Emerging Developments in Cyberlaw: 2019

Rick Aldrich, JD, LL.M, CISSP, CIPT, GLEG

American Bar Association, Information Security Committee, 3 Mar 2019

CSIAC (https://www.csiac.org)

- **Cyber Security and Information Systems Information Analysis Center (CSIAC)**
  - A Department of Defense (DoD) **Information Analysis Center (IAC)** sponsored by the Defense Technical Information Center (**DTIC**).
  - Consolidation of three predecessor IACs: the **Data and Analysis Center for Software (DACS)**, the **Information Assurance Technology IAC (IATAC)** and the **Modeling & Simulation IAC (MSIAC)**, with the addition of the **Knowledge Management and Information Sharing** technical area.
- **Basic Center of Operations (BCO)** collects and disseminates Scientific & Technical Information
  - Also performs up to four hours of support (free of charge) in response to **Technical Inquiries**.
  - Can also provide services as **Core Analysis Tasks (CATs)** procured and funded through the issuance of Delivery Orders (DO).
- CSIAC is chartered to leverage the best practices and expertise from government, industry, and academia in order to promote technology domain awareness and solve the most critically challenging scientific and technical problems in the following areas: Cybersecurity and Information Assurance, Software Engineering, Modeling and Simulation, and Knowledge Management/Information Sharing.

Legal Caveat

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

*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.

Recent Legislation

- California SB-1001:
  - Makes it unlawful for any person to
    - use a bot to communicate or interact with another person in California online,
    - with the intent to mislead the other person about its artificial identity
    - for the purpose of knowingly deceiving the person about the content of the communication
    - in order to incentivize a purchase or sale of goods or services in a commercial transaction
    - or to influence a vote in an election
  - Signed into law Sept 28, 2018, effective July 1, 2019

Recent Legislation

- California Consumer Privacy Act:
  - Has some provisions that are similar to the GDPR
    - Right to be forgotten
    - Right to data portability
    - Right to access data
  - But several important differences as well
    - Scope
    - Accountability
  - Signed into law June 28, 2018, effective Jan 1, 2020

Significant Recent Case Law

- Scope of 3rd Party Doctrine
- CFAA
- Border Searches
- Consent
- Biometrics
- Standing
- Private Search Doctrine
- Insurance
- Quick Updates
- Cases to Watch

3rd Party

Carpenter v. United States, 138 S. Ct. 2206 (2018)

- Several participate in armed robberies of Radio Shack and T-Mobile stores over 4 months
- 4 robbers later arrested. One confessed and provided his cell phone to FBI.
- FBI identified 16 phone numbers of interest and sought historic cell-site location info (CSLI) for each for 127 days from carriers under SCA (requiring only a showing of relevance to an ongoing criminal investigation, not the higher probable cause standard for warrants).
- Magistrate grants order. Carpenter identified in cell-site data, tried, convicted, sentenced to 116 years.
  - Issue: Is the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 127 days permitted by the Fourth Amendment.

Holding

- 6th Cir: Yes, because
  1. The current law protects "content" but not "transactional" information.
  2. Records were carrier's business records, subject to 3rd party doctrine
  3. *Jones* does not apply because government didn't do extended GPS monitoring, carriers collected the data, and GPS monitoring is 12,500 times more accurate than cell-site locations.
  4. *Riley* doesn't apply because amount of data stored on a cell phone is not applicable to cell-site location.
- S/C: No. Facts fit intersection of *Jones*, *Miller/Smith* (3rd party) cases, and *Riley* ("privacies of life"). Equilibrium adjustment.
- Declines to extend 3rd party doctrine to CSLI as it is qualitatively different: "near perfect surveillance" akin to ankle monitor. Ct anticipated tech developments.
- "Narrow" holding doesn't address sting rays, tower dumps, conventional techniques such as security cameras, nor FISA techniques.
- Takeaway: For companies that collect sensitive data, this case may provide a basis to resist warrantless requests from the government. Review customer privacy agreements for impact on REOP.

