Emerging Developments in Cyberlaw: 2020

Rick Aldrich, JD, LL.M, CISSP, CIPT, GLEG
Aldrich_Richard@bah.com, 703-545-2329
American Bar Association, Information Security Committee, 23 Feb 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.

Pending Bills

BILL	SHORT TITLE	SPONSORS	COMMITTEE	LAST MAJOR ACTION
H.R. 359	Enhancing Grid Security through Public-Private Partnerships Act	Rep. Jerry McNerney	House - Energy and Commerce	10/28/2019 Placed on the Union Calendar, Calendar No. 202.
H.R. 360	Cyber Sense Act of 2019	Rep. Robert E. Latta	House - Energy and Commerce	10/28/2019 Placed on the Union Calendar, Calendar No. 204
H.R. 370	Pipeline and LNG Facility Cybersecurity Preparedness Act	Rep. Fred Upton	House - Energy and Commerce	11/20/2019 Subcommittee on Railroads, Pipelines, and Hazardous Materials Discharged.
H.R. 1158	DHS Cyber Incident Response Teams Act of 2019	Rep. Michael McCaul	House - Homeland Security	09/25/2019 Message on Senate action sent to the House.
H.R. 1493	Cyber Deterrence and Response Act of 2019	Rep. Ted Yoho	House - Foreign Affairs, Financial Services, Oversight and Reform, Judiciary	04/08/2019 Referred to the Subcommittee on Immigration and Citizenship.
H.R. 1649	Small Business Development Center Cyber Training Act of 2019	Rep. Steve Chabot	House - Small Business	07/16/2019 Received in the Senate. Read twice. Placed on Senate Legislative Calendar under General Orders.
H.R. 1975	Cybersecurity Advisory Committee Authorization Act of 2019	Rep. John Katko	House - Homeland Security; Energy and Commerce; Oversight and Reform	09/25/2019 Ordered to be Reported (Amended) by Unanimous Consent.
H.R. 2331	SBA Cyber Awareness Act	Rep Jason Crow	House – Small Business	07/16/2019 Received in the Senate. Read twice. Placed on Senate Legislative Calendar under General Orders.
H.R. 2500	National Defense Authorization Act for Fiscal Year 2020	Rep. Adam Smith	House - Armed Services	09/10/2019 Received in the Senate.
H.R. 2660	Election Security Act of 2019	Rep. Bennie Thompson	House - House Administration, Homeland Security, Intelligence (Permanent Select), Science, Space, and Technology, Foreign Affairs, Judiciary	06/28/2019 Referred to the Subcommittee on the Constitution, Civil Rights, and Civil Liberties.
H.R. 2721	Cyber Ready Workforce Act	Rep. Susie Lee	House - Education and Labor	05/14/2019 Referred to the House Committee on Education and Labor
H.R. 2722	Securing America's Federal Elections (SAFE) Act	Rep. Zoe Lofgren	House - House Administration, Science, Space, and Technology	06/28/2019 Received in the Senate and Read twice and referred to the Committee on Rules and Administration.
H.R. 3238	Defending the Integrity of Voting Systems Act	Rep. John Ratcliffe	House – Judiciary	06/28/2019 Referred to the Subcommittee on Crime, Terrorism, and Homeland Security.
H.R. 3270	Active Cyber Defense Certainty Act	Rep. Tom Graves	House – Judiciary	06/28/2019 Referred to the Subcommittee on Crime, Terrorism, and Homeland Security.
H.R. 3318	Emerging Transportation Security Threats Act of 2019	Rep. John Joyce	House - Homeland Security	08/30/2019 Placed on the Union Calendar, Calendar No. 153.
H.R. 3320	Securing the Homeland Security Supply Chain Act of 2019	Rep. Peter T. King	House - Homeland Security	08/27/2019 Placed on the Union Calendar, Calendar No. 146.
H.R. 3484	DHS Rotational Cybersecurity Program Act of 2019	Rep. Cedric Richmond	House - Homeland Security	07/18/2019 Referred to the Subcommittee on Transportation and Maritime Security.

