EMCS 2600 The Future of Cybersecurity: Technology & Policy

Transborder Issues

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 asserts 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 wins, data residing abroad but controlled by and accessible to a company doing business in the US must be accessible to US government.
  – Would sovereignty of other nation be violated?
  – Might US tech companies lose trust of customers?
• If MSFT wins, bad actors might evade US law by moving data to an inaccessible country.
  – Can diplomatic channels be used to obtain access?
  – Would it incentivize data localization efforts?
• US v. MSFT to be argued on February 27, 2018
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.
  – Rules that privacy was given up when Gmail used
• Google appeal denied on 7/31/17
• Prosecutors want Google fined until it complies
• Case on hold until Supreme Court decides MSFT
(Budapest) Convention on Cybercrime*

• 2004 – First international treaty on cyber crime
   – Produced by Council of Europe, signed in Budapest
   – 56 states have ratified this treaty
   – US accession 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

~2006 ACLU Objections to Treaty

- Too broad, lacks privacy, civil liberties protections
- Lacks “dual criminality” requirement for US cooperation with foreign police
- 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 closed & secretive by law enforcement
  - No seat at table for industry or public-interest groups
Trans-Border Article 32B

- A Party (nation) may, without the authorization of another Party:
  - 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.
  – Must Kaspersky provide data it holds, even in US?
• If Russia were to sign treaty, would this law be seen as valid internationally?
• Are there any lawyers in the room who can help solve this problem?
Law Enforcement vs Sovereignty

- If the Supreme Court authorizes 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?

The CLOUD Act

• Clarifying Lawful Overseas Use of Data Act
  – No targeting of US citizen & resident data without warrant based on probably cause
  – No indirect targeting (sharing back) of US citizen data without significant harm or threat of such to US
  – Requests must be particularized
  – Request must be based on “articulable and credible facts”
  – Requests must be subject to “review or oversight” by court, judge, etc.
The CLOUD Act

- Clarifying Lawful Overseas Use of Data Act
  - Intercept orders for “fixed, limited duration” and for info that cannot be obtained by less intrusive means
  - No use of data to infringe on freedom of speech
  - Requires govts to agree to compliance reviews
  - Act applies only to state that “affords robust substantive and procedural protections for privacy and civil liberties”, as determined by attorney general and secretary of state. Congress has 90 days to object
Objections to CLOUD Act

• 24 privacy, civil liberties, HR orgs object to Act
  – US law enforcement could compel access to information on anyone living anywhere
  – Allows Attorney General to make agreements that bypass current law without approval from Congress
  – Would allow bypass of MLATs
    • MLATs require foreign govt requests be reviewed by DOJ
    • Judge must find probably cause, may consider human rights
  – Would not meet warrant requirement of 4th Amendment
  – Disagrees with tech companies – say the act makes “notable progress to protect consumers’ rights”
Objections to CLOUD Act

• Specific objections:
  1) Allows foreign governments to wiretap on US soil under terms that do not comply with US law
  2) Gives executive branch the power to enter into foreign agreements with no Congressional approval
  3) Possibly facilitate foreign governments access to information that is used to commit human rights abuses, like torture
  4) Allow foreign governments to obtain information that could pertain to individuals in the U.S. without meeting constitutional standards
Support for CLOUD Act

• Daskal & Swire argue CLOUD Act is a good bill*
  – Bill would improve privacy and protect civil liberties without such legislation
  – Updates Mutual Legal Assistance (MLA) process
    • Current MLA process is slow, cumbersome, needs fixing
    • In some cases, CLOUD Act obviates need for MLA process
  – If requests for data on US person, MLA must be used
  – If on non-US persons, no need for MLA process
  – US can review what govts do with data given by US

Support for CLOUD Act

• Daskal & Swire argue CLOUD Act is a good bill*
  – Foreign govts “frustrated by MLA system, which they see as imperialist attempt to insist that (they) obtain a warrant issued by a U.S. judge even for data needed in the investigation of local crimes.”
  – Such govts seek to bypass MLA system
    • Could result in data localization
  – US has limited time to use its leverage to set privacy-protective standards

Support for CLOUD Act

• Daskal & Swire would add to CLOUD Act:
  – More protection for human rights & privacy groups
  – Possible role for Privacy and Civil Liberties Oversight Board
  – Support adding provisions of the E-mail Privacy Act
    • To codify requirement for probable cause warrants for US demands for communication content

• Big Tech Supports Cloud Act†
  – Apple, Facebook, Google, Microsoft, Oath

† https://www.the-parallax.com/2018/03/14/tech-supports-cloud-act-overseas-data/
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
CLOUD Act