
  - Keyword Warrants
- Privacy
- Biometrics
- Evidence preservation
- License Plate Readers
- Cyber Insurance
- Blockchain

Geofence Warrants

United States v. Rhine, No. 21-0687 (RC) (D. D.C., Jan. 24, 2023)

- Rhine charged with multiple crimes as part of the Jan 6 riot.
- FBI serves geofence warrant on Google for location data from all devices within/around Capitol from 2:00-6:30 on Jan 6.
- Warrant included 3-step process that started with anonymized data (5,723 accounts) but culled to exclude those from control list times, then culled to 1,498 in Capitol (+37 of 70 who deleted their Location History [LH] data after Jan 6).
- Later warrant for D's CSLI based on LH, tip, video surveillance.
- D moves to suppress under 4th Amend
- Issue: Does obtaining Google LH data under a geofence warrant violate the constitution as a "general warrant"?

Geofence Warrants

United States v. Rhine, No. 21-0687 (RC) (D. D.C., Jan. 24, 2023)

- Rhine charged with multiple crimes as part of the Jan 6 riot.
- FBI serves geofence warrant on Google for location data from all devices within/around Capitol from 2:00-6:30 on Jan 6.
- Warrant included 3-step process that started with anonymized data (5,723 accounts) but culled to exclude those from control list times, then culled to 1,498 in Capitol (+37 of 70 who deleted their Location History [LH] data after Jan 6).
- Later warrant for D's CSLI based on LH, tip, video surveillance.
- D moves to suppress under 4th Amend
- Issue: Does obtaining Google LH data under a geofence warrant violate the constitution as a "general warrant"?

Court Holding

- Ct: No. The FBI met the particularized probable cause standard. Regardless, it would have been upheld under the Good Faith exception
- US: (1) Def. had no REOP in his LH in the Capitol to collection so no 4th Amend issue or (2) Warrant satisfied 4th Amend
- Court: (1) Declines to rule on this issue, because Ct ruled in favor of Gov't on (2).
- D replied (1) "overbreadth" (Google searched millions of innocent records), Capitol closed to public (2) Google shouldn't have provided records prior to deletion, (3) control lists were a violation
- Court: (1&2) What Google does is not relevant to validity of warrant. Plus, data was anonymized. (3) Control lists actually minimized deanonymizations
- Takeaway: While the law on geofence warrants is still scant, the court's analysis upheld its constitutionality via the 3-step approach and the facts of this case. Now that this type of warrant is so popular it will come up increasingly for review.

Keyword Warrants

Colorado v. Seymour, No. 21CR20001 (Denver D.C., Jan. 24, 2023)

- Arsonists set fire to a house in Colorado that killed a Senegalese family of five, ranging in age from 2 months to 29 years old.
- Police had no leads, so employed a variety of techniques, including cell site simulators (Stingrays), tower dumps, geofence warrant, data purchases from a data broker, and multiple keyword search warrants.
- Police asked Google for IP addresses that searched for the house address over 15 days.
- Final keyword search identified Seymour and two other teens. The arson was to avenge a phone theft, but they picked the wrong house.
- D moves to suppress under 4th Amend
- Issue: Does obtaining IP addresses associated with keyword searches violate the 4th Amendment as a "general warrant" or its Colorado equivalent?

Keyword Warrants

Colorado v. Seymour, No. 21CR20001 (Denver D.C., Jan. 24, 2023)

- Arsonists set fire to a house in Colorado that killed a Senegalese family of five, ranging in age from 2 months to 29 years old.
- Police had no leads, so employed a variety of techniques, including cell site simulators (Stingrays), tower dumps, geofence warrant, data purchases from a data broker, and multiple keyword search warrants.
- Police asked Google for IP addresses that searched for the house address over 15 days.
- Final keyword search identified Seymour and two other teens. The arson was to avenge a phone theft, but they picked the wrong house.
- D moves to suppress under 4th Amend
- Issue: Does obtaining IP addresses associated with keyword searches violate the 4th Amendment as a "general warrant" or its Colorado equivalent?

Court Holding

- D/Ct: No. Warrant was "specific," "procedurally sound," and "supported by probable cause." The search of billions of Google's records was done by Google, not the police.
- Currently on appeal at the Colorado Supreme Court. Oral argument heard May 4, 2023.
- At issue in the CO S/C was the *Tattered Cover* case, a 2002 CO S/C which established a higher standard for warrants (compelling need/alt. reasonable means) in 1st Amend. right to receive information cases. (Police found meth lab with drug-making books mailed to suspect. Police served a warrant on the book store for all books purchased by a suspect.) Question whether this standard applies in this case.
- Takeaway: The law on keyword warrants is virtually non-existent. May depend on how courts apply *Carpenter, Jones*, and the geofence cases.

