Policy

PROFESSIONAL EDUCATION

CSAIL
MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY

© 2015-2016 Massachusetts Institute of Technology

Foundations of Trustworthiness: The role of public policy in promoting secure networks

Daniel J. Weitzner

Principal Research Scientist. Director, MIT Cybersecurity and Internet Policy Research Initiative

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Massachusetts Institute of Technology

MIT PROFESSIONAL EDUCATION

CSAIL
MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY

© 2015-2016 Massachusetts Institute of Technology

Summary

- Inquiry into the role the public policy plays in sustaining and securing the Internet.
- Six key policy goals embodied in today's digital communications environment, how they arose and what keeps them on track.
- Regulation of cybersecurity in its infancy. Progress requires that policymakers need to understand the background against which new rules are made.

© 2015-2016 Massachusetts Institute of Technology

Overview- Policy Goals

1. Network transport - globally connected, available and reliable
2. Open Internet platforms - foundations on which everything is built.
3. Communications security - integrity and confidentiality of bits moving across networks
4. Application-level security – protecting information in specific sectors such as health, financial services, etc.
5. Commercial Privacy - defending a variety of values that we wrap up into one bundle called ‘privacy’
6. Global policy interoperability - sufficient convergence of legal frameworks to avoid balkanization

© 2015-2016 Massachusetts Institute of Technology

1. Network transport- globally connected, available and reliable

Technical design goal: interoperability, reliability

	Legal Authority	US Organizations	International Organizations	Global/Voluntary
Radio/TV	Spectrum licenses	FCC	International Telecommunications Union	
Telecommunications & Cable TV	Network operating certifications and regulations	FCC	United Nations/ITU	
Internet	n/a	n/a	n/a	Internet Engineering Task Force (IETF) World Wide Web Consortium (W3C)

© 2015-2016 Massachusetts Institute of Technology

Network transport- globally connected, available and reliable

Administrative arrangements – naming & numbering

	Legal Authority	US Organizations	International Organizations	Global/Voluntary
Radio/TV	channel assignment	FCC	International Telecommunications Union	
Telecommunications & Cable TV	North American Numbering Plan	FCC	United Nations/ITU	
Internet	US Commerce Department agreement on Domain Name System Operation	ICANN	TBD	TBD

© 2015-2016 Massachusetts Institute of Technology

Network transport- globally, connected, available and reliable

Key differences in seeking trustworthiness:

- *traditional*:
  - national regulatory control (often over monopoly providers)
  - flows up to international treaty authority
- *Internet:*
  - voluntary standards with no legal basis have global reach
  - lightweight regulation (FCC Net Neutrality) of small segment of market

New policy approaches to cybersecurity will want to learn from these different approaches.

© 2015-2016 Massachusetts Institute of Technology

2. Open Internet platforms - foundations on which everything else is built

Platforms:

- ISP (Verizon, Comcast)
- Hosting providers (Rackspace)
- Cloud services (Amazon AWS)
- Search Engines
- Social Networks (Twitter, Facebook)
- File Sharing (YouTube, Bittorrent)
- Applications (Google Apps)
- Marketplaces (Amazon, eBay)

Important of platforms:

- Commerce
- Speech
- Innovation
- Productivity

© 2015-2016 Massachusetts Institute of Technology

Open Internet platforms - foundations on which everything else is built

Liability Limitations with special responsibilities

- 47 USC 230: “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”
- Digital Millennium Copyright Act: Notice and Takedown
- European Union ECommerce Directive:
- OECD Internet Policymaking Principles

© 2015-2016 Massachusetts Institute of Technology

3. Communications privacy - integrity and confidentiality of networks traffic

Communications Privacy:

- intrusion resistant - with punishments for violations
  - ECPA and other laws against unauthorized surveillance by both state/citizens
    - big exceptions - employers, network operators
  - Computer Fraud and Abuse Act
- Footnote about property -- those who own the network don't necessarily own/control everything on it.

© 2015-2016 Massachusetts Institute of Technology

Communications privacy - integrity and confidentiality of network traffic

Delicate balance of state surveillance and trustworthiness

- Limited/accountable state surveillance
- Excess vulnerability to state surveillance can reduce trust:
  - China/Huawei
  - NSA-Snowden

© 2015-2016 Massachusetts Institute of Technology

4. Application-level security – protecting information in health, financial services, etc.

Alternative approaches to security

- Financial services networks:
  - Reg Z - pro-consumer liability limits $50.
  - PCI standards with contractual penalties [Target]
  - Outcome-oriented policy
- Health: HIPAA
  - risk assessment process, institutional procedures, documentation, audits
  - process-based
- Commercial banking: banking regulators, private contract and heavy self-insurance
- State Data Breach Notification Laws
  - Goal – enforce transparency to encourage better security practices
  - 47 states with varying thresholds

© 2015-2016 Massachusetts Institute of Technology

5. Commercial Privacy: a variety of values wrapped up in one bundle called 'privacy'

Does privacy mean the right be to alone?

"The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness….They conferred, as against the government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men."

OLMSTEAD v. U.S., 277 U.S. 438 (1928)(Brandeis dissenting)

© 2015-2016 Massachusetts Institute of Technology

Or, working together?

This Court has recognized the vital relationship between freedom to associate and privacy in one's associations…. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.

