OPEN ACCESS, PRIVACY AND HACKER CULTURE

An Inside Higher Ed webinar with

Tracy Mitrano

Director of IT policy and
the Institute for Internet Culture Policy and Law
at Cornell University

October 2, 2013

INSIDE HIGHER ED

Internet

World-Historical Phenomenon

The introduction of the Internet represents the tipping point for economic, social, political, cultural and ideological transformation.

Global Information Economy

INSIDE HIGHER ED

Lessig Lesson on the Internet

Dynamic interaction among four principal factors:

Technology

Law

Market

Social Norms

INSIDE HIGHER ED

Technology v. Law

Consequently, when we talk about a gap between the law and technology, this phrase is often short-hand for complex, dynamic tensions among, at least, these four factors.

Technology (Social Norms and the Market)

v.

The Law

INSIDE HIGHER ED

Three Key Laws

- Copyright Act of 1976
  - Amended by:
    - Copyright Extension Act of 1998
    - Digital Millennium Copyright Act of 1998
    - TEACH Act of 2001
- Computer Fraud and Abuse Act of 1986
- Electronic Communications Privacy Act of 1986

INSIDE HIGHER ED

Copyright

- Definition: holder has rights to copy, distribute, display and perform …
- Scope: original work in a tangible medium
- Terms:
  - Individual: 70 years + life, corporation 95 years
- Damages
  - Span from least impactful at $750 to $250,000 per infringement

- My Opinion: include in discussion of hacking because copyright issues set the tone for mass violation of the laws given Internet technologies. Since U.S. has not resolved that matter, this precedent opens the door to violations in other areas, [illegible] network security and electronic surveillance, on the pa[illegible] government and its peoples.

INSIDE HIGHER ED

Cases, Laws and Market Adjustments

- Duke student sentenced to jail time for massive infringement
- Capital v. Thomas, damages for file sharing
- BU student damages for file sharing
- Higher Education Opportunity Act file share provisions
  - “Solutions” outdated before regulations went into effect
- iTunes and Netflix
- Malefactors on the right and left
  - “pox on both houses”
- Gap between the technology and behavior remain unresolved in the law

INSIDE HIGHER ED

Copyright Reform

1. Limit Scope
2. Limit Terms
3. Re-imagine Registration
4. Differentiate between personal and profitable infringement in damages
5. Create Orphan Works
6. Codify transformative into fair use exceptions
7. End I.S.P. discrimination
8. Add substantive law to DMCA for content owners
9. Expand licensing for users
10. Recognize distinctions between developed and developing countries in copyright treaties

Computer Fraud and Abuse

- Definition: no electronically breaking into “protected computers”
  - i.e. don’t hack a computer connected to a networked system
- Purpose
  - Provide criminal penalties for breaking into banking and financial transactions managed through networked systems
- Used for all forms of security violations of and on devices connected to the Internet

INSIDE HIGHER ED

Cases

- Robert Morris
- Bradley/Chelsea Manning
- Aaron Schwartz
- (Probably) Edward Snowden

INSIDE HIGHER ED

Computer Fraud and Abuse Reform

- Distinguish financial fraud from security incidents
- Identify the type and degree of security violation
- Map punishment to the nature of the crime
  - Intent
  - Purpose
  - Effect
- Create explicit exceptions for innovation and research

INSIDE HIGHER ED

Electronic Communications Privacy Act

- *Olmstead* 1928
  - No 4th Amendment for telephone
- *Katz* 1967
  - 4th Amendment for telephone
- Omnibus Safe Streets and Crime Control Act 1968
  - Applying Katz, makes a distinction between metadata and content for telephony
- Electronic Communications Privacy Act 1986
  - Adds “data networking” i.e. Internet, but does not distinguish between the technology per 4th A.

Houston, We Have a Problem!

If the central concept of this law is to map 4th Amendment jurisprudence to electronic communications, including the Internet, the current version of this law fails to meet that goal.

Telephony and Internet technologies have different "metadata," i.e. tracking information. The use of Internet Protocol addresses, which sometimes link to web pages, can offer content for less than probable cause, the legal standard.

INSIDE HIGHER ED

USA-Patriot Act of 2001, as amended

- Exacerbated this problem because it lowered even more the legal showing by which law enforcement could collect metadata: a letter filed with a clerk.
- True for both regular Title III, criminal courts, and for the FISA (Foreign Intelligence Surveillance Act) “secret” Court.
- Partially explains why section 215 of FISA is so controversial
  - Section 215 used to obtain “billing” records

INSIDE HIGHER ED

Snowden Disclosures

- Under these laws, is it illegal for the National Security Agency (NSA) to collect all telephone metadata?
  - Untested by the courts, but not on its face a clear violation given the “war on terrorism” that at least since World Trade Center and September 11 events involves domestic surveillance

INSIDE HIGHER ED

Snowden Disclosures

- Under these laws, including FISA, which is an *ex parte* proceeding, is it illegal for the NSA to request of Internet companies the content of postings and communications … the Prism Program?
  - "In sum, a significant purpose of the electronic surveillance must be to obtain intelligence in the United States on foreign powers (such as enemy agents or spies) or individuals connected to international terrorist groups. To use FISA, the government must show probable cause that the 'target of the surveillance is a foreign power or agent of a foreign power.'"

INSIDE HIGHER ED

What is an NSA letter?

“A national security letter (NSL) is a letter from a U.S. government agency demanding information related to national security. It is independent of legal courts and therefore is different from a subpoena. It is used mainly by the FBI, when investigating matters related to national security. [1] It is issued to a particular entity or organization to turn over records and data pertaining to individuals. By law, NSLs can request only non-content information, such as transactional records, phone numbers dialed or sender or recipient email addresses. They also contain a gag order, preventing the recipient of the letter from disclosing that the letter was ever issued.”

Electronic Surveillance Reform

- Revise the ECPA to map technology to the 4th Amendment
  - Especially important with Voice over IP!
- Revise FISA for same jurisprudence
  - The standard by which it is triggered for NSA letters
    - “reasonable suspicion” “significant persons”
  - Network effect among correspondents
    - How many degrees of separation?

- My Opinion: Revoke FISA and end secret court regime!
  - What needs to be secret can be done in regular Title III courts
  - Secret Courts are inconsistent with democratic republic, even if that policy is an “empire”
    - Or we have to address the question of deciding what we kind of society we want to be

INSIDE HIGHER ED

Questions about Electronic Surveillance Reform

- Will revision of the foundational legislation (ECPA, FISA), plus legal “privacy” specialists’ oversight (Obama proposal) balance out the immunity provided to communications companies?
- What about technological oversight?
- Are “secret,” *ex parte* courts commensurate with a democratic polity?

INSIDE HIGHER ED

Challenging Questions …

- How do all of these challenges affect higher education?
  - Copyright
    - File-sharing and the HEOA
    - Section 1200 anti-circumvention and research
    - As producers and consumers of copyright, can we lead reform?
  - Computer Fraud and Abuse
    - How do we protect and preserve research applications and data? Intellectual property? Institutional Information?
    - Persistent nation-state attacks? Hackers? Hacktivism?
      - The MIT Question
  - Electronic Surveillance
    - Privacy and autonomy required for free speech and open inquiry?
    - What role do colleges and universities, in pursuit of their missions and as a public good for U.S. if not global society have in addressing the question of what kind of society the United States wants to be, and how in a global information economy do we achieve that dream?