Recent Developments in Cyberlaw: 2018

Legal Caveat

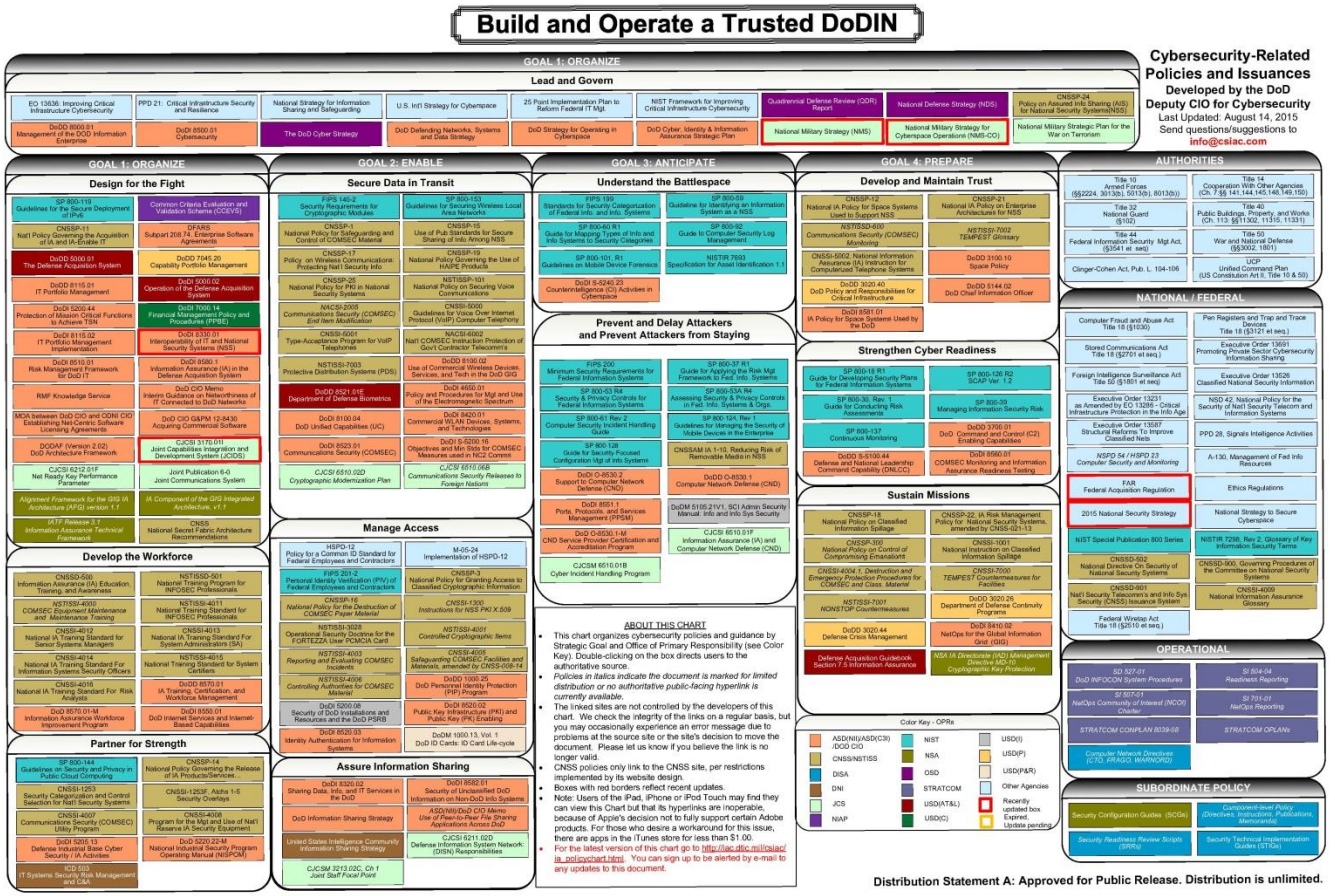
- Presentation is not legal advice*
- Designed to raise awareness of general legal principles applicable to information assurance and cyber security

