EMCS 2600 The Future of Cybersecurity: Technology & Policy

Transborder Issues – Part I

John E. Savage

Outline

- The Microsoft and Google cases
- The Budapest Convention
  - Article 32b
- The Russian position on the convention
- Supreme court hearing
- The CLOUD Act
- Proponents and opponents of CLOUD Act

The Microsoft (MSFT) Case

- DOJ obtained a warrant under the Stored Communications Act (SCA) asking MSFT to produce a suspected drug trafficker's email under MSFT control on its Irish servers.
- MSFT refused and lost the case.
- On appeal, the court deadlocked.
- Supreme court granted DOJ appeal on 10/16/17

The Microsoft Case*

- MSFT asserted that a) SCA does not apply abroad and b) the relevant territorial question is "where the data is stored?" not "where MSFT is located?"
- DOJ argues: "The provision [of the SCA] is applied domestically when a court issues a warrant to a provider in the United States requiring disclosure in this country of material over which the provider has control, regardless of whether the provider stores that material abroad."
- DOJ cites banking cases where courts allowed subpoenas to compel banks to produce foreign-held banking records. If the *disclosure* happens in the U.S., that is the relevant location – wherever the provider chooses to store it.

* https://lawfareblog.com/primer-microsoft-ireland-supreme-courts-extraterritorial-warrant-case

Is this a Privacy or Sovereignty Case?

- If DOJ won, data residing abroad but controlled by and accessible to a company doing business in the US would be accessible to the US government.
  - Would sovereignty of other nation be violated?
  - Might US tech companies lose trust of its customers?
- If MSFT won, bad actors might evade US law by moving data to an inaccessible country.
  - Could diplomacy (MLATs) be used to obtain access?
  - Would it incentivize data localization efforts?
- US v. MSFT to be argued at SCOTUS 2/27/18

The Google Email Case

- Google case almost identical to MSFT case
- 2/4/17 Federal judge requires compliance
  - He rules that moving email to US servers did not qualify as seizure.
  - He ruled privacy was given up when using Gmail
- Google appeal denied on 7/31/17
- Prosecutors want Google fined until it complies
- Case held until Supreme Court decision on MSFT

(Budapest) Convention on Cybercrime*

- 2004 – First international treaty on cyber crime
  - Produced by Council of Europe, signed in Budapest
  - 63 states have ratified this treaty
  - US accession occurs to it in 2007
- Harmonizes national laws on cybercrime
  - E.g. fraud, threats, copyrights, interference, racist or xenophobic acts, child pornography, etc.
- Fast and effective regime for intl. cooperation
  - Mutual legal assistance treaties (MLATs) are slow
- Helps recover real and stored communications data
  - The "transborder provision" replaces MLATs

* http://cs.brown.edu/people/jes/EMCS2600Readings/Module8/2001_11_23_CoE_CybercrimeConvention.pdf

~2006 ACLU Objections to Treaty

- Too broad, lacks protections for privacy & civil liberties
- Lacks "dual criminality" requirement for US cooperation with foreign police – extradition only if similar law in both
- Protection for political activities is too weak
  - E.g. Potential political use of the transborder provision
- Threatens to further unbalance US IP law – no fair use
  - Appears to make copyright violations extraditable
- It would give police invasive surveillance powers
- Drafting was closed & secretive by law enforcement
  - No seat at table for industry or public-interest groups

Convention Trans-Border Article 32b

- A Party (A) may, without the authorization of another Party (B):
  - Access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
  - Access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Position of the Russian Federation

- Not a signatory: it sees 32b as violation of its sovereignty
  - Asserted by Ilya Rogachev at EWI 2015 Cyberspace Summit

  - Director of Russian Foreign Ministry Department for New Challenges and Threats, which includes transnational crime
- He told me that Russia would sign if 32b removed!
- If so, how many Russian allies would join?
- Would that help reduce cybercrime?

Understanding 32b

- A Party (Nation A) may, without the authorization of another Party (Nation B): Access or receive, through a computer system in its territory (A), stored computer data located in another Party (B), if the Party (A) obtains the lawful and voluntary consent of the person (B) who has the lawful authority to disclose the data to the Party (A) through that computer system.
- To which jurisdiction does lawful authority refer?
  - If B, then domestic legislation could prevent transfers
  - If A, then MSFT could be forced to give up email

Understanding 32b

- Because of Yarovaya Law, Russian companies must disclose data to authorities.
  - If comms data encrypted, must give FSB access
  - Internet and telecom companies must disclose "all other information necessary" to authorities on request without court order. (See Wikipedia.)
- Must Kaspersky provide such data, even if in US?
- If Russia were to sign Budapest Convention, would this law be seen as valid internationally?

China's Internet Regulation

- National Intelligence Law of the PRC*, 6/27/2017

  Article 7 An organization or citizen shall support, assist in and cooperate in national intelligence work in accordance with the law and keep confidential the national intelligence work that it or he knows.

- How would this law be viewed if China were to ratify the Budapest Convention?
- How does this law impact Huawei's business?

* http://cs.brown.edu/courses/csci1800/sources/2017_06_28_China_NationalIntelligenceLawOfThePeoplesRepublicOfChina.pdf

Law Enforcement vs Sovereignty

- If the Supreme Court had authorized global reach of US law concerning data, would it legitimate the same action by other nations?
- Would this imply that in cyberspace there are no legal boundaries?
- Would that be the end of sovereignty?