Summary of pending bills courtesy of Booz Allen Hamilton's Cybersecurity Policy Review

Pending Bills

BILL	SHORT TITLE	SPONSORS	COMMITTEE	LAST MAJOR ACTION
H.R. 3611	Securing American Research From Cyber Theft Act	Rep. Brian Babin	House - Science, Space, and Technology, Armed Services	07/02/2019 Referred to the Committee on Science, Space, and Technology
H.R. 3710	Cybersecurity Vulnerability Remediation Act	Rep. Sheila Jackson Lee	House - Homeland Security	10/15/2019 Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
H.R. 3811	IoT Standards Leadership Act of 2019	Rep. Doris Matsui	House - Foreign Affairs	07/17/2019 Referred to the House Committee on Foreign Affairs.
H.R. 3907	Department of Homeland Security Insider Threat and Mitigation Act of 2019	Rep. Peter T. King	House - Homeland Security	08/21/2019 Referred to the Subcommittee on Intelligence and Counterterrorism.
H.R. 4170	ENCRYPT Act of 2019	Rep. Ted Lieu	House - Judiciary, Energy and Commerce	09/25/2019 Referred to the Subcommittee on Crime, Terrorism, and Homeland Security.
H.R. 4189	Homeland and Cyber Threat Act	Rep. Jack Bergman	House – Judiciary	08/16/2019 Referred to the House Committee on the Judiciary.
H.R. 4217	State and Local Cybersecurity Improvement Act	Rep. John Katko	House - Homeland Security	09/06/2019 Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation.
H.R. 4237	Advancing Cybersecurity Diagnostics and Mitigation Act	Rep. John Ratcliffe	House - Oversight and Reform; Homeland Security	09/10/2019 Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation.
H.R. 4458	Cybersecurity and Financial System Resilience Act of 2019	Rep. Patrick T. McHenry	House - Financial Services	10/31/2019 Ordered to be Reported (Amended) by Voice Vote.
H.R. 4772	CFTC Cybersecurity and Data Protection Enhancement Act	Rep. Rodney Davis	House – Agriculture	11/13/2019 Referred to the Subcommittee on Commodity Exchanges, Energy, and Credit.
H.R. 4774	Internet of Things Cyber Security Training for Federal Employees Act	Rep. Ro Khanna	House - Oversight and Reform	10/21/2019 Referred to the House Committee on Oversight and Reform.
H.R. 4792	Cyber Shield Act of 2019	Rep. Ted Lieu	House - Energy and Commerce	10/22/2019 Referred to the House Committee on Energy and Commerce.
H.R. 4195	Small Business Cybersecurity Enhancement Act	Rep. Bradley Schneider	House - Small Business	10/30/2019 Referred to the House Committee on Small Business.
H.R.4990	Election Technology Research Act of 2019	Rep. Mikie Sherril	House - Science, Space, and Technology; House Administration	11/14/2019 Ordered to be Reported (Amended) by Voice Vote.
H.R. 5394	Strengthening State and Local Cybersecurity Defenses Act	Rep. Van Taylor	House - Homeland Security; Oversight and Reform	12/11/2019 Referred to the Committee on Homeland Security, and in addition to the Committee on Oversight and Reform
S. 174	Securing Energy Infrastructure Act	Sen. Angus S. King Jr.	Senate - Energy and Natural Resources	08/16/2019 Placed on Senate Legislative Calendar under General Orders.
S. 406	Federal Rotational Cyber Workforce Program Act of 2019	Sen. Gary Peters	Senate - Homeland Security and Governmental Affairs	07/25/2019 Committee Consideration and Mark-up Session Held.
S. 482	Defending American Security from Kremlin Aggression Act of 2019	Sen. Lindsey Graham	Senate - Foreign Relations	12/18/2019 Placed on Senate Legislative Calendar under General Orders. Calendar No. 389.

Summary of pending bills courtesy of Booz Allen Hamilton's Cybersecurity Policy Review

