“The Non-Code Layers of the Cyberstack & the Globalization of Criminal Evidence”

Peter Swire

IISP: Friday Cyber Lecture

October 13, 2017

Georgia Tech | Ernest Scheller Jr. College of Business

Overview

- Swire background
- Non-code layers of the cyber stack
  - Lessons for the big picture on cybersecurity vulnerabilities
  - Goal – publication in something like Communications of the ACM
  - This audience may have very useful suggestions on how to improve this presentation/paper; peter.swire@scheller.gatech.edu
- Globalization of criminal evidence
  - Third year of research project in this area

Peter Swire Background

- Princeton, Yale Law School
- Law professor, first article on law of the Internet in 1993
- President Clinton’s Chief Counselor for Privacy
  - HIPAA, financial privacy rules
  - Chaired WH Working Group on Encryption
  - Chaired WH Working Group on how to update wiretap laws for the Internet
- One of first law professors to teach law of cybersecurity (2003)
- President Obama’s Review Group on Intelligence and Communications Technology (“NSA Review Group”)
- Assoc. Director of Policy, GT Institute for Information Security & Privacy
- CoC/MGMT/PubPol 4726/6726: “Privacy Technology, Policy, and Law” (fall 2018)
- CoC/MGMT/PubPol 4725/6725: “Information Security Strategies and Policies” (spring 2019)