*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. The Cyber Security and Information Systems Information Analysis Center (CSIAC) is a Department of Defense (DoD) Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC).

https://www.csiac.org/

DoD Cybersecurity Policy Chart

- Last updated 1 Feb 2018
- Covered in multiple publications including Wired.com
- This individual webpage has ranked 6th among all IA websites worldwide
- Feedback via website over-whelmingly positive
- Site provides alerts to followers



http://iac.dtic.mil/csiac/ia_policychart.html

Active Cyber Defense Certainty Act (H.R. 4036)

- Establishes an exception under the CFAA for the use of "attributional technology"
- Permits accessing without authorization the computer of the attacker to the victim's own network to gather information in order to:
  1. establish attribution of criminal activity to share with law enforcement and other United States Government agencies responsible for cybersecurity;
  2. disrupt continued unauthorized activity against the victim's own network; or
  3. monitor the behavior of an attacker to assist in developing future intrusion prevention or cyber defense techniques
- But does NOT include conduct that:
  1. intentionally destroys or renders inoperable information that does not belong to the victim that is stored on a computers of another;
  2. recklessly causes physical or financial injury to another person;
  3. creates a threat to the public health or safety; or
  4. intentionally exceeds the level of activity required to perform reconnaissance on an intermediary computer to allow for attribution of the origin of the persistent cyber intrusion;
  5. [plus three other exceptions related to intermediaries or certain government computers]

Reauthorization of FISA Section 702

Authorizes: Warrantless surveillance of non-U.S. persons reasonably believed to be outside the country (may include incidental collections on US persons)

From the House Permanent Select Committee on Intelligence:

- ALLEGATION: The government violates Americans' constitutional rights when the agencies conduct [back-door] types of queries.
- FACT: When the Government looks into its own database of lawful collection using U.S. person information, it is not a Fourth Amendment "search." The Government is not collecting any new information. Rather, the Government is simply reviewing the database of foreign communications it already has in its possession. This act is similar to police officers looking through an evidence locker to see if evidence from past crimes might help solve an open case. The police do not violate anyone's constitutional rights because they are simply reviewing evidence already in their lawful possession, not carrying out a new search. Source: https://intelligence.house.gov/uploadedfiles/uspq_faq_2017_clean.pdf

But what of the practice of overcollection of computer files?

Significant Recent Case Law

- Scope of 3rd Party Doctrine
  - Cell-site location information
- Extraterritorial searches
- Encryption
- Applying the 4th Amendment to electronic searches
  - Scope of warrants
- Artificial Intelligence
- Quick updates

Scope of 3rd Party Doctrine

***Carpenter v. United States,* 819 F.3d 880 (6th Cir.,2016), cert. granted, No. 16-402 (U.S. June 5, 2017)**

- 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.
- Does it matter that CSLI can be more accurate than GPS in urban locations? 911 requirement in law?
- Is CSLI really like dialed numbers?
- J. Sotomayor stated that *Jones* may require re-looking at 3rd party doctrine
- *Katz* 2-part test: Are carriers eyewitnesses?

Extraterritoriality

United States v. Microsoft, No. 14-2985 (2d Cir., 2016), *cert. granted, No. 17-2* (US, Oct. 16, 2017, argued Feb. 27, 2018)

- Under Stored Communications Act NY District Court judge ordered Microsoft to produce emails from an account hosted on a server in Ireland.
- Data stored at ~100 data centers around world based on country code of customer. Emails are not on servers in US, but could be brought back to US with special program.
- MS provided user account data but refused to provide e-mails. Said U.S. must use MLAT to obtain via Ireland. MS held in contempt, appeals to 2nd Cir.
- Issues:
  - Do sneak-and-peek searches violate the 4th Amendment?
  - Do the searches violate the 1st Amendment?
  - Does Microsoft have standing?