4th Amendment

Wisconsin v. Bowers, 2021AP1767-CR (Ct of Apps Dist. III, Dec. 29, 2022)

- Taylor County Sheriff's Dept agreed to work with TV show "Cold Justice" by sharing a cold murder case (M1).
- Det. Bowers unilaterally decided to share two additional murder cases (M2 & M3) via a personal Dropbox account that used his county email address.
- Taylor County sought to access Bowers' Dropbox account, but Dropbox was uncooperative.
- Taylor County IT Dept. then forced a password reset on Bowers' account and accessed the response email by accessing his county email.
- County contends that Bowers had no REOP in the Dropbox account, but if he did, search justified by prob cause and exigent circumstances
- Issue: Bowers moves to suppress the files obtained by the County's access to the files in his Dropbox account. Who prevails?

4th Amendment

Wisconsin v. Bowers, 2021AP1767-CR (Ct of Apps Dist. III, Dec. 29, 2022)

- Taylor County Sheriff's Dept agreed to work with TV show "Cold Justice" by sharing a cold murder case (M1).
- Det. Bowers unilaterally decided to share two additional murder cases (M2 & M3) via a personal Dropbox account that used his county email address.
- Taylor County sought to access Bowers' Dropbox account, but Dropbox was uncooperative.
- Taylor County IT Dept. then forced a password reset on Bowers' account and accessed the response email by accessing his county email.
- County contends that Bowers had no REOP in the Dropbox account, but if he did, search justified by prob cause and exigent circumstances
- Issue: Bowers moves to suppress the files obtained by the County's access to the files in his Dropbox account. Who prevails?

Court Holding

- Ct: Yes, County's access violated Bowers' 4th Amendment rights.
- County relied on a policy statement signed by Bowers that stated, "I have no expectation of privacy for any material on Taylor County equipment, even if that material was generated for my personal use." But materials were not seized from County equipment.
- Court applied the two-part test:
  - Subjective expectation of privacy: County did not contest
  - Objective expectation of privacy was reasonable due to password protection
- Third-party exception did not apply in light of *Carpenter, Riley*, and fact that County didn't obtain documents from Dropbox (3rd party)
- County loses on exigent circumstances exception because Dropbox holds deleted files for 30 days and County failed to seek a preservation order.
- Takeaway: Ensure your organization knows where its sensitive data is and can protect against its unauthorized removal. (And don't force password resets for those who use a government email address.)

State Secrets

FBI v. Fazaga, 595 U.S. ___ (2022)

- FBI uses a confidential information for 14 months to conduct covert surveillance on the Islamic Center of Irvine (ISOI), CA. Included wearing and planting recording devices, then suggesting violent actions. ISOI reported him to police and obtained restraining order against him.
- Fazaga (an others from ISOI) assert violations of 1st, 4th, and 5th (due process clause), and FISA, et. al.
- US AG asserts "state secrets privilege."
- D/C dismisses most claims. 9th Cir. reversed allowing class action to proceed. FBI appeals.
- Issue: Does Section 1806(f) of FISA displace the state-secrets privilege and authorize a district court to resolve the merits of a lawsuit challenging the lawfulness of government surveillance by considering the privileged evidence?

FBI v. Fazaga, 595 U.S. ___ (2022)

- FBI uses a confidential information for 14 months to conduct covert surveillance on the Islamic Center of Irvine (ISOI), CA. Included wearing and planting recording devices, then suggesting violent actions. ISOI reported him to police and obtained restraining order against him.
- Fazaga (an others from ISOI) assert violations of 1st, 4th, and 5th (due process clause), and FISA, et. al.
- US AG asserts "state secrets privilege."
- D/C dismisses most claims. 9th Cir. reversed allowing class action to proceed. FBI appeals.
- Issue: Does Section 1806(f) of FISA displace the state-secrets privilege and authorize a district court to resolve the merits of a lawsuit challenging the lawfulness of government surveillance by considering the privileged evidence?

Court Holding

- No. In 9-0 decision S/C holds § 1806(f) of FISA did not displace state secrets privilege.
- State secrets privilege arose from common law or constitution, but not mentioned at all in FISA, so was not affected by it.
- This decision, issued on 4 Mar 2022, may complicate the EU/US announcement of an "agreement in principle" on Privacy Shield 2.0 because it seems to close the door on EU citizens' ability to challenge perceived privacy violations.
- Case was heard in the 9th Cir. on remand on 23 Jun 2023. (Case is based on FBI actions beginning in 2006.)