3rd Party

United States v. Eugene, No. 18-0209/AR (CAAF 2018)

- PFC Eugene gives his cell phone to his wife prior to deployment because cell phones are prohibited on deployment.
- He places no limitations on her use. She finds Kik contacts with underage girls on the phone that included videos and nude photos.
- She reports it to Army CID and consents to CID's search of the phone. A logical extraction reveals no evidence. (Allegedly due to phone being placed in airplane mode.) Later PFC Eugene returns and requests the phone be returned to him. CID refuses. Months later a more detailed electronic search provides evidence against defendant.
- Issue: Can the cell phone's owner revoke the 3rd party consent of his wife as one with equal or superior access or control? (*Georgia v. Randolph* held such for homes.)

Holding

- T/C judge: Not answered, because PFC Eugene's request for return of phone from CID was not unequivocal revocation of consent to search. Seemed like he wanted it back, most likely just so he could use it.
- Army CCA: Affirmed. Eugene's request was merely an attempt to regain his phone for personal convenience. Alternatively, inevitable discovery doctrine applies.
- CAAF: Same, because issue is a question of fact and the court affords deference to judge on motions to suppress.
  - While no "magic words" necessary, PFC Eugene's request for return of phone seemed at most an objection to the seizure, not to the search.
- Takeaway: Use "magic words:" "I explicitly revoke consent to any search and/or seizure of [any or all device(s) in question]." Still may not work because most courts have held *Georgia v. Randolph* limited to homes.

CFAA

Mathey Dearman v. H&M Pipe Beveling, No. 18-cv-250-GKF-JFJ (N.D. Okla., Sept. 5, 2018)

- MD is a company that manufactures and markets a variety of industrial products used in a wide array of industries. Expends significant resources to protect its confidential information. (Aside: Dropbox w/password?)
- Boyd and Wilson, codefendants, served as Global and Area Sales Managers respectively, and had privileged access to confidential information. Both decided to work for competitor H&M and copied 80,000+ confidential files and transferred them to H&M prior to their departure.
- Boyd deleted thousands of MD files, email, and reset his corporate smartphone to factory settings.
- All sued on multiple charges including some under CFAA
- How should court rule on motions to dismiss:
  1. CFAA sections alleging they accessed a protected computer "without authorization" to transfer confidential information?
  2. CFAA sections alleging they accessed a protected computer "exceeded authorized access" to transfer confidential information?
  3. CFAA section alleging Boyd "intentionally cause[d] damage without authorization, to a protected computer" by deleting files, emails on corporate laptop and smartphone?

Holding

Court rules to

1. Dismiss, because MD concedes they had privileged access, so access was not "without authorization"
2. Dismiss, because MD concedes they had privileged access, so access did not "exceed authorized access."
3. No dismissal, because does not depend on "access" without or exceeding authorization, but rather "damage" without authorization.

- Issues in items 1 & 2 have created a circuit split:
  - 2nd, 4th, and 9th Circuits focus on objective grant of access by the employer, not the defendant's intent or purpose in that access
  - 1st, 5th, 7th, and 11th, permit a defendant to be held liable based on an improper purpose
- This court (in the 10th Cir.) sides with first group, absent binding 10th Cir. Precedent
  - Congress meant to deter hacking, not purposes for access
  - Primarily a criminal statute, so should be interpreted so as not to impose unexpected liability
- This issue seems ripe for Supreme Court review
- Takeaway: Limit privileged access, don't expect CFAA remedy

CFAA

United States v. Manning, No. 20130739 (Army Ct. Crim. App., May 31, 2018)

- Bradley Manning (nka Chelsea Manning) was convicted under Article 134 (general article) of violating the CFAA by "exceeding authorized access."
- CM was charged with accessing the SIPRNet to obtain >75 classified Dept of State (DoS) cables which she later transmitted to Wikileaks.
- CM obtained the DoS cables using Wget, a program that she uploaded to the SIPRNet. Wget facilitates downloading and copying enormous amounts of information quickly, so as to avoid manually downloading each piece of data.
- CM was authorized SIPRNet access and access to DoS cables. Convicted at trial.
- How should court rule on appeal?

Holding

- Case of first impression for military courts.
- Holds CM "exceeded authorized access" by the manner she accessed the DoS cables so conviction upheld.
- The Circuit split in federal courts is between (1) the broad interpretation (includes improper purpose) and (2) narrow interpretation (requires bypassing controls)
- T/C used latter approach, so Army CCA applies same without ruling which approach is proper
- Army CCA seems to create a third interpretation: "beyond the manner" authorized
- CM went beyond the manner authorized by using Wget in apparent violation of authorized use policy (AUP) generally prohibiting the uploading of executable programs without authorization or using freeware on a government computer without authorization.
- Had CM accessed DoS files in traditional way 75 times, "it would be a different issue."

