RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: LAW-W05

What You Need to Know about the Cybersecurity Landscape and Cyber Cases

Julie Bowen, Moderator
Senior VP / General Counsel
The MITRE Corp.
jbowen@mitre.org

Rick Aldrich, Presenter
Cybersecurity Policy & Compliance Analyst
Booz | Allen | Hamilton
@AldrichRick, Aldrich_Richard@bah.com

Dr. Adriana Sanford, Presenter
International TV Commentator, International TV Commentator/ Professor- Cyber Security Law, Pepperdine University
www.adrianasanford.com
adriana.sanford@pepperdine.edu

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 or services*

* **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

US CASES

- Border Searches
- Data Breaches
- Privacy and Emerging Technology

FOREIGN CASES

- Noncompliance with GDPR
- Biometrics and Bulk Data Retention
- Surveillance and Intelligence Sharing
- Vicarious Liability for Data Breaches
- Border Searches and Digital Strips

Rick Aldrich
(US Domestic Law)

Dr. Adriana Sanford
(Multijurisdictional Conflicts)

RSAConference2019

US Cases

Booz | Allen | Hamilton®

Border Searches

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

- Facts of the case
- Issue: Can border agents conduct a forensic search of a cell phone at the border with no reasonable suspicion?

Court Holding

- 11th Cir.: Yes
- Circuits are split: 4th and 9th hold contra
- Compare with *Riley*
- 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.

Data Breaches and Standing

In re Zappos.com, 888 F.3d 1020 (9th Cir. 2018)

- Facts of the case
- Issue: Does a person who sues for a data breach based on fear of future identify theft or fraud have standing?

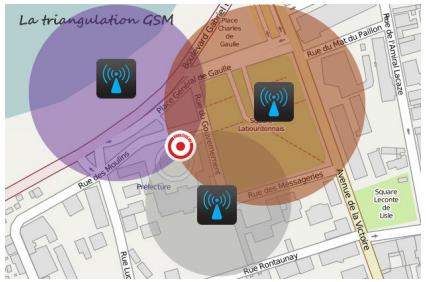
Court Holding

- 9th Cir. Court: Yes, based on *Krottner v. Starbucks*, rejecting contention that Supreme Court's decision in *Clapper v. Amnesty Int'l* overruled it. Reversed T/C dismissal (based on lack of Art. III standing)
- 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.

4th Amendment Equilibrium Adjustment

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

- Facts of the case
- Issue: Is the warrantless search and seizure of 127 days of cell site location information a 4th Amendment violation?



Court Holding

- Supreme Court: Yes
- Extending *Riley* and *Jones* while limiting the application of the 3rd party doctrine
- 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 REOP.

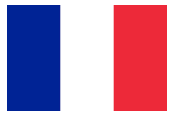
US Cases and Issues to Watch

- Cyber insurance
  - *Mondelez Int'l v. Zurich American Insurance*, No. 2018L011008 (Pending case in which Zurich denied a $100M claim by Mondelez for damage from NotPetya on the basis that it was caused by an "act of war."
- Private search in the cloud
  - *United States v. Reddick,* No. 17-41116 (5th Cir., 2018) (Gov't search of cloud files without a warrant did NOT violate 4th Amendment because Microsoft's hash scan already frustrated defendant's expectation of privacy.)
- Biometrics
  - *In the Matter of Search of a Residence in Oakland, California,* No. 4-19-70053 (N.D. Calif, Jan. 10, 2019) (Judge denies search warrant seeking among other things to authorize federal agents to compel all present at search to submit biometrics to unlock electronic devices or to seize digital devices other than those owned/possessed by the suspects named in the affidavit.)
- CFAA
  - *Dearman v. H&M Pipe Beveling,* No. 18-cv-250-GKF-JFJ (N.D. Okla., Sept. 5, 2018) (Privileged users who transfer corporate intellectual property to competitor not liable under Computer Fraud and Abuse Act.)

RSAConference2019

Foreign Cases

Noncompliance with GDPR - Forced Consent

France (2019) 

GOOGLE

- Google fined nearly $57 million
* Importance: first big tech company to be fined under Europe's strict GDPR

France's Regulatory Authority (CNIL):

- "….infringements observed regarding the essential principles of the GDPR: transparency, information and consent"

Collection/Use of Personal Data under More Scrutiny

Germany (2019) 

FACEBOOK

- “Far-reaching restrictions" on Facebook's practice of merging its users' data from WhatsApp, Instagram and millions of third-party websites and apps

* Importance: Under GDPR, tech companies face increased scrutiny over handling personal data.