December 2013: The Situation Room

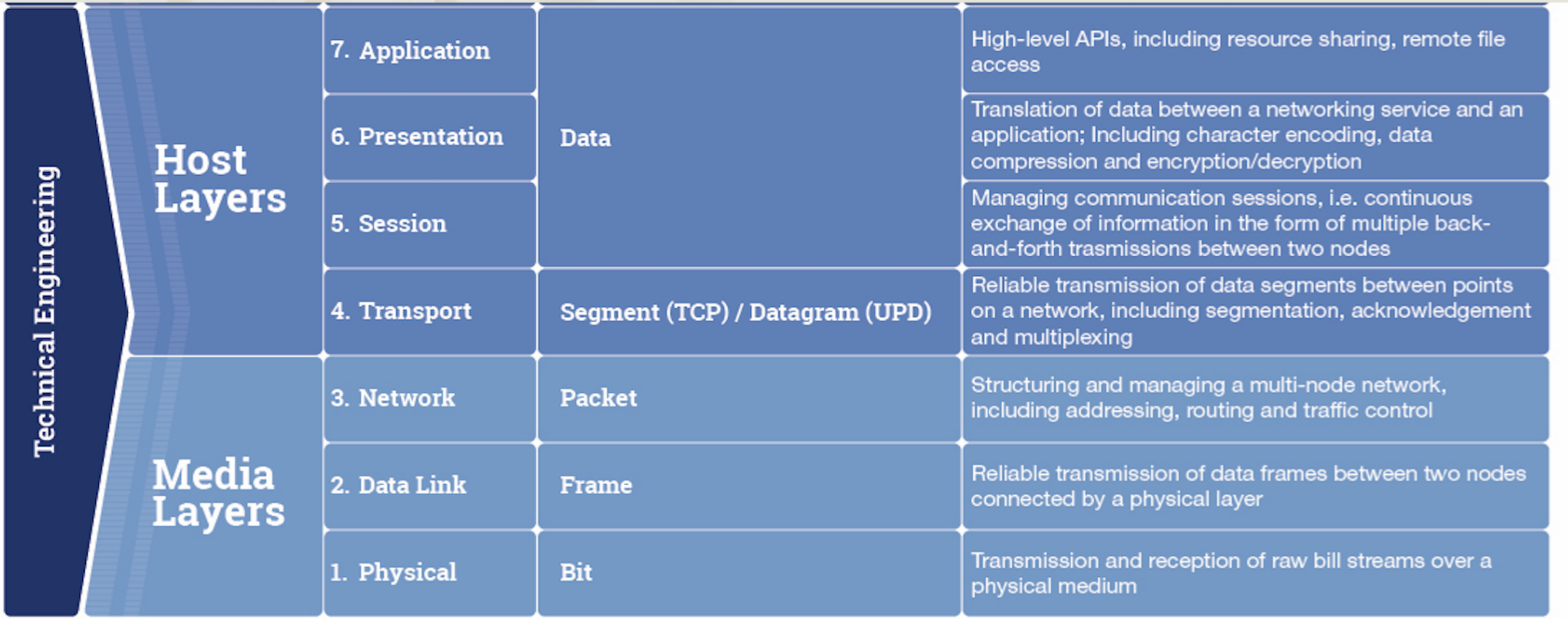
Non-code layers of the stack

- I have taught law and policy of cybersecurity for 15 years
- For coursework and research on cybersecurity:
  - **“Real”** cybersecurity is about writing code and doing technical work
  - The **“soft”** issues are seen as **not central** to the task of cybersecurity
  - Vague approval of “**inter-disciplinary**” studies for cybersecurity
    - But, with a **lower priority** than “real” cybersecurity
- My remarks today:
  - A new **conceptual framework**
  - **Organizes** numerous, important, & non-technical cyber-issues
  - Presents the curriculum and issues in ways that make sense to **both technical and non-technical audiences** in cybersecurity

The Genesis of this Project

- CoC/MGMT/PubPol 4726/6726 “Information Security Strategies and Policy”
  - This is my fourth time teaching the course, now required for Masters in Information Security
  - How do all the pieces of this course fit together? There seems to be something coherent, but it’s been hard to describe
  - Last year – 3 parts of the course
    - **Government laws/regulations** – project on proposed V2V cybersecurity regulation
    - **Corporate cybersecurity policies and governance** – project on GM or Ford implementing the regulation
    - **Nation state and international** – project on responding to cyberattack on Air Force One
  - My answer now: 3 layers of the cyber stack – organizational, governmental, international

Seven Layers of the OSI “Stack”



Technical Engineering	Host Layers	7. Application	Data	High-level APIs, including resource sharing, remote file access
		6. Presentation		Translation of data between a networking service and an application; Including character encoding, data compression and encryption/decryption
		5. Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth trasmissions between two nodes
		4. Transport	Segment (TCP) / Datagram (UPD)	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
	Media Layers	3. Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
		2. Data Link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
		1. Physical	Bit	Transmission and reception of raw bill streams over a physical medium

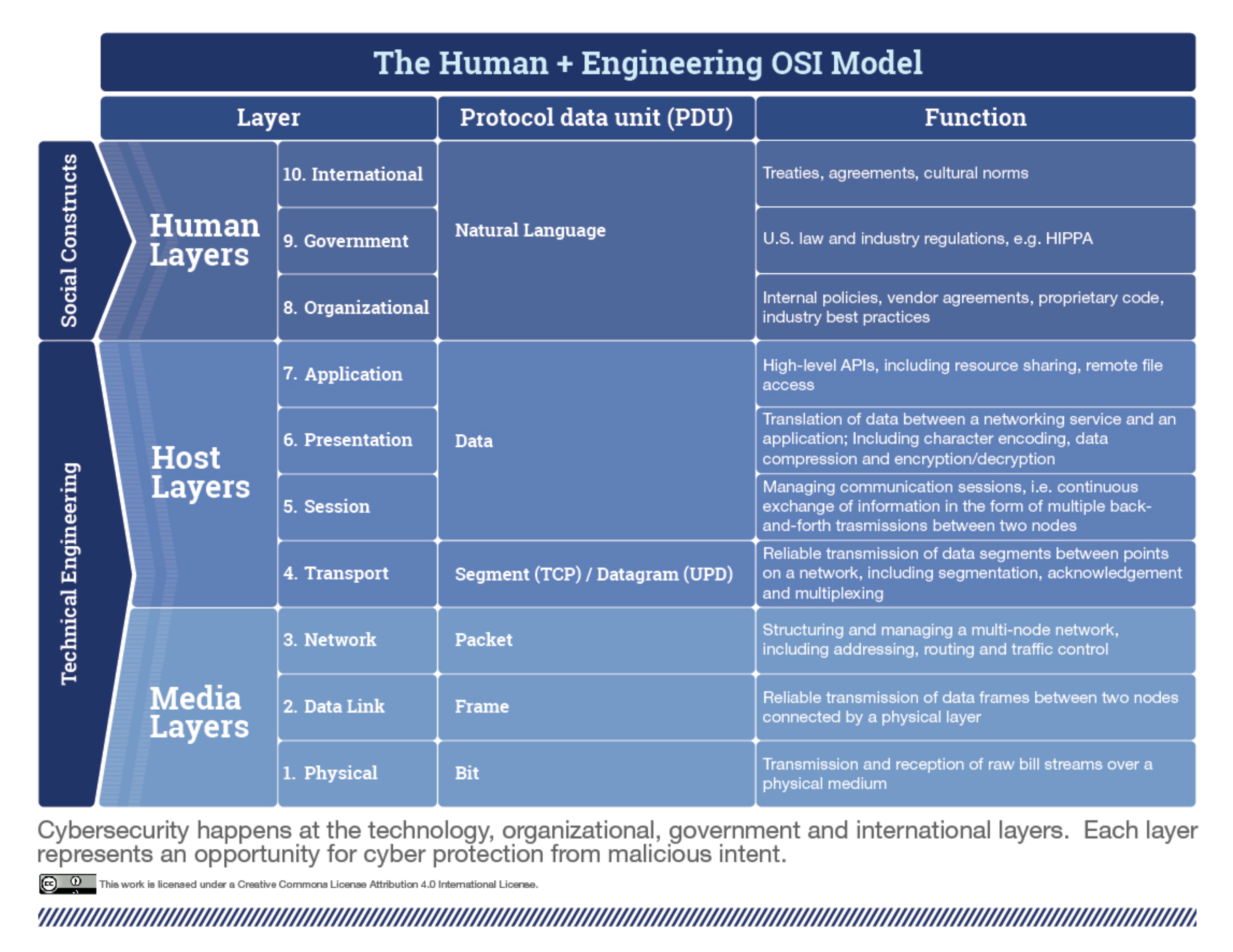
In my experience, these seven layers are well known to knowledgeable computer people who work on cybersecurity. Intuitively, they also know that cyber-attacks can happen at any of these 7 levels.