Biometrics

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

- Bennet tells agent that he found ~20 child porn images on tablet that Wright loaned him. Agent arrested Wright for failure to update sex offender registration, seized electronic devices, including watch, phone, tablet.
- Agent used warrantless, non-consensual face ID to open phone.
- Wright claims flagrant disregard of 5th Amend warrants suppression of evidence.
- Issue: Did warrantless, non-consensual use of Wright's biometric info violate 4th or 5th Amend? If so, does it justify suppression of tablet data?

Biometrics

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

- Bennet tells agent that he found ~20 child porn images on tablet that Wright loaned him. Agent arrested Wright for failure to update sex offender registration, seized electronic devices, including watch, phone, tablet.
- Agent used warrantless, non-consensual face ID to open phone.
- Wright claims flagrant disregard of 5th Amend warrants suppression of evidence.
- Issue: Did warrantless, non-consensual use of Wright'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 somewhat 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, so law enforcement is best advised to seek consent, a warrant, or leverage password cracking tools.

Preservation Orders

United States v. Rosenow, No. 20-50052 (9th Cir., Jun. 8, 2022, amended Oct. 3, 2022)

- Rosenow (R) was convicted of two crimes related to child sexual abuse and child porn. R arranged activities via Yahoo and Facebook.
- FBI executed several evidence preservation orders (EPOs), under 18 USC § 2703(f) to preserve evidence of crimes.
- R moved to suppress under 4th Amend alleging the EPOs were unlawful warrantless seizures
- Issue: Does the execution of an EPO under these facts constitute a 4th Amend violation?

18 USC § 2703(f)

Preservation Orders

United States v. Rosenow, No. 20-50052 (9th Cir., Jun. 8, 2022, amended Oct. 3, 2022)

- Rosenow (R) was convicted of two crimes related to child sexual abuse and child porn. R arranged activities via Yahoo and Facebook.
- FBI executed several evidence preservation orders (EPOs), under 18 USC § 2703(f) to preserve evidence of crimes.
- R moved to suppress under 4th Amend alleging the EPOs were unlawful warrantless seizures
- Issue: Does the execution of an EPO under these facts constitute a 4th Amend violation?

18 USC § 2703(f)

Court Holding

- Ct: No. Court's rationale is potentially wide-reaching and precedent-setting:
- "applied only retrospectively, did not meaningfully interfere with Rosenow's possessory interests in his digital data because they did not prevent Rosenow from accessing his account. Nor did they provide the government with access to any of Rosenow's digital information without further legal process."
  - Would this permit large scale EPOs to be routinely issued, just in case…
  - Court amended its opinion to decline addressing the 4th Amendment issue
- "It also is worth noting that Rosenow consented to the ESPs honoring preservation requests from law enforcement under the ESPs' terms of use."
  - Would this allow 4th Amend rts to be negated via TOS? (Also removed in the amended opinion)
- Takeaway: District courts divided on the constitutionality of EPOs. No other Circuit court has ruled on this issue (2nd Cir ruling was vacated for other reasons). Potential breadth of initial holding could have significantly broadened use of EPOs, but amended opinion leaves current law intact.

CFAA

WhatsApp (Facebook) v. NSO Group, No. 20-16408 (9th Cir., Nov. 8, 2021)

- Plaintiff alleges NSOG sent malware (Pegasus) to 1400 mobile devices to access WhatsApp messages after they were decrypted on the devices (to circumvent WhatsApp's end-to-end encryption).
- This was in violation of WhatsApp's TOS and in violation of the CFAA § 1030(a)(2) (intentionally accessed protected computers w/o authorization), § 1030(a)(4) (knowingly accessed protected computers w/intent to defraud), and § 1030(b)(2) (conspiracy), causing >$5000 damage w/in 1 year based on P's costs to investigate and remediate.
- TOS not only prohibited privacy violating conduct and reverse engineering of code, but also assisting others in doing so.
- Issue: Did NSO Group violate the CFAA by its actions?

CFAA

WhatsApp (Facebook) v. NSO Group, No. 20-16408 (9th Cir., Nov. 8, 2021)

- Plaintiff alleges NSOG sent malware (Pegasus) to 1400 mobile devices to access WhatsApp messages after they were decrypted on the devices (to circumvent WhatsApp's end-to-end encryption).
- This was in violation of WhatsApp's TOS and in violation of the CFAA § 1030(a)(2) (intentionally accessed protected computers w/o authorization), § 1030(a)(4) (knowingly accessed protected computers w/intent to defraud), and § 1030(b)(2) (conspiracy), causing >$5000 damage w/in 1 year based on P's costs to investigate and remediate.
- TOS not only prohibited privacy violating conduct and reverse engineering of code, but also assisting others in doing so.
- Issue: Did NSO Group violate the CFAA by its actions?