Pending Bills

BILL	SHORT TITLE	SPONSORS	COMMITTEE	LAST MAJOR ACTION
S. 734	Internet of Things Cybersecurity Improvement Act of 2019	Sen. Mark Warner	Senate - Homeland Security and Governmental Affairs	09/23/2019 Placed on Senate Legislative Calendar under General Orders. Calendar No. 215.
S. 1321	Defending the Integrity of Voting Systems Act	Sen. Richard Blumenthal	Senate – Judiciary	07/19/2019 Referred to the House Committee on the Judiciary.
S. 1466	Cyber Ready Workforce Act	Sen. Jacky Rosen	Senate - Health, Education, Labor, and Pensions	05/14/2019 Read twice and referred to the Committee on Health, Education, Labor, and Pensions.
S. 1790	National Defense Authorization Act for Fiscal Year 2020	Sen. James Inhofe	Senate - Armed Services	12/20/2019 Became Public Law No: 116-92.
S. 1798	Department of Defense Principal Cyber Advisors Act of 2019	Sen. Mike Rounds	Senate - Armed Services	06/12/2019 Read twice and referred to the Committee on Armed Services.
S. 1799	Defense Cybersecurity Personnel Authorizations and Inventory Oversight Act of 2019	Sen. Mike Rounds	Senate - Armed Services	06/12/2019 Read twice and referred to the Committee on Armed Services.
S. 1846	State and Local Government Cybersecurity Act of 2019	Sen. Gary Peters	Senate - Homeland Security and Governmental Affairs	11/26/2019 Received in the House. 11/21/2019 Passed Senate with an amendment by Unanimous Consent.
S. 1951	Designing Accounting Safeguards To Help Broaden Oversight and Regulations on Data	Sen. Mark Warner	Senate - Banking, Housing, and Urban Affairs	10/24/2019 Committee on Banking, Housing, and Urban Affairs. Hearings held.
S. 2065	Deepfake Report Act of 2019	Sen. Rob Portman	Senate - Homeland Security and Governmental Affairs | House - Energy and Commerce	10/28/2019 Referred to the House Committee on Energy and Commerce.
S. 2095	Enhancing Grid Security through Public-Private Partnerships Act	Sen. Cory Gardner	Senate - Energy and Natural Resources	10/24/2019 Placed on Senate Legislative Calendar under General Orders. Calendar No. 267.
S. 2154	JROTC Cyber Training Act	Sen. Jacky Rosen	Senate - Armed Services	07/17/2019 Read twice and referred to the Committee on Armed Services.
S 2181	Cyber AIR Act	Sen. Edward Markey	Senate - Commerce, Science, and Transportation	07/18/2019 Read twice and referred to the Committee on Commerce, Science, and Transportation.
S. 2182	SPY Car Act of 2019	Sen. Edward Markey	Senate - Commerce, Science, and Transportation	07/18/2019 Read twice and referred to the Committee on Commerce, Science, and Transportation.
S. 2316	Manufacturing, Investment, and Controls Review for Computer Hardware, Intellectual Property, and Supply Act of 2019	Sen. Mike Crapo	Senate - Intelligence (Select)	07/30/2019 Read twice and referred to the Select Committee on Intelligence.
S. 2333	Energy Cybersecurity Act of 2019	Sen. Maria Cantwell	Senate - Energy and Natural Resources	10/23/2019 Placed on Senate Legislative Calendar under General Orders. Calendar No. 264.
S. 2664	Cyber Shield Act of 2019	Sen. Edward Markey	Senate - Commerce, Science, and Transportation	10/22/2019 Read twice and referred to the Committee on Commerce, Science, and Transportation.
S. 2775	HACKED Act of 2019	Sen. Roger Wicker	Senate - Commerce, Science, and Transportation	11/13/2019 Committee on Commerce, Science, and Transportation. Ordered to be reported with an amendment favorably.
S. 3033	K-12 Cybersecurity Act of 2019	Sen. Gary Peters	Senate - Homeland Security and Governmental Affairs	12/12/2019 Read twice and referred to the Committee on Homeland Security and Governmental Affairs.

Summary of pending bills courtesy of Booz Allen Hamilton's Cybersecurity Policy Review

Significant Recent Case Law

- Cases Interpreting *Carpenter*
- GDPR-related Cases
- Border Searches
- Encryption
- Pen Testing
- CFAA
- Insurance
- Quick Updates
- Cases to Watch

Video Surveillance

People v. Tafoya, No. 17CA1243 (Colo. Ct. App., Nov. 27, 2019)

- Informant tells police T's house is a "stash house" for illegal drugs. Police install video camera on utility pole across the street from T's house.
- Video camera could pan and zoom and see over T's 6' high privacy fence.
- Police observed T do something with front tire (obscured by fence) then carry white plastic bags inside. Obtained search warrant to search house and found white plastic bags contained 20 lbs. of illegal drugs.
- T moves to suppress based on warrantless surveillance.
  - Issue: Does warrantless video surveillance from a public utility pole for ~3 months violate 4th Amendment?