Border Searches

United States v. Touset, 890 F.3d 1227 (11th Cir., 2018)

- T identified as a child porn suspect due to pattern of low dollar transfers to persons in countries associated with sex tourism. Xoom alerted Yahoo based on email and messenger accounts.
- Yahoo found child porn in an associated email, sent alerts to NCMEC, DHS.
- When T arrived in Atlanta on int'l flight, CBP inspected electronic devices, did forensic searches on 4 of them. Found child porn on all four. Later Gov't obtained search warrants for home and found more evidence of child porn.
- T challenges forensic border search, alleging no reasonable suspicion because Western Union money transfers were 1.5 years old, so stale.
- How should court rule?
  1. Does forensic border search of computers require reasonable suspicion?
  2. If so, was it present or stale?

Holding

- Magistrate: Reasonable suspicion is proper standard and was present.
- District court: Reasonable suspicion is proper standard and was present.
- 11th Cir.: Reasonable suspicion not required for search of computers and like devices at the border.
  - Reasonable suspicion only required for invasive searches of the body (strip searches or x-rays)
  - Refuses to extend rationale Riley (search incident to lawful arrest not applicable to cell phones—requires a warrant) to border searches
- Extends split among circuits:
  - 4th and 9th have held computer searches at the border require reasonable suspicion
- Alternately, if reasonable suspicion is required, it was present here
  - Pedophiles rarely if ever delete files of child porn, so the basis for the reasonable suspicion was not stale
- Takeaway: Corporate IT moved outside of the US is subject to search and seizure. To protect proprietary data, ensure appropriate policies for IT going abroad.

Consent

***United States v. Cruz-Zamora,* No. 17-40100-CM (D. Kan., Jun. 4, 2018)**

- CZ was stopped in Kansas by a trooper based on a suspended registration. CZ asked if the trooper spoke Spanish, but the trooper did not.
- Unaware the department had a live translator, the trooper used Google Translate to ask if he could search the car. Google translated it as "¿Puedo buscar el auto?" After some confusing interactions between the trooper and CZ, CZ said "yeah, yeah, go." The trooper found 14 pounds of meth and cocaine.
- At trial, CZ moved to suppress the drugs claiming he did not understand the question, so his alleged consent was not free and voluntary. Placed into Google translate in reverse order the above translates to "Can I find the car?"
- How should court rule?
  1. Did CZ's response constitute consent to search?
  2. Should "good faith" exception apply?

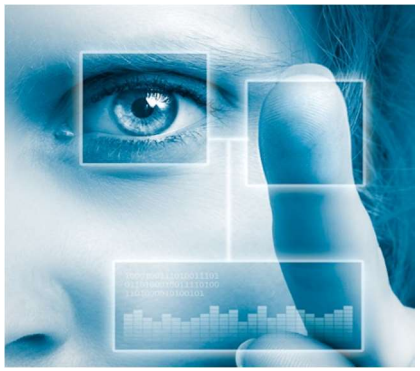
Holding

- No valid consent, as question was improperly translated so response could not be deemed to be clearly free and voluntary.
- Fruits of search should be suppressed.
- Government urged the court to apply the good faith exception based on prior case law that indicated a police officer's reliance on an erroneous entry in a government database justified application of the good faith exception.
- Court ruled that reliance on Google Translate was legally differentiable from reliance on a government database, so applying good faith was not appropriate.

Biometrics

In the Matter of Search of a Residence in Oakland, California, No. 4-1970053 (N.D. Calif., Jan. 10, 2019)

- US Gov't seeks a warrant relating to two individuals believed to be involved in extortion. Suspects alleged to have used Facebook Messenger to communicate with victim, threatening to distribute embarrassing video of him if he didn't provide money.
- Gov't also seeks the authority to compel any individual present at the time of the search to press a finger (including a thumb) or utilize other biometric features, such as facial or iris recognition, for the purposes of unlocking the digital devices found in order to permit a search of the contents as authorized by the search warrant.
- Issue: Should Magistrate issue warrant?