German Federal Cartel Office, Bundeskartellamt:

- “Facebook will no longer be allowed to force its users to agree to the practically unrestricted collection and assigning of non-Facebook data to their Facebook user accounts”

Bulk Data Collection; Surveillance; Intelligence Sharing

United Kingdom (2018) 

Big Brother Watch & Others v. UK

- Case challenged three types of surveillance conducted by UK's signals-intelligence agency

* Importance: 1st ruling against UK mass-surveillance programs since Snowden's 2013 revelations

European Court of Human Rights (ECHR):

- UK's bulk data-collection programs *violate* human rights law
- Mass surveillance and intelligence sharing *do not violate* international law

Landmark "Right To Be Forgotten" Case

United Kingdom (2018) 

GOOGLE

- Businessman wins case to remove search results about criminal conviction. Internet searches contained details from over 10 years ago

* Importance: Landmark case for GDPR (cases in courts in EU states turn on individual circumstances and facts; case-by-case basis). More likely that there will be an increase in the number of *successful* requests

High Court in London:

- Remorseful businessman has right to be forgotten
- Since 2014, individuals from France, Germany and the UK generated 51% of requests received by Google to remove 2.4m links from search results

Landmark Privacy Ruling - Biometrics

India (2017)

Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India and Ors

- Petition challenging the constitutional validity of the world's greatest biometric ID card program, Aadhaar

* Importance: Largest democracy in the world issued historic privacy ruling

India's Supreme Court:

- "Unprecedented need for regulation regarding [how] such information can be stored, processed and used"
- Regulatory innovation in India has far reaching implications

Data Breach: Vicarious Liability for Rogue Employees

United Kingdom (2018) 

WM Morrison Supermarkets PLC v Various Claimants

- Employer held liable for criminal actions of rogue employee in disclosing personal information although he was not '*on the job*' when tortious act was committed
- Rogue employee's wrongful acts were "deliberately aimed at the party whom the claimants sought to hold responsible", such that to reach the conclusion seemed "to render the court an accessory in furthering his criminal aims"
- * Motive Irrelevant: Rogue employee's motive was, by causing harm to third parties through a data breach, to cause financial or reputational damage to employer

Court of Appeal employs:

- The '*within the field of activities assigned to the employee*' test

Repeated Pattern in Online Defamation Cases/ Autocomplete Feature; Linking to Defamatory Content

Australia (2018)

GOOGLE

- Google's autocomplete feature returned phrases like "is a former hit man," ''criminal" and "underworld“

* Importance: Highlights complex multijurisdictional problem

Australian High Court:

- Trkulja can sue for defamatory search results
- Under US law, defamation is hard to prove and US websites are not liable for comments made by their users

Intrusive Border Device Searches in Other Territories

New Zealand (2018)

- Travelers must surrender passwords, codes, encryption keys and other information to enable access to electronic devices
- Fined up to $5000 (US$3,300); device seized and forensically searched
- Border agents have similar powers in Australia
- Canada was the first country to fine travelers who refuse to hand over their passwords (between November 2017 - March 2018 the Canadian Border Services Agency examined the devices of 4,529 travelers)
- Concerns about customs/security searches of digital devices are increasing among corporate travelers

Multijurisdictional Cases and Issues to Watch

- **GDPR Variations and CCPA Spinoffs**
- **Possible Criminal Liability**
  - Planned Obsolescence
  - Extraterritorial Searches; Extreme and Disproportionate Measures
- **Potential for Hefty Fines**
  - Bundling search engine and apps into operating system
  - ‘Abusive’ App Developer Practices
  - Tracking people through cookies on third-party websites
- **More Privacy Concerns**
  - Artificial Intelligence, Blockchain

RSAConference2019

“Apply” Slide

Strategic Next Steps

Apply What You Have Learned Today

- Next week you should:
  - Review your organization's policy on transporting electronic files across borders
- In the first three months you should:
  - Identify personal information your company holds on individuals that could subject you to a class action if lost or stolen
  - Review contracts with cloud providers and insurance providers
- Within six months you should:
  - Take actions to update policies to minimize risk with regards to personal information, cloud providers, insurance providers, and cross-border data transportation

- New Multijurisdictional Challenges Ahead
  - Numerous nations have issued data protection laws. Identify foreign territories where suppliers, customers, and third parties are located. Some territories may appear even stricter than GDPR in terms of cross-border data transfer for purposes which include safeguarding cyberspace sovereignty, national security, or public interests
  - Take action to amend and update data protection guidelines (make policies clearer and privacy settings easier to find). Introduce tools for people/users to access, download, and delete their information so in compliance with foreign laws, particularly GDPR or variations therefrom

- New Multijurisdictional Challenges Ahead
  - Keep up with foreign laws and regulations and seek timely professional advice for interpretation and compliance with new foreign rules that may conflict with domestic rules
  - Discuss the complexities of open-ended situations with senior management and the Board, particularly when there are severe consequences from foreign jurisdiction non-compliance

"Your decisions may have strong repercussions on a global scale"