Holding

- Court: Yes. *Carpenter's* "narrow decision" did not call into question conventional surveillance techniques … such as security cameras." Nevertheless, the court held that a pole camera is not a security camera and its pervasive tracking for over 3 months violated the 4th Amendment.
- Contra: United States v. Kelly, 385 F. Supp. 3d 721 (2019), held a stationary video surveillance of the exterior of an apartment building and the hallway outside of an apartment for 49 days did not require a warrant under Carpenter. "Unlike a cell phone, the video surveillance did not track the totality of the defendant's movements."
- Takeaway: Courts still grappling, but the more it seems like digital devices engaged in "pervasive tracking" the more likely it will require a warrant.

GPS Data

United States v. Diggs, 385 F. Supp. 3d 648 (2019)

- Diggs is charged with robbery of a jewelry store. While investigating the robbery, police believed the abandoned getaway vehicle was registered to Diggs' wife based on plates.
- Diggs' wife bought the car from a dealer with a contract provision that provided, "If your vehicle has an electronic tracking device, you agree that we may use this device to find the vehicle."
- Police put out alert seeking information on vehicle. Dealer contacted police and provided them with Diggs's wife's account and login credentials for the GPS site. Site included historical information which linked car to the robbery and other co-defendants. Diggs moves to suppress.
- Issue: Was the police access to long-term historical GPS data without a warrant, but per terms of wife's contract, a violation of 4th Amendment?

Holding

- Dist. Ct.: Yes
- Extending *Carpenter* and *Jones* while limiting the application of the 3rd party doctrine, court finds 4th Amend. violation
- US argues, unlike Jones, gov't didn't invade private property of Diggs. Court holds that 1-month of detailed GPS data violates Jones/Carpenter rationale.
- Gov't argues 3rd party doctrine. Court holds Carpenter narrowed 3rd party doctrine where exhaustive data results in a pervasive intrusion on privacy.
- Gov't argues abandonment. Ct rejects.
- Takeaway: If your company collects sensitive data, this case may provide a basis to resist warrantless requests from the government. Review customer privacy agreements for impact on one's reasonable expectation of privacy.
- Can suspect remove the GPS device? See Heuring v. Indiana, No. 10A-CR-140 (Ind. Ct. App., July 18, 2019) suggesting it may be theft and justify warrant for house. But IN S/C seems skeptical.

Pings

Commonwealth v. Almonor, 482 Mass. 35 (2019)

- Defendant had an altercation with an individual in a car, ultimately using a sawed-off shotgun to kill him. Police investigation led them to people who witnessed the shooting and who knew the defendant. One person provided police with defendant's cell number.
- Police sent a "mandatory information for exigent circumstance requests" form to the defendant's service provider based on the fact that defendant was a murder suspect and still had a shotgun.
- Service provider pinged defendant's phone and provided GPS location information to the police. Police went to address and the owner granted consent to entry. Police located defendant in upstairs bedroom and saw shotgun and vest in plain view. Sought warrant and seized both.
- D moves to suppress under 4th Amend and MA analog
- Issue: Does pinging a phone under the above circumstances constitute a search?

Holding

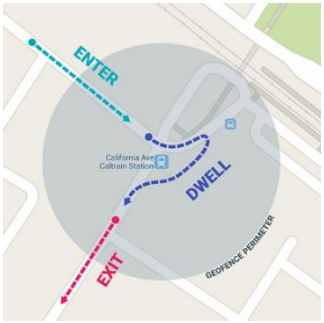
T/C holds Yes.

- Answers a question left open by Carpenter: "We do not express a view on matters not before us [such as] real-time [location information]."
- Relies in part on rationale of *Carpenter* to conclude that ruling otherwise would allow the "power of technology to shrink the realm of guaranteed privacy."
- Pinging a phone at police request requires the phone to compute and transmit its GPS location. Such info would otherwise not be collected or retained by the service provider.
- Because cell phones are so ubiquitous, it essentially becomes a tracking device that can be activated by police at any time.
- Ct distinguishes this case from the 6-hour "telephone call" CSLI rule
- Takeaway: The questions left open by *Carpenter* are increasingly being answered in ways that expand the scope of *Carpenter*.

