

# RSA®Conference2020

San Francisco | February 24 – 28 | Moscone Center

**HUMAN**  
ELEMENT

SESSION ID: LAW-W13

## Cyber-Litigation 2020: Recent Cases in the Courts and Agencies



**MODERATOR: Julie Bowen, Moderator**

Senior VP, GC and Corp. Sec'y  
MITRE Corporation  
jbowen@mitre.org

**PANELISTS: Rick Aldrich, Presenter**

Cybersecurity Policy & Compliance Analyst  
Booz | Allen | Hamilton  
@AldrichRick, Aldrich\_Richard@bah.com

#RSAC

# Disclaimer and Legal Caveat

- This presentation is designed to raise awareness of general legal principles raised in several recent domestic and foreign cyber-related cases
- This session, and any information contained in this presentation, should not be construed as legal advice\*

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

# Significant Developments in Cyber Cases

- Interpreting *Carpenter*
  - Video surveillance
  - GPS
- GDPR-related cases
- Border Searches
- Cases and Issues to Watch



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

# **RSA**®Conference2020

## Cases

# Video Surveillance

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

- Facts of the case
- Issue: Does warrantless video surveillance from a public utility pole for ~3 months violate 4<sup>th</sup> Amendment?



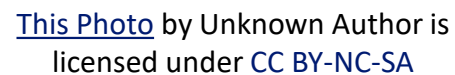
[This Photo](#) by Unknown Author is licensed under [CC BY-ND](#)

## Court 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 4<sup>th</sup> Amendment.
- 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 forty-nine 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: This is another extension of *Carpenter* that continues the trend of requiring warrants for digital devices that permit "pervasive tracking."

## Court Holding

- Dist. Ct.: Yes
- Extending *Carpenter* and *Jones* while limiting the application of the 3<sup>rd</sup> party doctrine, court finds 4<sup>th</sup> Amend. violation
- 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.





# GDPR-related Cases

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

- Facts of the case
- Issue: Can Google be required to de-reference on all versions of its search engine worldwide?



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

## Court 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.
- Takeaway: Suggests the GDPR will be interpreted in a way that limits impact outside of EU and recognizes conflict of laws issues.

# GDPR-related Cases

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

- Facts of the case
- Issue: Can Facebook be required to remove “lousy traitor,” “corrupt oaf,” and a member of a “facist party” as well as “equivalent” posts worldwide?



## Court Holding

- CJEU: Yes
- Facebook’s agreement to remove the original post for users in Austria deemed insufficient. 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)**

- Facts of the case
- Issue: Can manual or forensic searches of a cell phones at the border with no reasonable suspicion be limited under the 1<sup>st</sup> or 4<sup>th</sup> Amend?



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-SA](#)



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

## Court Holding

- Dist. Ct.: Yes
- Circuits are split: 4<sup>th</sup> and 9<sup>th</sup> require reasonable suspicion for forensic searches. 11<sup>th</sup> holds contra
- Extends rationale of *Riley* (computers are different)
- 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.

# Cases and Issues to Watch

- 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. Case to be heard starting the last week of January 2020.)

- 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 were only willing to negotiate the charges down to criminal trespass. To date the charges have still not been dropped. Sending shock waves through the pen testing community. Apparently SCA drafted an ambiguous contract, failed to get it legally reviewed. Coalfire had done similar pen testing for SCA four years earlier so did not expect problems.

- CFAA

- *WhatsApp (Facebook) v. NSO Group* (Facebook claims that NSO Group violated the CFAA by accessing and using WhatsApp's servers and the WhatsApp service without authorization by violating the terms of service.)

- Standing

- *In re OPM Security Breach Litigation, No. 17-5217 (DC Cir., 2019)* (“Viewing the allegations in the light most favorable to the Plaintiffs, as we must, we conclude that ... Plaintiffs face a substantial—as opposed to a merely speculative or theoretical—risk of future identity theft.”)

# Cases and Issues to Watch

- Biometrics

- *Nimesh Patel, et al v. Facebook, Inc., Case No. 18-15982 (9th Cir., 2019)* (unanimous ruling that the mere collection of an individual's biometric data was a sufficient actual or threatened injury under the Illinois Biometric Information Privacy Act ("BIPA") to establish standing to sue in federal court)

- Automatic License Plate Readers

- *Canosa v. Coral Gables* (Lawsuit contesting the city of Coral Gables 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. Coral Gables and other state defendants' motions to dismiss were denied on the key counts.)

- Government "Pings" of suspect's cell phone

- *Commonwealth v. Almonor, 482 Mass. 35 (2019)* (Government "ping" of suspect's phone to reveal its real-time location is a search under state's 4th Amend. equivalent.)

- Insurance

- *Landry's v. Insurance Co. of the State of PA* (Defendant, a subsidiary of AIG, claims it does not have to fund Landry's defense in a suit by JP Morgan Chase over breach-related costs.)

# **RSA**Conference2020

**Apply Slide**

**Strategic Next Steps**

# Apply What You Have Learned Today

- Next week you should:
  - Review your organization's exposure to GDPR or CCPA-related suits
  - Review contracts related to penetration testing
- In the first three months you should:
  - Take actions to update your organization's policies to minimize risk with regards to personal information, cloud providers, and cross-border data transportation
- Within six months you should:
  - Take actions to update your organization's policies to minimize risk with regards to insurance providers

**RSA**<sup>®</sup>Conference2020

**Questions**