NAACP v. Patterson - 357 U.S. 449 (1958)

© 2015-2016 Massachusetts Institute of Technology

US Federal Privacy Laws

- Americans with Disabilities Act (ADA) - Primer for business.
- Cable Communications Policy Act of 1984 (Cable Act)
- California Senate Bill 1386 (SB 1386) - Chaptered version.
- Children's Internet Protection Act of 2001 (CIPA)
- Children's Online Privacy Protection Act of 1998 (COPPA)
- Communications Assistance for Law Enforcement Act of 1994 (CALEA)
- Computer Fraud and Abuse Act of 1986 (CFAA)
- Consumer Credit Reporting Reform Act of 1996 (CCRRA)
- Electronic Funds Transfer Act (EFTA)
- Fair and Accurate Credit Transactions Act (FACTA) of 2003
- Fair Credit Reporting Act (Full Text).
- Federal Information Security Management Act (FISMA)
- Federal Trade Commission Act (FTCA)
- Driver's Privacy Protection Act of 1994
- Electronic Communications Privacy Act of 1986 (ECPA)
- Electronic Freedom of Information Act of 1996 (E-FOIA) DFair Credit Reporting Act of 1999 (FCRA)
- Family Education Rights and Privacy Act of 1974 (FERPA)
- Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA)
- Privacy Act of 1974
- Privacy Protection Act of 1980 (PPA)
- Right to Financial Privacy Act of 1978 (RFPA)
- Telecommunications Act of 1996
- Telephone Consumer Protection Act of 1991 (TCPA) -
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)
- Video Privacy Protection Act of 1988 discussion and overview. Text of law at: Cornell Law Library.

© 2015-2016 Massachusetts Institute of Technology

Internet arrives: US and Europe diverge

United States – privacy on the ground

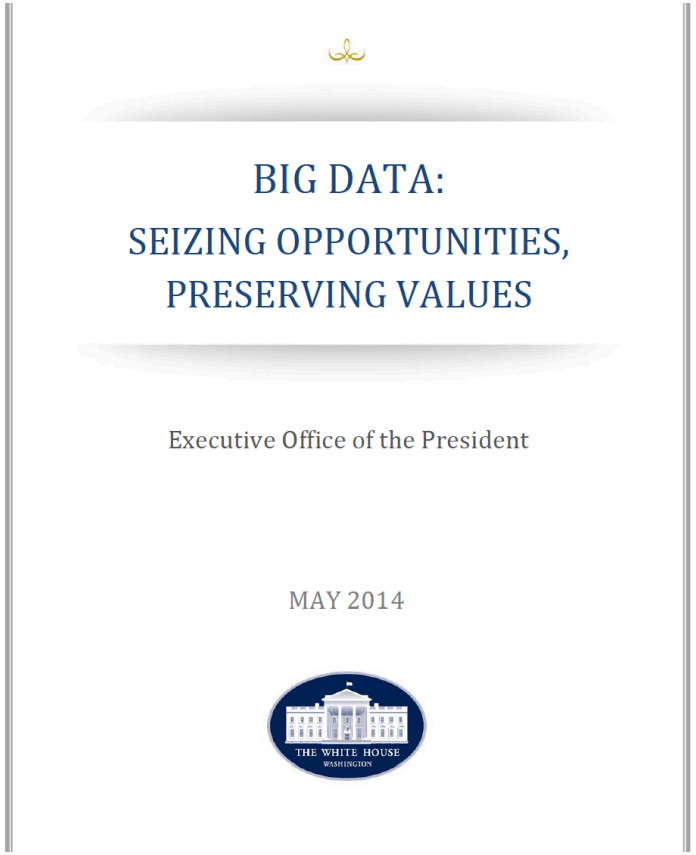
- FTC and White House ‘bully pulpit’
  - Privacy policies
  - FTC enforcement through ‘unfair and deceptive practices’ (FTC Act §5)
- Little legislation
  - Kids privacy
- Lots of enforcement
- Bottom up approach with teeth
  - Consumer Privacy Bill of Rights
  - Increased FTC enforcement

European Union – privacy on the books

- Omnibus law: European Data Protection Directive
- Growth of EU member-state Data Protection Authorities
- ‘Adequacy principle’: Viral propagation of data protection rules around the globe
- Treaty of Lisbon – Privacy as a fundamental right

© 2015-2016 Massachusetts Institute of Technology

New Privacy Challenges: Prevent Discrimination and Sustain Trust



Discrimination: "The increasing use of algorithms to make eligibility decisions must be carefully monitored for potential discriminatory outcomes for disadvantaged groups, even absent discriminatory intent."

Trust: "Public trust is required for the proper functioning of government….

As President Obama has unequivocally stated, "It is not enough for leaders to say: trust us, we won't abuse the data we collect." (p 10)

© 2015-2016 Massachusetts Institute of Technology

6. Global policy interoperability - sufficient convergence of legal frameworks to avoid balkanization

Freedom	Accountability
Innovation	Reliability
Evolving norms	Fundamental rights

© 2015-2016 Massachusetts Institute of Technology

THANK YOU

Daniel J. Weitzner

Principal Research Scientist

Director, MIT Cybersecurity and Internet Policy Research Initiative

© 2015-2016 Massachusetts Institute of Technology