Geofence Warrants

United States v. Chatrie, No. 3:19-cr-00130-MHL (2020)

- 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"?



Holding

Case still pending. Hearing on motion is 20 Feb.

- Answers a question left open by Carpenter regarding "tower dumps"
- Chatrie: 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
- Ct distinguishes this case from the 6-hour "telephone call" CSLI rule
- Takeaway: The questions left open by *Carpenter* are increasingly being answered in ways that expand the scope of *Carpenter*.

GDPR

Google v. CNIL, C-507/17, ECLI:EU: C:2019:772

- CNIL ruled that Google had to remove links to a person's personal data from all of Google's domains worldwide (aka de-referencing)
- Google instead implemented an approach that delisted results only related to EU domains (e.g., Google.de, Google.fr, etc.). Google also proposed "geo-blocking," a technical approach that involves blocking search results from users within the EU even if they use a non-EU search domain.
- CNIL found the approach was noncompliant and fined Google €100,000. Google appealed to the Court of Justice of the European Union (CJEU) seeking a ruling on whether Google was required to de-reference personal data on all of its domains worldwide.
- Issue: Can Google be required to de-reference on all versions of its search engine worldwide?

Holding

- CJEU: No
- Google's agreement to delist results within EU domains was reasonable. Right to be forgotten is not an absolute right. Balancing various rights is likely to involve conflicts of law issues.
- Ct held, "EU law does not currently require that the de-referencing granted concern all versions of the search engine in question, it also does not prohibit such a practice."
- Takeaway: Suggests the GDPR will be interpreted in a way limits impact outside of EU and recognizes conflict of laws issues.

GDPR

Glawischnig-Piesczek v. Facebook Ireland Limited, C-18/18, ECLI:EU:C:2019:821

- Plaintiff, an Austrian politician, requested Facebook remove disparaging posts associated with her image (i.e. "lousy traitor," a "corrupt oaf," and a member of a "fascist party.")
- Facebook refused the request, so G-P sued in the VCC and won a judgment requiring Facebook remove offending posts, but also all "identical" and "equivalent" posts. Facebook removed offending posts for users in Austria.
- Both parties appealed to the Austrian S/C which asked the CJEU to opine.
- Issue: Must Facebook take down posts worldwide? Must Facebook also take down "equivalent" posts

Holding

- CJEU: Yes, and yes.
- Facebook's agreement to remove the original post for users in Austria deemed insufficient.
- Facebook was ordered "to remove information covered by the injunction or to block access to that information worldwide."
- Court holds Facebook can be required to remove initial posts, any re-posts and any "equivalent" posts worldwide. Query: What is equivalent to a "corrupt oaf"? In all languages, in all countries?
- Takeaway: Suggests the GDPR can be used as a sword within the EU to force global companies with assets in the EU to comply with orders that may not otherwise be enforceable within the U.S. or other countries.

Border Searches

Alasaad v. Nielson, 2019 U.S. Dist. Lexis 195556 (D. Mass., Nov. 12, 2019)

- Plaintiffs are 10 US citizens and 1 lawful permanent resident.
- CBP and ICE conducted searches/seizures of Ps' devices at borders and int'l airports of locked and unlocked smartphones, laptops, other e-media.
- One P objected to search of photos by male officers of females with headscarves removed based on religious beliefs. CBP retained e-evidence and sometimes commented on missing photos. Ps objected also on basis of atty-client privilege and journalist's rights.
- Issue: Can manual or forensic searches of a cell phones at the border with no reasonable suspicion be limited under the 1st or 4th Amend? Can plaintiffs require government expunge previously retained electronic evidence?

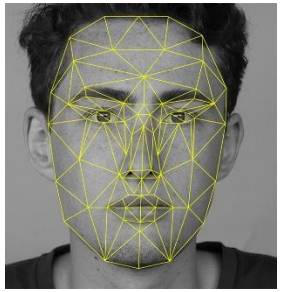
Holding

- Dist. Ct.: Yes, both manual and forensic searches of smartphones and e-devices generally require reasonable suspicion under 4th Amendment.
- Border search exception applies to "routine" NOT "non-routine" searches. Distinction hinges on degree of invasiveness, based on particularized facts.
- Circuits are split: 4th and 9th require reasonable suspicion for forensic searches. 11th holds contra
- Extends rationale of Riley (computers are different), holding both manual and forensic search of e-devices are non-routine, requiring reasonable suspicion in both.
- Ct rules no different standard for 1st Amend. Ct denies request for expungement.
- Takeaway: Corporate IT moved across the US border may be subject to search and seizure. To protect proprietary data, ensure appropriate policies for IT going abroad.

