Open Access, Privacy and Hacker Culture

SCRLC

December 18, 2013

Tracy Mitrano
Internet

World-Historical Phenomenon

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

Global Information Economy
Lessig Lesson on the Internet

Dynamic interaction among four principal factors:

Technology
Law
Market
Social Norms
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 for our factors.

Technology (Social Norms and the Market) v. The Law
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
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
Cases and Market Adjustments

• Duke
• Thomas
• BU
• Settlement Letters
• HEOA
• iTunes and Netflix
• Disparity of the law remains the same
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 breaking electronically 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 form of security violations of and on devices connected to the Internet
Cases

• Robert Morris

• Bradley/Chelsea Manning

• Aaron Schwartz

• (Probably) Edward Snowden
Computer Fraud and Abuse Reform

- Distinguish financial fraud from security incident
- 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
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 links to web pages, can offer content for less than probable cause, the legal standard.
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
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
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.’”
What is a 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?
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?
Finally ... 

How do all of these issues affect libraries?