Some Cyber Vulnerabilities

Layer	Vulnerability
1. Physical	Cut the wire; stress equipment; wiretap
2. Data link	Add noise or delay (threatens availability)
3. Network	DNS and BGP attacks, false certificates
4. Transport	Man in the middle
5. Session	Session splicing (Firesheep); MS SMB
6. Presentation	Attacks on encryption; ASN-1 parser attack
7. Application	Malware; manual exploitation of vulnerabilities; SQL injection; buffer overflow

Thanks to Bob Blakely for assistance with this material.

What is Missing from the 7 Layer OSI Model?



The Human + Engineering OSI Model

	Layer		Protocol data unit (PDU)	Function
Social Constructs	Human Layers	10. International	Natural Language	Treaties, agreements, cultural norms
		9. Government		U.S. law and industry regulations, e.g. HIPPA
		8. Organizational		Internal policies, vendor agreements, proprietary code, industry best practices
Technical Engineering	Host Layers	7. Application	Data	High-level APIs, including resource sharing, remote file access
		6. Presentation		Translation of data between a networking service and an application; Including character encoding, data compression and encryption/decryption
		5. Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth trasmissions between two nodes
		4. Transport	Segment (TCP) / Datagram (UPD)	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
	Media Layers	3. Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
		2. Data Link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
		1. Physical	Bit	Transmission and reception of raw bill streams over a physical medium

Cybersecurity happens at the technology, organizational, government and international layers. Each layer represents an opportunity for cyber protection from malicious intent.

Layers 8, 9, and 10: Natural Language

Layer 10	International	Natural language	Diplomacy
Layer 9	Governmental	Natural language	Law
Layer 8	Organizational	Natural language	Contracts
Layers 1-7	OSI stack	Computer Code	Various protocols

Layer 8: Private-Sector Organizations: Role of Contracts

	Within the Organization	**Relations with Other Actors**	**Other Limits on Private Sector**
Examples of cyber law and policy	• Internal policies (e.g., incident response plans) • Training • Cyber hygiene • Roles, such as CISO	• Vendor relations • Other counter-parties, including customers • Cyber-insurance • Private-sector information sharing	• PCI-DSS and other industry standards • Technical standards such as IETF • Norms – follow the standards

Layer 9: Public Sector, Governmental Layer: The Law

	Within the Organization	Relations with Other Actors	Limits on Government
Examples of cyber law and policy	• HIPAA, GLBA, and other cyber rules • Other state-created defensive measures (FTC Sec. 5, etc.) • Rules limiting strong encryption	• Computer Fraud & Abuse Act and other limits on offense • CISPA and public-private partnerships and information sharing	• Constitutional limits on state action, such as 4th Amendment • Statutory limits on state action, such as ECPA and FISA

Layer 10: International Layer: Diplomacy

	Within the Nation	Relations with Other Nations	Other Limits on Nations
Examples of cyber law and policy	• Unilateral cyber actions, on spectrum from war to “cyber-peace” • Deterrence against aggressive cyberattacks	• Formal treaties, including MLATs • Less formal agreements, such as US/Russia • Aggressive actions • Cooperation against attacks	• Possible supra-national governance, such as by UN or ITU • Role of international law, including laws of war • ISO standards/norms

Where do Users fit?

