ATTRIBUTION & THE GLOBALIZATION OF CRIMINAL EVIDENCE

PETER SWIRE
GT CYBERSECURITY SUMMIT
SEPTEMBER 27, 2017
1) Attribution increasingly vital
2) Attribution is harder when the attacks come from other countries
3) We are getting the “globalization of criminal evidence”
4) Mutual Legal Assistance (MLA) is a key way nations cooperate
5) We at Georgia Tech are leading research on MLA
6) If we don’t fix MLA, we’ll get a much worse Internet
STEWART BAKER: “PICKING AWAY AT THE IMPUNITY PROBLEM”

“It could be, or it could not be, it depends only on politics,” Protexer responded. “If U.S. law enforcement wants to take me down, they will not wait for me in some country’s airport. Relations between our countries are so tight I would be arrested in my kitchen, at the first request.”

(1) Do attribution (2) Get usable criminal evidence (3) Prosecute in US or abroad
CROSS-BORDER EVIDENCE IS MUCH HARDER FOR LAW ENFORCEMENT

1) **Easy:** Hacker is in the US, get evidence in the US, arrest in the US

   1) That drove the spammers out of the US:

   ‘Spam King’ Sanford Wallace Sentenced to 2½ Years for Facebook Scheme

2) **Much harder:** Hacker is in a not-so-friendly government, evidence often there, *maybe* can arrest there

3) **To make this better:** *Stronger international cooperation* to get the evidence and make the arrests
1) In pre-cyber days, local crime and local evidence

2) Globalization today – police can’t get evidence locally, for data at rest and data in transit

3) Data at rest:
   1) Evidence of the hack often in servers and networks in a different country
   2) Email, social network information, much more stored in the cloud
   3) Cloud often in a different country – local legal process doesn’t work

4) Data in transit:
   1) Police used to do wiretaps, locally
   2) Today, wiretaps don’t work due to encryption (HTTPS, etc.)

5) “Globalization of Criminal Evidence” – huge pressure on cross-border cooperation
Cross-Border Requests for Data Project

1. **Fulfill legitimate law enforcement requests**, to investigate cybercrimes and other crimes where evidence is held in a different country;

2. **Protect privacy and civil liberties** in the United States and globally, by assuring due process before evidence is sent to a different country;

3. **Provide a workable regime** for the companies holding the communications records; and

4. **Safeguard the Internet** by resisting calls to localize data and splinter the Internet.

**Lead Funding:**
- Hewlett Foundation
- Apple
- Facebook
- Google
- Microsoft
Surveillance, Privacy and Data across Borders: Transatlantic Perspectives

Panel 2: Hacking, Attribution, Technology & MLA

Keynote: Achieving Individual Privacy and International Security Cooperation in a Shifting Landscape

Bruno Gencarelli, Head of Unit, DG-Justice, European Commission
1) The Goal
   1) Develop evidence of attribution
   2) Cooperate to investigate and prosecute

2) Critiques of current system of Mutual Legal Assistance
   1) Slow – average 10 months or more
   2) Designed for small sub-set of crimes, before globalization of criminal evidence
1) Improve the mechanics
   • Online MLA portals/requests, standardize forms, more transparency, etc.

2) Enable direct access to partner countries
   • Similar to Visa Waiver Program, with its 37 countries and reciprocal safeguards
   • US/UK agreement in Congress now, allowing UK direct access to US content (and vice versa), with (perhaps sufficient) safeguards
   • Swire & Desai Lawfare article on a similar approach to scale to India and others

3) Research to map the protections of national legal systems
   • GT papers on U.S. & France, to show differences yet similar overall protections

4) Law enforcement vs. intelligence vs. military sharing
   • Attribution might happen in non law-enforcement settings; how to share that
1) If we **don’t** improve MLA and attribution, then law enforcement will push harder for other tools to get the evidence

1) If local wiretaps don’t work in investigations, that supports **limits on strong encryption**
   - For instance, the cloud providers or other networks are abroad, so need to wiretap locally

2) If can’t get MLA, then use more **“lawful hacking”**
   - For instance, no cooperation in Russia or other country, so enable law enforcement to conduct hacks there (and other countries will hack us, too)

3) If can’t get MLA, and evidence abroad, then **require localization of data**
   - For instance, Russia and others require data to be stored locally, and that could spread to many countries, splintering the Internet

**WHAT IF WE DON’T IMPROVE CROSS-BORDER COOPERATION?**
1) We face the “globalization of criminal evidence”
   - That evidence is crucial to attribution and prosecution, to reduce “impunity”
   - Mutual legal assistance improves the lawful structure for cross-border cooperation

2) If don’t, then get more pressure for
   - Limits on strong encryption
   - Lawful government hacking
   - Data localization

3) In conclusion, improving MLA is far more important today:
   - To help attribution
   - To fight cyberattacks and other crime
   - To preserve the global Internet
THANK YOU!

GT CROSS-BORDER REQUESTS FOR DATA PROJECT
CYBER.GATECH.EDU/CROSS-BORDER-DATA-PROJECTS

PETER SWIRE
PETER.SWIRE@SCHELLER.GATECH.EDU