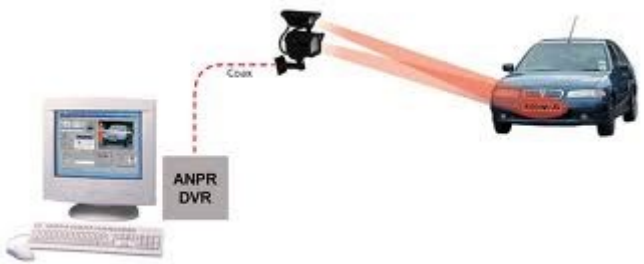
Holding

- Stay tuned…case still developing
- D/C's ruling that NSO Group could not claim sovereign immunity under FSIA upheld by 9th Cir. (and rhrg pet denied)
- US S/C denied cert. on Jan 9, 2023. Trial is set to begin Dec 2, 2024.
- First CFAA violation based on TOS violations, but under S/C's ruling in Van Buren this seems a "gates down" case
- Additional issues:
  - Arguably the devices hacked were those of private citizens, not WhatsApp.
  - WhatsApp claims NSOG reverse-engineered WhatsApp code to emulate WhatsApp network traffic using WhatsApp servers
  - NSOG code "burdened" WhatsApp network
- Even if WhatsApp doesn't win
  - It may raise awareness among customers and burnish WhatsApp's reputation
  - It may shame NSO Group into vetting clients
  - May help Facebook fight government demands it provide back doors to its E2E encryption
- Takeaway: May presage a new era in data privacy litigation

ALPR

Canosa v. City of Coral Gables, No. 2018-33927-CA-01 (Oct. 4, 2021)

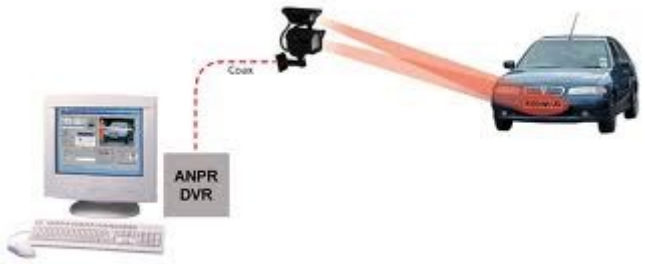
- Canosa, a resident of Coral Gables, sues the city of Coral Gables over the use of 30 strategically placed automatic license plate readers (ALPRs), storing data on 106 million license plates for 3 years and made available to 68 other jurisdictions.
- Canosa alleges the practice violates the Fourth Amendment of the US Constitution and its analog under the Florida constitution. The suit seeks declaratory judgments on nine counts seeking to stop various state government entities from collecting, storing, sharing, etc. data from its ALPR system
- City collected 393 photos of Canosa with date/time/lat/long and nearest intersection.
- Issue: Does operating the ALPR system violate the 4th Amendment?



ALPR

Canosa v. City of Coral Gables, No. 2018-33927-CA-01 (Oct. 4, 2021)

- Canosa, a resident of Coral Gables, sues the city of Coral Gables over the use of 30 strategically placed automatic license plate readers (ALPRs), storing data on 106 million license plates for 3 years and made available to 68 other jurisdictions.
- Canosa alleges the practice violates the Fourth Amendment of the US Constitution and its analog under the Florida constitution. The suit seeks declaratory judgments on nine counts seeking to stop various state government entities from collecting, storing, sharing, etc. data from its ALPR system
- City collected 393 photos of Canosa with date/time/lat/long and nearest intersection.
- Issue: Does operating the ALPR system violate the 4th Amendment?



Holding

- No.
- Ct held plaintiff lack "concrete injury" because the City had not queried or searched the ALPR database for Canosa's data (except pursuant to his request for his case).
- Further, City's guidelines indicate it will only use the data in a lawful manner for criminal and intelligence needs.
- Distinguished from *Carpenter* as not a cell phone that follows the person beyond public throughfares. Distinguished from *Jones* because ALPR cameras are fixed, so different from GPS tracker.
- Case has been appealed to the FL circuit court.
- Compare with *Commonwealth v. McCarthy,* 484 Mass. 493 (2020), which held that while "enough cameras in enough locations" may trigger a 4th Amend violation, 4 ALPRs on 2 bridges did not.