- A user is not a government or an international actor
- I suggest part of Layer 8
  - Could be called “private sector” instead of “organizational” layer
  - Private sector actors range from individual users/sole proprietorship to modest size to large organizations
- Users lack an IT department, a general counsel, and face lots of risks
- 8A: “Within the household” – how individual/family manages
- 8B: “Relations with other actors” – Terms of service, insurance, hire Geek Squad
- Users likely a big concern at 9A (government regulation of business), such as HIPAA, GLBA, and consumer protection

The 3x3 Matrix of Cells

- Distinctions are good but not perfect:
  - Public vs. private, and protecting a government agency much like protecting a corporation
  - Within and outside of the organization – gray areas, such as whether relations with a parent/affiliate are inside or outside of the organization
  - My hope – readers can generally agree which problems go in which of the 3x3 cells; if so, then a useful framework for categorizing

The Role of Protocols and Separation of Layers

- Tech friends comment that there is supposed to be a clear separation of layers of the stack; concern is that this doesn't exist at the non-code layers
  - For instance, users agree to TOS with vendors (8B) but subject to government rules (9A or 9B)
  - In response, can usefully analyze the TOS, and can also usefully analyze the quality of the legal rule
- Protocols are supposed to be well designed to bind sender and receiver; in international affairs and other settings, no similar clear protocol
  - I think I agree; note the lack of code-based rigor, but the framework still useful

Potential for the Cyber Curriculum

- Helps describe what topics are done in which course:
  - Mostly international relations and cyber norms, and course covers 10A, 10B, and 10C, with some layer 9
  - Mostly corporate governance for CISOs, lots of 8A and 8B, with a little bit of the others
  - An overall curriculum could determine how full the coverage is of the 3x3 matrix
- Can also shift from a project course, reacting to new developments to a lecture course:
  - Module on each cell of the 3x3 matrix, with typical governance and vulnerability issues for each cell
  - For instance, 9A and compare market approaches to HIPAA or GLBA; if govern badly, then sensitive data is breached

Contributions of the 10-layer stack

- **Parsimonious structure** to organize the numerous issues now crowding into cyber law, policy, and business courses
  - I have covered every issue in my cyber course in 3 charts
  - For students and teachers, a way to keep the many issues straight
- **Attacks can happen at layers 8, 9, and 10**, if the company has bad policies, the nation has bad laws, or the international community does not prevent attacks
- **Vulnerabilities** at layers 8, 9, and 10 thus **fundamentally similar** to vulnerabilities at layers 1 to 7
- **Next steps**:
  - **Complete the text** and diagrams for the 10 layers of the cyber-stack – I welcome your comments and suggestions
  - Apply the 10 layers to **privacy and other cyber-issues**

Globalization of Criminal Evidence

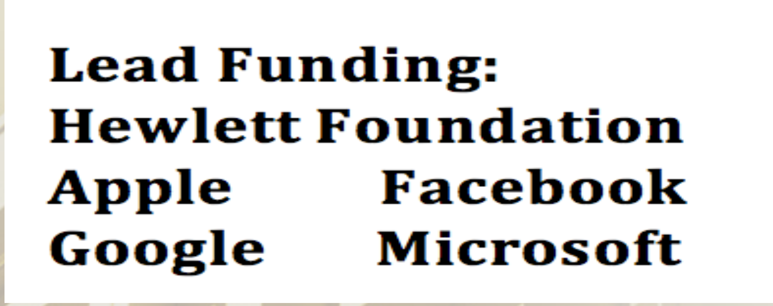
- Georgia Tech/IISP Project on Cross-Border Access to Data
- http://www.iisp.gatech.edu/cross-border-data-project