Microsoft

Holding

- Mooted by passage of CLOUD Act?
- Trial court: No 4th Amend violation. MS must turn over data. While statute talks of "warrant" it is really a hybrid warrant/subpoena.
- 2nd Cir.: Congress used the word "warrant" and this would be an extraterritorial application, which was not covered by the statute
- Ct treated the data as an object with a territorial location, unlike some other courts which have held it is "un-territorial" (especially as to cloud data)
- DoJ appealed for an *en banc* hearing. 2nd Cir has 11 judges but 3 recused themselves, leaving 8. Vote was 4-4 to hear the case *en banc*, leaving the prior decision undisturbed.
- SCOTUS granted cert.
- No Circuit split, but compare with Google and Yahoo cases in D/C.

The CLOUD Act

- Clarifying Lawful Overseas Use of Data (CLOUD) Act passed as part of the "Consolidated Appropriations Act, 2018"
- Attempts to resolve two issues:
  1. How U.S. law enforcement officers can seek access to data held extraterritorially
  2. How foreign law enforcement officers can seek to access to data held by U.S. firms

1. New § 2713 of SCA: A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to *preserve, backup, or disclose* the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's *possession, custody, or control*, regardless of whether such communication, record, or other information is located within or outside of the U.S.
   - Lower protections than 4th Amendment, but may avoid data localization in countries with even lower standards
   - No notice to target, but allows provider to challenge it
   - Procedures to address conflicts of laws issues
     - Qualifying countries
       - Would cause a violation of law of the qualifying foreign government
       - "Totality of circumstances" requires modification or quashal
       - Subscriber is non-U.S. person who resides abroad
     - All other cases: apply common law comity standards
   - Microsoft, Google, Facebook, Apple and Verizon appear to support it. Civil liberties groups do not.

The CLOUD Act (cont.)

2. Permits U.S. and foreign law enforcement to obtain access to electronic records without and Mutual Legal Assistance Treaty (MLAT) request pursuant to a CLOUD Act Agreement
   - U.S. Atty General and Sec'y of State must concur foreign country's law provide "robust substantive and procedural protections…"
   - Orders issued via CLOUD Act Agreement must:
     - Relate to a "serious crime"
     - Identify specific person, account, device, identifier
     - Be lawful under local law
     - Be justified by "articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation"; and
     - Be subject to "review or oversight by a court, judge, magistrate, or other independent authority."
   - Adds a provision to Wiretap Act, SCA, and Pen/Trap to permit above.

Divulging Smartphone Passcode

Florida v. Voigt, Case No. F16015256

- Fitness model and Instagram star Hencha Voigt and boyfriend Wesley Victor demand $18K from "Snapchat Royalty" YesJulz or they will reveal nude videos allegedly obtained from hacking YesJulz's phone.
- YesJulz provides text messages from Victor to police who arrest suspects the next day and seize 4 phones—all locked. Nude videos released shortly thereafter.
- iMessages do not appear in toll records but only as generic data usage.
- One phone had fingerprint enabled, but phone had been turned off so now required code. Unable to bypass codes, FL seeks order for suspects to reveal their passcodes.
- Issue: Does 5th Amendment protect Voigt and Victor from producing passcodes?

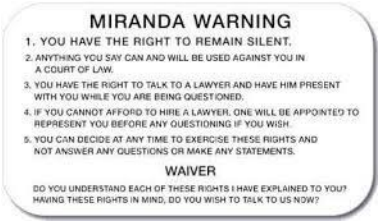
Holding

- Voigt must reveal passcode to her phone and Victor must reveal passcodes to his 3 phones, following precedent of Florida Court of Appeals in *Florida v. Stahl*, but *contra In re Grand Jury Subpoena Duces Tecum* (11th Cir. 2012)
- Victor subsequently claims he can't remember passcode. Judge refuses to jail him in contempt claiming passage of 10 months may have caused him to forget the code. (*Contra Rawls* and other cases.)
- FBI agreed to pay for Cellbrite to bypass the passcode and successfully hacked one of the phones.
- Courts are still all over the board on this issue. Most agree forcing a suspect to relate the passcode is a 5th Amendment violation. Some have held forcing production of a decrypted phone is not. Most have also held that forcing the production of fingerprints does not raise 5th Amendment issues. No cases to date on facial ID, but expected to be the same as fingerprints.