Supreme Court Hearing

- MSFT Ireland case heard on February 27, 2018
  - Justices on both sides of the MSFT case
  - Some said Congress should decide or update SCA
  - Sovereignty concerns are real, some judges indicate
  - How might the world react?
- Before the case was heard, Congress enacted the CLOUD Act, discussed in Part II of this lecture

* https://www.lawfareblog.com/analysis-microsoft-ireland-supreme-court-oral-argument

EMCS 2600 The Future of Cybersecurity: Technology & Policy

Transborder Issues – Part II

The CLOUD Act

John E. Savage

The CLOUD Act is Passed, 3/23/18

- Clarifying Lawful Overseas Use of Data Act
  - Creates new subsections under
    - Secure Communications Act
    - Wiretap Act
  - Amends sections of both acts
- Serious objections from two important NGOs:
  - Electronic Privacy Information Center (EPIC)
  - Electronic Frontier Foundation (EFF)

EPIC Objections*

- "Act provides a mechanism for communications provider to challenge the order if disclosing the data would risk violating foreign law."
- "[L]egal protection of an individual's rights depends on the objection by a provider."
- "[N]o direct mechanism for individuals to challenge an order under the CLOUD Act"
- "A court will consider a provider's challenge of an order for disclosure of data"

* https://epic.org/privacy/cloud-act/

EPIC Objections*

- "U.S. court can require production of that data despite the objection, even where the laws of another nation would be violated."
- It "permit[s] federal officials to enter into executive agreements granting foreign access to data stored in the United States, even if that data would otherwise be protected under ECPA."

* https://epic.org/privacy/cloud-act/

EPIC Objections*

- But “federal officials must first decide that a foreign government meets certain generalized standards for sufficient protections of privacy and civil liberties.”
- “The foreign government must also agree to abide by several other limitations, including minimizing any U.S. person data collected."

* https://epic.org/privacy/cloud-act/

EPIC Objections*

- "The initial agreement need only be certified by executive branch officials to take effect"
- "Congress can object to the agreement but need not formally approve the agreement."
- "The agreement is also not subject to review by any court."
- "Once an agreement is in place, … [t]he foreign access will be granted without review of whether the request complies with the requirements of the executive agreement or other legal standards."

* https://epic.org/privacy/cloud-act/

CLOUD Act*

- "[T]o transfer U.S. persons' communications content, the communications must merely be determined to 'relate[] to significant harm' and non-content information may be transferred without limitation."
- "[T]he U.S. government could access U.S. persons' communications without satisfying existing U.S. legal standards."

* https://epic.org/privacy/cloud-act/

EPIC Objections*

- “While the Cloud Act earns applause from some of Silicon Valley’s biggest consumer-facing companies for making ‘notable progress to protect consumers’ rights,’ some digital-rights groups argue that it does the exact opposite.”
- “The Cloud Act ‘creates an aggressive expansion of U.S. jurisdiction against the rest of the world,' adds Camille Fischer, a free-speech and government transparency fellow at the Electronic Frontier Foundation. ‘It allows the U.S. to seek data, no matter where it’s stored.’ ”

* https://epic.org/privacy/cloud-act/

Dangerous Expansion of Police Snooping on Cross-Border Data - EFF†

- "Senators Hatch, Graham, Coons, and Whitehouse introduced a bill that diminishes the data privacy of people around the world."
- Act allows local & federal law enforcement to
  - "[A]ccess … a user's content and metadata, even if it is stored in a foreign country, without following that foreign country's privacy laws."
- President can "enter into 'executive agreements' with foreign governments that would allow each government to acquire users' data stored in the other country, without following each other's privacy laws."

† https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data

EFF Objections†

- A “foreign country that enters [an] …executive agreement with the U.S. could potentially wiretap people located anywhere on the globe (so long as the target … is not a U.S. person or [in the US]) without the procedural safeguards of U.S. law typically given to data stored in the United States, such as a warrant, or even notice to the U.S. government. This is an enormous erosion of current data privacy laws.”

† https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data

EFF Objections†

- "The CLOUD Act would give unlimited jurisdiction to U.S. law enforcement over any data controlled by a service provider, regardless of where the data is stored and who created it. "
- [This} "creates a dangerous precedent for other countries who may want to access information stored outside their own borders, including data stored in the United States."

† https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data

Microsoft/DOJ Case Mooted

- On April 17, 2018 Supreme Court dropped the Microsoft vs. US DoJ case.
  - Both Microsoft and DoJ agreed to drop the case
- However, many CLOUD Act implementation issues remain unresolved*, e.g.
  - Warrants or subpoenas for data on non-US persons?
  - Can data obtained used for capital punishment?
  - Will judicial authorization be required to send data?
  - What about requests violating freedom of speech?

* https://www.lawfareblog.com/cloud-act-implementation-issues

Sovereignty Issues

- Does the CLOUD Act violate sovereignty?
- What issues can you foresee emerging?

Review

- The Microsoft and Google cases
- The Budapest Convention
  - Article 32b
- The Russian position on the convention
- Supreme court hearing
- The CLOUD Act
- Proponents and opponents of CLOUD Act