Cross-border Criminal Evidence is becoming the new normal

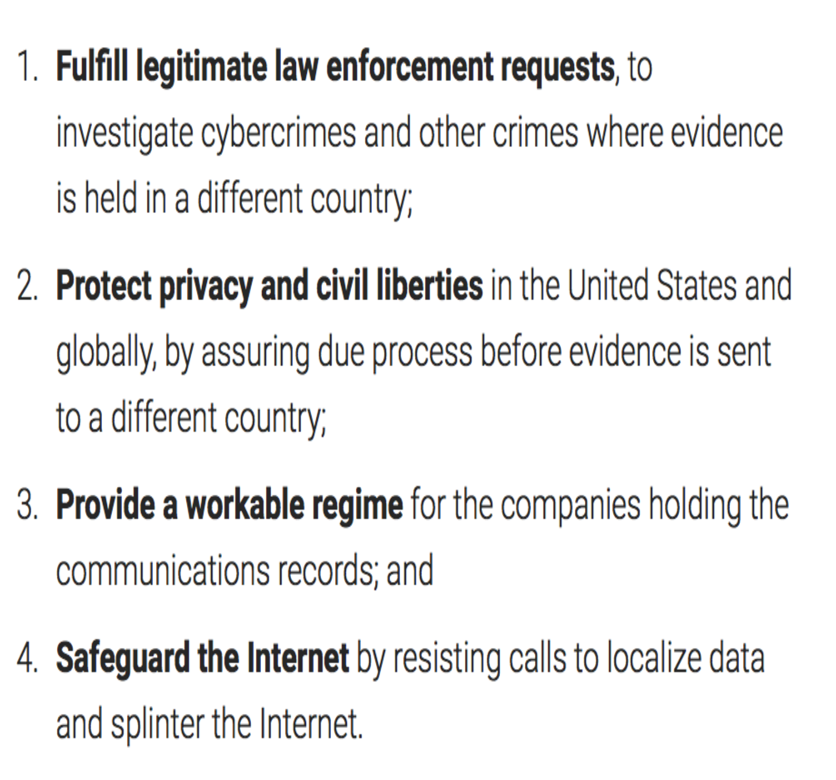
- In pre-cyber days, local crime and local evidence
- Globalization today – police can't get evidence locally, for data at rest and data in transit
- **Data at rest:**
  - Evidence of the hack often in servers and networks in a different country
  - Email, social network information, much more stored in the cloud
  - Cloud often in a different country – local legal process doesn't work
- **Data in transit:**
  - Police used to do wiretaps, locally
  - Today, wiretaps don't work due to encryption (HTTPS, etc.)
- **"Globalization of Criminal Evidence"** – huge pressure on cross-border cooperation

Cross-border requests for data project

Cross-Border Requests for Data Project

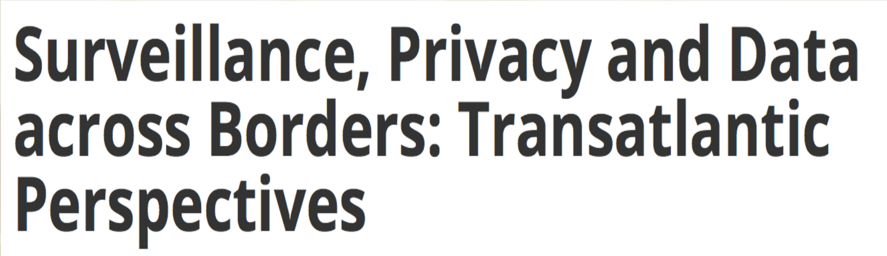


Lead Funding:
Hewlett Foundation
Apple Facebook
Google Microsoft

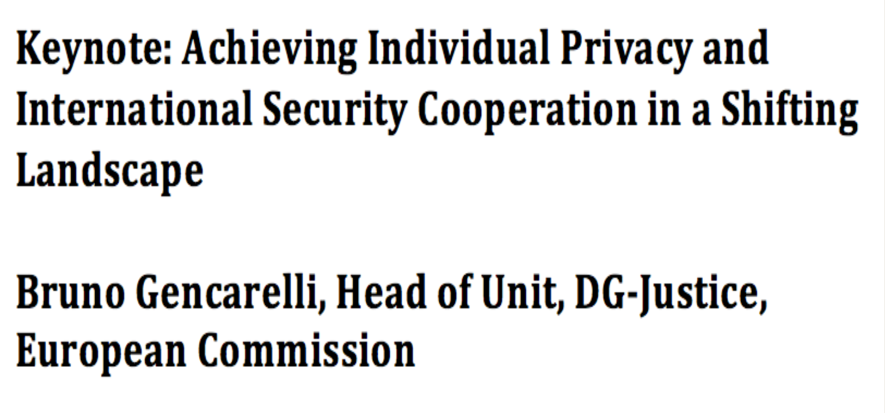


1. **Fulfill legitimate law enforcement requests**, to investigate cybercrimes and other crimes where evidence is held in a different country;
2. **Protect privacy and civil liberties** in the United States and globally, by assuring due process before evidence is sent to a different country;
3. **Provide 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.