Divulging Smartphone Passcode

United States v. Mitchell, 76 M.J. 413 (CAAF, 2017)

- Mitchell was being investigated for harassing his wife. She told investigators that he texted her after he was issued a no-contact order.
- Mitchell was escorted to police station where investigators informed him of his rights. M invoked his right to counsel. Released and returned to his unit.
- Investigator (T) obtained verbal search authorization for phone. M brought to Company Commander's office and informed of same. M questioned validity of verbal SA, but T confirmed validity. Asked if M had any phones with him. He provided one, but it was locked. T asked M to unlock it but he refused. T encouraged M to unlock it, threatening it could unlocked by forensics anyway. M unlocked it.
- Issue: Did T violate M's 5th Amendment by asking M to unlock his device after M invoked his right to counsel?
  - Does the fact that M's phone has 2 registered fingerprints have any bearing on this case?



Holding

- CAAF: Gov't violated protective rule of *Edwards* by questioning M after his invocation of his right to counsel.
- M was in custody when he originally invoked his right to counsel. He was returned to effective custody two hours later when directed to report to his Commander's office with two military investigators present.
- In the Commander's office M was subjected to interrogation again. Interrogation is "any words or actions on the part of the police … that the police should know are reasonably likely to elicit an incriminating response from the suspect."
- Asking for passcode was not equivalent to asking for consent to search.
- Fingerprints don't prove inevitable discovery because unclear whether that function was turned on or not.
- CAAF did not address 5th Amend, testimonial or compelled nature of response.
- Dissent takes majority to task for the prior bullet, claiming unless what is elicited is testimonial and incriminating, *Edwards* doesn't apply; says "question" was "knock and announce."

Scope of Search Warrants

***United States v. Griffith,* (DC Cir., Aug 18, 2017)**

- Homicide involving rival gangs occurs. Surveillance cameras caught a car at the scene. Two months later matched car to one owned by Griffith's mother. Eight months later G's mother alleges G is the primary user. During most of this time G was in prison on unrelated charges.
- When G is released from prison, moves in with girlfriend Lewis (L). Police get warrant to search L's apartment for any cell phones or electronic devices.
- When police knock on door, G throws gun out window. Police seize gun and several cell phones.
- G seeks to suppress gun, claiming search warrant was invalid as not based on probable cause. T/C denies motion, convicts.
- Issue: Can G claim 4th Amendment protection in L's apartment? If so, was there probable cause?
    - If so, should the gun be suppressed?

Holding

- DC Cir: Yes, G lived in the apartment with L so had a reasonable expectation of privacy and 4th Amendment right. And no probable cause to suspect evidence of crime on phones or electronic devices, so fruits of invalid warrant should be suppressed.
- Affidavit provided no info that G owned a cell phone, possessed a cell phone, or used a cell phone. Fact that he was in prison for 10 months suggested he probably didn't own a cell phone. His alleged co-conspirator did not own a cell phone and police knew this.
- Affidavit provided no info that cell phone would be in L's apartment.
- Warrant permitted seizure of *any* phone, even L's (Does this matter?)
- 2-stage "computer" search:
    - 1. Physical (permitting over seizure)
    - 2. Electronic (narrowed to scope of investigation)

Scope of Search Warrants

***United States v. Blake,* (11th Cir., Aug 21, 2017)**

- Blake and Moore ran a child prostitution ring. Based on leads, FBI investigated and sought 3 warrants
  1. B & M's townhouse: Found locked iPad, obtained Writ to force Apple to assist. Apple did and FBI got data.
  2. Microsoft: For emails related to sex trafficking
  3. Facebook: Every IM, post, photo (including those M was tagged in), IP address logged in from, search conducted, purchase made on Facebook Marketplace, contact list from creation of account, with 2nd search narrowed to specified crime.
- Both convicted. B sentenced to 324 months, M to 240 months.
- All three warrants challenged at trial and on appeal
- Issue: Is each warrant legal and enforceable?