Biometrics

In re Facebook Biometric Information Privacy Litigation (15-cv-03747-JD) (N.D. Cal.)

- Plaintiffs are Facebook users who challenged the "Tag Suggestions" program (based on scans of uploaded photos)
- Plaintiffs alleged Facebook collected and stored their biometric data w/o notice or consent in violation of Illinois' BIPA (Biometric Information Privacy Act)
- No private entity may collect, capture, purchase, receive through trade, a customer's biometric identifier unless it first:
  1. informs the subject in writing that a biometric identifier or biometric information is being collected or stored;
  2. informs the subject in writing of the specific purpose and length of term for which a biometric is being collected, stored, used; and
  3. receives a written release executed by the subject of the biometric identifier
- Issue: Do plaintiffs have Art. III standing if no injury in fact? Can Illinois law be applied extraterritorially in California? Does the voluntary uploading of photos to Facebook constitute consent?



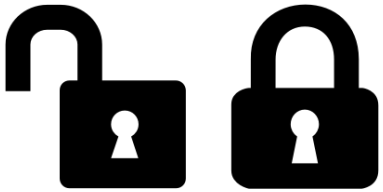
Holding

- 9th Cir. held in related case of *Patel v. Facebook* that plaintiffs overcame Art. III standing issues by alleging a substantive harm to concrete privacy interests.
- IL S/C held similarly in *Rosenbach v. Six Flags.*
- 9th Cir. also held that rejected the extraterritoriality argument based on its inference that the Illinois legislature contemplated such application.
- *Rosenbach* also held that voluntariness of disclosure was irrelevant unless done after written notification, as req'd in the law.
- After class certification was upheld on appeal, and U.S. S/C denied cert., Facebook settled the suit for $550M. (By law, "reckless" violation can result in $5,000/violation and there are 5-6M Facebook users in IL.)
- Takeaway: Companies that collect or profit from the use of facial scans, fingerprints, voice prints, retina scans, etc. should be very cautious about the reach of this law.

Encryption

India v. Facebook

- Consolidation of cases across India in the Supreme Court of India. India is seeking to force Facebook to decrypt Messenger and Facebook messages.
- Facts are unclear, but some are claiming that India has a counterpart to Section 230 of the U.S. Communications Decency Act (which provides immunity from liability for providers and users of an interactive computer service which publishes information provided by others), but that India is claiming such immunity applies only if the company can monitor its communications. If it encrypts the communications in a way that it can't monitor them itself, it loses the immunity.
- US, UK and Australia also urging Facebook to create backdoor access to encrypted messages. So far Facebook has resisted. How should court rule?
- Australia has already passed a law requiring companies to create a means to access encrypted communications but has an exception when such functionality would create a "systemic weakness."



Holding

- India case to be heard starting the last week of January 2020.
- China, Russia, and Turkey already ban services offering end-to-end encryption.
- Now US DoJ is seeking to compel Apple to unlock the phone of the Saudi student pilot who went on a shooting rampage at Naval Air Station Pensacola.
- Appears to be a replay of the San Bernardino incident from 2018. In that case the FBI backed down after finding a commercial company that could hack the phone.

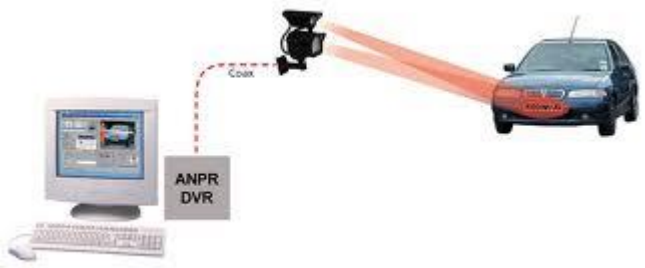
ALPR

Canosa v. Coral Gables, No. 2018-33927-CA-01 (Oct. 16, 2019)

- 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 30 million license plates for 3 years and made available to 80 LE agencies.
- 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
- Coral Gables and other state defendants' move to dismiss, citing among other reasons that the data has not been used against Canosa.
- Issue: Should the court dismiss the case on the government's motion?