Evidence Preservation

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

- Edwards is the father of a high school student who was sent racist and homophobic messages via Facebook. Messages were sent by Harper, a H.S. student, as part of JSA.
- JSA conducted an internal investigation, but could not find messages on Harper's phone. Edwards provided .jpeg images from son's phone, but JSA additional evidence.
- Issue: Are images of offensive Facebook Messenger messages legally sufficient, or must plaintiff produce messages in original HTML or JSON format?

Evidence Preservation

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

- Edwards is the father of a high school student who was sent racist and homophobic messages via Facebook. Messages were sent by Harper, a H.S. student, as part of JSA.
- JSA conducted an internal investigation, but could not find messages on Harper's phone. Edwards provided .jpeg images from son's phone, but JSA additional evidence.
- 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.

Cyber Insurance

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

- Merck is pharmaceutical company
- M was hit by NotPetya, suffering ~$1.4B in damages, bricking 40,000 computers.
- NotPetya was a cyber-attack that appeared to be originally directed against Ukrainian organizations, but which ultimately caused over $10 billion in damages around the world.
- Disguised to appear like Petya which was a criminal ransomware
- M had a $1.75B policy just for such events and filed a claim against Ace under the provision covering “all risks”: “physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction ....”
- Issue: Is collateral damage from NotPetya excluded under an “act of war” exclusion from insurance coverage?

Cyber Insurance

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

- Merck is pharmaceutical company
- M was hit by NotPetya, suffering ~$1.4B in damages, bricking 40,000 computers.
- NotPetya was a cyber-attack that appeared to be originally directed against Ukrainian organizations, but which ultimately caused over $10 billion in damages around the world.
- Disguised to appear like Petya which was a criminal ransomware
- M had a $1.75B policy just for such events and filed a claim against Ace under the provision covering "all risks": "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction ...."
- 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 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?
- Takeaway: While insurer lost here, *Mondelez* was later settled for an undisclosed amount.
- 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.

Cases and Issues to Watch

- *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)
- 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. Several US states have adopted specific laws, while others may recognize such contracts under existing law.
  - 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.
  - Immutability and coding errors create risks for these contracts

Summary

- Trends
  - Fourth Amendment continues to evolve with technology
    - Reverse warrants raise interesting new issues
    - Biometrics may challenge privacy protections
    - Data brokers may afford end runs around the 4th Amendment
    - *Carpenter, Jones,* and *Riley* all suggest equilibrium adjustment
  - Computer Fraud and Abuse Act
    - Supreme Court resolves Circuit split
    - Apple and Meta press the envelope with suits against NSO
  - Cyber insurance and "war" exclusions raise new concerns
  - Blockchain contracts blur legal/technical issues
- Understand implications—cyberlaw is still immature/evolving

Questions?

Rick Aldrich, JD, LL.M, CISSP, CIPT, GLEG
Aldrich_Richard@bah.com, 703-545-2329
American Bar Association, ISC, 23 Apr 2023

Geofence Warrants

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

- Defendant passed a note to a credit union teller demanding $100K and threatening the teller's family and ultimately brandishing a gun to obtain $195K.
- Police reviewed surveillance video to see robber used a phone. Police applied for and obtained a geofence warrant for account information (including name and email) on all phones within a 150' radius of the credit union during a 2-hour period around the robbery.
- Warrant includes 3-step process that started with anonymized data (19 accounts) but narrowed the scope at each stage and obtained name and email at stage 3 (3 accounts).
- D moves to suppress under 4th Amend
- 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.

Computer Fraud & Abuse Act

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

- Van Buren (VB) was a Georgia law enforcement officer. His role authorized him to search databases with license plate data.
- VB was allegedly "shaking down" Andrew Albo (AA) for money. The FBI conducted a sting using AA, asking VB to check the database for a stripper's license plate to see if she was an undercover officer. AA paid $5000 and provided a fake plate number.
- VB ran the fake plate through the database.
- VB charged with multiple felonies including "exceeding authorized access" under CFAA.
- Issue: Does 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.

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

- Austrian attorney Max Schrems originally won a case in *Irish DPC v. Facebook Ireland* over the Safe Harbor mechanism (Schrems I)
- EU-US Privacy Shield replaces the Safe Harbor mechanism, FB Ireland resumes transferring data to the US.
- Schrems II challenged Privacy Shield based largely on concerns over intelligence surveillance under FISA.
- 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.