Holding

- Magistrate denies warrant application
- The Government may not compel or otherwise utilize fingers, thumbs, facial recognition, optical/iris, or any other biometric feature to unlock electronic devices [under 4th & 5th Amends.]
- 4th Amend.
  - Kerr: Warrants should only deal with where and what is to be searched or seized, not how
  - How should be an ex post issue, not ex ante
  - Fingerprinting generally only requires reasonable suspicion
- 5th Amend.
  - Kerr: 5th Amend. requires "express invocation"
  - A biometric doesn't constitute "testimonial" self-incrimination
  - Foregone conclusion hinges only on testimonial act
- Furthermore, the Government may only seize those digital devices that law enforcement reasonably believes are owned and/or possessed by the two suspects named in the affidavit.
  - Contra 4th Amend law. Only issue is whether the things to be searched or seized are at the place listed in the warrant.

Standing

In re Zappos.com, No. 16-16860 (9th Cir., 2018)

- Hackers breached Zappos.com and stole the names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information of more than 24 million Zappos customers.
- Plaintiffs in this appeal did *not* allege hackers used the information for fraudulent purposes, but merely the risk of identity theft.
- Art. III standing generally requires a plaintiff show
  - (1) it has suffered an "injury in fact" that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical;
  - (2) the injury is fairly traceable to the challenged action of the defendant; and
  - (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.
- Issue: Does a person who sues for a data breach based on fear of future identify theft or fraud have standing?

Holding

9th Cir rules:

- Yes, based on *Krottner v. Starbucks*, 9th Cir. case holding risk of identity theft is enough.
- Rejected Zappos' contention that *Krottner* had been overruled by *Clapper v. Amnesty Int'l (2013)*.
- *Clapper* involved attorneys, human rights orgs, and media orgs who frequently communicated via phone or email with persons abroad. They sued to invalidate a provision in FISA that permitted intelligence agencies to intercept communications with non-US persons.
- US Supreme Court held *Clapper* plaintiffs lacked standing because their claim was too speculative to constitute a "certainly impending" injury.
- S/C set out a multi-link chain of inferences in *Clapper*, but 9th Cir. says no such chain exists here. Also S/C's *Susan B. Anthony List* case in 2014 expanded test to "substantial risk of injury."
- Most Circuits seem aligned on this now. May depend on type of data stolen (See 8th Cir. *Supervalu* case)
- Takeaway: If your company handles PII this case opens you up to potentially far greater liability for the loss of that data.

Private Searches

United States v. Reddick, No. 17-41116 (5th Cir., 2018)

- Microsoft SkyDrive (now known as OneDrive) uses a program called PhotoDNA to scan the hash values of user-uploaded files to compare them against the hashes of known child porn. It then reports them to NCMEC
- In 2015 Microsoft sent a tip to NCMEC based on hashes related to files Reddick uploaded to SkyDrive. NCMEC forwarded to Corpus Christi PD where a detective opened the identified files w/o a warrant. He confirmed they each contained child porn, so used that evidence to obtain a search warrant for Reddick's home, resulting in more evidence. Reddick moves to suppress.
- Issue: Reddick appeals. Who wins and why?

Holding

T/C rules:

- Assumed w/o deciding that search was covered by the 4th Amend., exceeded the private search exception and fell under no other exception, but images found in home were admissible under the good faith exception.

5th Cir rules:

- Initial search by detective didn't violate 4th Amend. Question is whether defendant's expectation of privacy has not already been frustrated by the private search.
- Microsoft's hash scan already frustrated defendant's expectation of privacy. (Do Google's email scans frustrate REOP for all Gmail users?)
- S/C held in *Jacobsen* that DEA was authorized to test a suspicious white powder provided by FedEx employees who found it in package damaged in transit. DEA subsequently used evidence to obtain arrest warrant for recipients of the package.
- Takeaway: To what extent are cloud provider contracts undermining your expectation of privacy?

Insurance

Mondelez Int'l v. Zurich American Insurance, 2018 WL 4941760 (Ill. Cir. Ct.)