GT conference April 2017

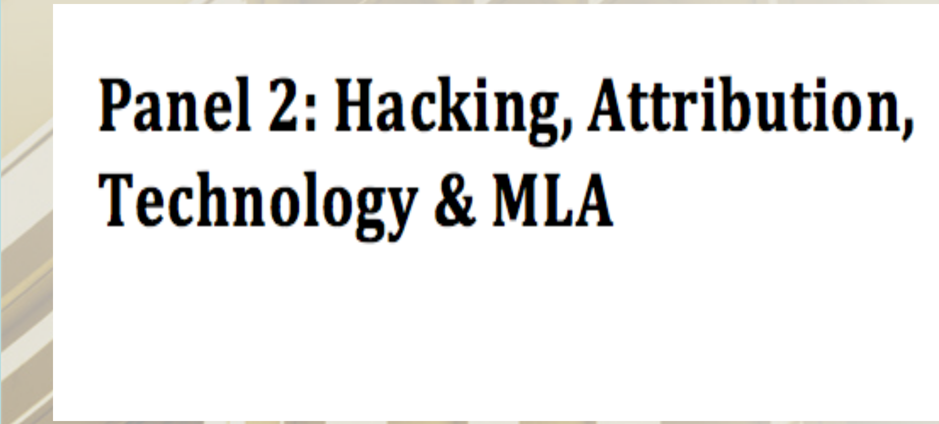


Surveillance, Privacy and Data across Borders: Transatlantic Perspectives

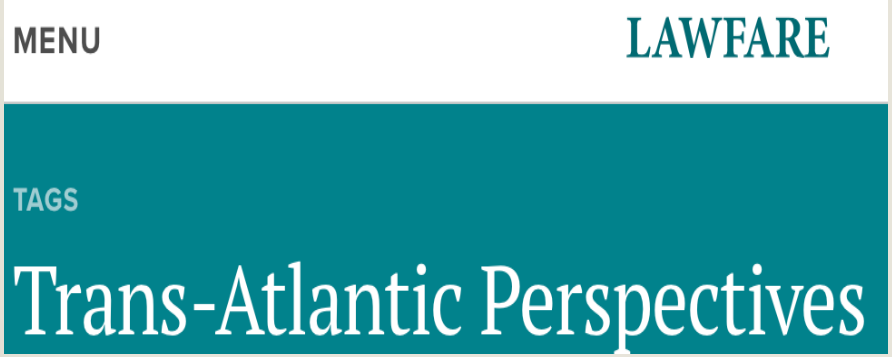


Keynote: Achieving Individual Privacy and International Security Cooperation in a Shifting Landscape

Bruno Gencarelli, Head of Unit, DG-Justice, European Commission



Panel 2: Hacking, Attribution, Technology & MLA



Trans-Atlantic Perspectives

Cross-border Cooperation Needs to change

- **The Goal**
  - Develop evidence of attribution
  - Cooperate to investigate and prosecute
- **Critiques of current system of Mutual Legal Assistance**
  - Slow – average 10 months or more
  - Designed for small sub-set of crimes, before globalization of criminal evidence

MLA Reform Issues

- **Improve the mechanics**
  - Online MLA portals/requests, standardize forms, more transparency, etc.
- **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
- **Research to map the protections of national legal systems**
  - GT papers on U.S. & France, to show differences yet similar overall protections
- **Law enforcement vs. intelligence vs. military sharing**
  - Attribution might happen in non law-enforcement settings; how to share that

What if we don’t improve cross-border cooperation?

- If we **don’t** improve MLA and attribution, then law enforcement will push harder for **other tools** to get the evidence
  - 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
  - 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)
  - 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

Conclusion

- We face the "**globalization of criminal evidence**"
  - That evidence is crucial to attribution and prosecution
  - Mutual legal assistance improves **the lawful structure for cross-border cooperation**
- If don't, then get more pressure for
  - Limits on strong encryption
  - Lawful government hacking
  - Data localization
- In conclusion, improving MLA is far more important today:
  - To help attribution
  - To fight cyberattacks and other crime
  - To preserve the global Internet