Holding

- 11th Cir: Warrants 1 and 2, yes. Warrant 3, no.
- Warrant 1: Permissible under All Writs Act: necessary and appropriate, not inconsistent with Congress's intent, Apple not too far removed, burden not unreasonable.
- Warrant 2: Probable cause and sufficient particularity
- Warrant 3: 2-stage computer search applicable to home computers not applicable to social media. 2-stage "computer" search:
  - 1. Physical (permitting over seizure)
  - 2. Electronic (narrowed to scope of investigation)

  But court allows data in under "Good Faith" exception, so additional explanation is dicta.
- How does the 2-stage approach extend the Plain View doctrine?

Artificial Intelligence

***Loomis v. Wisconsin,* 371 Wis. 2d 235 (2016)**

- Loomis was allegedly part of a drive-by shooting, but pled guilty to eluding the police, operating a vehicle w/o owner's consent, both as repeat violations. Was sentenced to 6 years.
- Presentencing report included Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) assessment tool, an AI tool used to predict recidivism risk.
- The algorithm used by the tool is proprietary, kept secret, and takes into account gender and race. It scored him a high risk on violence, recidivism, and pre-trial flight via bar charts.
- State argued COMPAS factors and judge referenced COMPAS factors in sentencing.
- Issue: Does use of COMPAS as an aid in sentencing violate due process?

Holding

- S/C of Wisconsin: No violation of due process
- COMPAS originally developed to help corrections departments allocate resources by grouping prisoners.
- Caution in presentence investigative report: "It is very important to remember that risk scores are not intended to determine the severity of the sentence or whether an offender is incarcerated."
- NY and a couple of other states did statistical validation studies, but WI's hadn't been completed.
- Court held his access to final scores was enough—due process didn't require COMPAS to reveal how it was computed.
- But circuit court submitted in post-conviction hearing that it would have sentenced him the same with or without the COMPAS report.

Quick Updates

- Does possession of the same child porn images on four different devices constitute four crimes, with sentencing for each? (3 external hard drives and 1 Gmail account)
  - Yes, per *United States v. Forrester*, 76 M.J. 389, No. 17-0049/MC (CAAF, 2017). But how does that work in the cloud, where each image may be stored on multiple computers over time or may be accessed from multiple computers? Backups?
- Does the 4th Amendment require a temporal limitation on searches, limiting to the time of the alleged misconduct?
  - No, per *United States v. Richards*, No. 16-0727/AF (CAAF, 2017). But DCFL's pulling of *all* files, pictures, chat logs, Word documents, Internet history, didn't limit it to communications between 2010-11 and so *seems* more like a prohibited "general search," but court found otherwise.
- If a person consents to a search, but 25 minutes into it, revokes consent, must the police return the electronic media seized? Can they claim inevitable discovery?
  - Yes, must return, and no inevitable discovery per *United States v. Hoffman*, No. 15-0361/MC (CAAF, 2016), overturning the NMCCA. No "meaningful interference with possessory interest in that property" merely by moving it to the center of the room before accused revoked consent. Judge made no record of evidence of probable cause at the time, and evidence in the record undermines such. Accused was suspected of soliciting a minor and there was no probable cause to believe accused possessed child porn on his barracks computer.

Summary

- Trends
  - The increasingly international nature of data storage has created both domestic and foreign search issues
  - The courts are grappling with how to apply the law to the cloud, handhelds and IoT
    - The scope of the 3rd party doctrine will be decided by *Carpenter*
    - Extraterritoriality becomes a key issue in the cloud
    - IoT increasingly becoming a “witness”
  - Encryption could pose a hurdle for the IC and LE, but data backed up to the cloud, or shared with 3rd parties may provide alternate approaches, as could sneak & peak warrants prior to the warrant for the device
- Understand implications; cyberlaw is still immature/evolving
- Use briefing to help identify potential issues
  - Seek legal counsel when uncertain