- Mondelez Int'l is one of the largest snack food companies in the world (Nabisco, Oreo, belVita, others) marketing its products in 165 countries worldwide
- Mondelez was hit broadly by NotPetya, suffering ~$100M in damages, including the bricking of 1700 servers and 24,000 laptops.
- Files claim with insurer, Zurich, under "all risks" provision, which specifically includes "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 ...." Zurich required voluminous supporting evidence, which Mondelez provided.
- During this time Zurich ran ads citing NotPetya as a reason companies should purchase their cyber insurance.
- Zurich later denied coverage based on an exclusion for losses from "hostile or warlike actions" by any government (de jure or de facto) or their agents.
- Issue: Who wins and why?

ZURICH

Holding

Pending case, so no ruling yet but …

- Ultimate decision could dramatically rattle the cyber insurance industry.
- The US, the UK, Denmark, Lithuania, Estonia, Canada, and Australia all attributed NotPetya to Russia, based on intelligence, but unclear basis could be used in court or would meet legal standard.
- Other attacks: WannaCry attributed to North Korea, 12-year cyberespionage campaign attributed to China, Aramco attributed to Iran
- Takeaway: Companies should carefully review cyber insurance contracts to determine to what extent the insurer may be able to deny coverage if any linkage to a government sponsor can be shown or alleged.

Quick Updates

- Can a person be convicted of attempted viewing of child porn, and viewing of child porn, based on 3 images—two in web browser cache and one in unallocated space?
  - Yes, per *United States v. King*, 78 M.J. __, No. 18-0288/AF (CAAF, 2018). Court finds it was a "circumstantially strong case" because (1) appellant password-protected his computer, (2) he had thousands of "offensive photos," (3) he searched using terms indicative of child porn ("dany camy" and "preteen girls"), and (4) he admitted he was "thrilled" by the images.
- Does the Government violate one's 4th Amendment right if it signs into your Facebook account as you, using information it obtained from a monitored telephone line, and obtains incriminating evidence against you there?
  - No, per *United States v. Langhorne*, ___ M.J. __, No. 39047 (A.F. Ct. Crim. App. Dec. 5, 2017), citing the third-party doctrine. "When Appellant voluntarily revealed his Facebook username and password to TSgt PF, he no longer had a reasonable expectation of privacy in his Facebook account." How far does this rationale extend? If I similarly revealed the numeric code for my car door lock to 3rd party, could the police search my car without a warrant? If I similarly revealed the numeric code for my home door lock to 3rd party, could the police search my home without a warrant?

Additional Cases and Issues to Watch

- Does an investigator exceed the scope of a search warrant if he searches for a decryption key when the warrant was limited to "pictures, video, emails, documents, and texts related to other sexual misconduct"?
  - Unclear. CAAF held that the issue was waived even though the Government had conceded that it was *not* waived. *United States v. Smith*, No. 18-0211/AR (CCAF, Feb. 22, 2019). CAAF held that the Government had misconstrued the court's own precedent on the issue.
  - In a complicated set of facts that continue develop during the appellate process, the investigator obtained a search authorization to search an iPhone, and also other devices in his home in case he had synched to them. iPhone was locked, so Army couldn't search it, but searching other devices Army found the file that permitted decryption of the phone. Army conceded on appeal the magistrate did not have probable cause to authorize search of the other devices, but held investigator operated in good faith. On further appeal, defense cites investigator's concession that he searched for the key, which was not within the scope of the search authorization.

Additional Cases and Issues to Watch

- How do “private prosecution” statutes that permit citizens who “witness” a crime to file a complaint apply to those who witness it via social media?
  - Limited to very few states, and even in those it generally requires a state official (prosecutor, magistrate) to approve it.
  - Seven Euclid, OH, residents filed an affidavit against Michael Amiott who beat a black man pursuant to a traffic stop based on a viral video of the event.
  - OH law requires the state to make the decision on prosecution. Apparently it chose not to prosecute, choosing instead to fire him.
  - After Euclid (OH) fired Amiott, he appealed to an arbitrator who cleared him, and the city rehired him.

Summary

- Trends
  - Fourth Amendment continues to evolve with technology
    - *Carpenter, Jones,* and *Riley* all suggest equilibrium adjustment
  - Circuit splits still in need of resolution
    - CFAA "without" or "exceeds" authorization interpretation
    - Encryption: 4th and 5th Amendment, forcing passphrases vs. forcing decryption, foregone conclusion, biometrics
    - Border searches: Do forensic searches require reasonable suspicion?
  - Cyber insurance and "war" exclusions raise new concerns
- Understand implications; cyberlaw is still immature/evolving