Holding

- No.
- On motion to dismiss, court assumes facts alleged by plaintiff are true.
- "A motion to dismiss a complaint for declaratory judgment is not a motion on the merits. Rather it is a motion only to determine whether the plaintiff is entitled to a declaration of its rights, not whether it entitled to a declaration in its favor."
- Canosa's allegation that the city has collected ALPR information about his vehicle for year and continues to do so creates a bona fide, actual, present need for declaratory judgment as to whether it violates his privacy rights.
- Case returned to the trial court for further proceedings.



Standing

In re OPM Security Breach Litigation, No. 17-5217 (DC Cir., 2019)

- Some of the 22M victims of the 2014 OPM breach who were not satisfied with the free fraud monitoring offered by OPM sued in multiple jurisdictions. Some alleged misuse of their information. Suits were consolidated into two suits and moved to DC.
- Plaintiffs claim OPM "willfully failed" to establish appropriate safeguard for their private information. OPM moved to dismiss for inter alia, lack of standing.
  - 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 *Attias v. CareFirst*, D.C Cir. case substantial risk of identity theft is enough.
- Court criticized trial court for doing extra-judicial research to conclude that China was behind the attacks and then use that to support OPM's argument that identity theft was probably not a substantial risk.
- Motions to dismiss must adhere to the facts in the record and draw all reasonable inferences in the plaintiff's favor.
- Dissenters argued that theft of data from government databases raises espionage as an "obvious alternative explanation," but this was rejected by the majority.
- 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.

CFAA

WhatsApp (Facebook) v. NSO Group, No. 3:19-cv-07123 (N.D. Calif.)

- Plaintiff alleges NSOG sent malware (Pegasus) to 1400 mobile devices to access WhatsApp messages after decryption 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
- CFAA violations based on TOS have generally been raised in cases of rogue employees or subcontractors, especially related to scraping. Under that line of cases the 9th Cir. came down pretty firmly against TOS violations being a CFAA violation (Oracle v. Rimini)
- Additional complications:
  - 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

Insurance

Landry's v. Insurance Co. of the State of PA, 4:18-cv-02679 (S.D. Tex.)

- Landry's suffered a data breach at several of its restaurant properties. It's card processor, Paymentech was assessed $22M by Visa and Mastercard for Landry's violation of PCI data security standards. Paymentech's contract with Landry's required reimbursement if Landry's failed to comply with Visa and Mastercard's standards.
- Paymentech sued Landry's, then Landry's sought payment from Defendant under its insurance policy
- Landry's invoked the "personal and advertising" injury clause of its insurance policy. The clause includes "injury … arising out of … oral or written publication, in any manner, of material the violates a person's right of privacy." D denied coverage, so Landry's sued D.
- D moves for summary judgment
- Issue: Can D win a summary judgment to deny coverage?

Holding

T/C holds Yes.

- Applies TX 8-corners rule. Insured's duty to defend based on allegations in the pleading and policy terms in contract.
- On that basis court concluded that the insurance provision cited by Landry's is part of a general commercial liability policy not related to cybersecurity breaches.
- Existing case law does not support 3rd party breach of data as a knowing or willing publication by plaintiff. Damages not "privacy" damages.
- Landry's appealed to 5th Cir and is awaiting a hearing.
- Takeaway: Companies should carefully review insurance contracts to determine to what extent they cover cybersecurity issues. In still pending *Mondelez* case insurer alleged no coverage for any "act of war." Other cases have been mixed on compensable coverage for cyber attacks.

Additional Issues to Watch

- **Penetration Testing**
  - *Coalfire cases* (two pen testers were arrested on charges of felony burglary and possession of burglary tools while conducting physical security testing under contract to the Iowa State Court Administration (SCA). The County law enforcement officers held them overnight in jail and only dropped the charges after almost 5 months.

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 and/or non-routine searches require reasonable suspicion?
  - Cyber insurance and "war" exclusions raise new concerns
- 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, Information Security Committee, 3 Mar 2019