Legal and Ethical Issues Facing Computer & Network Security Researchers

Aaron Burstein
UC Berkeley School of Information
November 23, 2009
Constraints on Network Research

• U.S. law is often unclear (and unfriendly).

• Ethical issues are novel, and the scientific context changes rapidly.
Overview

• Law
  – Electronic Communications Privacy Act (ECPA)
    • Collecting and sharing network packet traces
    • Running infected hosts
  – Computer Fraud & Abuse Act (CFAA)
  – Copyright / Digital Millennium Copyright Act (DMCA)

• Ethics
  – Basic principles
  – Human Subjects Research & Institutional review boards (IRBs)
COMMUNICATIONS PRIVACY LAW
Network Research: Privacy Law Issues

• Common research activities:
  – Collecting network measurement data
    • Packet headers
    • Payload
  – Publishing network traces
  – Collecting mobile device traces
    • E.g., Location data
## ECPA at a Glance

<table>
<thead>
<tr>
<th></th>
<th>Content</th>
<th>Non-content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time</td>
<td>Wiretap Act</td>
<td>Pen/Trap</td>
</tr>
<tr>
<td>Stored</td>
<td>Stored Communications Act</td>
<td></td>
</tr>
</tbody>
</table>
Electronic Communications Privacy Act (ECPA)

  - Prohibits real-time interception of communications contents
- Stored Communications Act (18 U.S.C. § 2701-110)
  - Prohibits certain disclosures of content and noncontent/addressing information
- Pen/Trap statute (18 U.S.C. § 3121-27)
  - Prohibits real-time interception of noncontent/addressing information
## Disclosure vs. Internal Use

<table>
<thead>
<tr>
<th></th>
<th>Voluntary disclosure OK?</th>
<th>Internal use OK?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time, contents</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Stored contents</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Real-time, non-content</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Stored, non-content</td>
<td>Yes (to non-govt recipient)</td>
<td>Yes</td>
</tr>
</tbody>
</table>
No Research Exemptions in ECPA!

• Some trace collection permitted by:
  – **Consent** of users or
  – “**Provider**” exception (allowing network operators to monitor networks to defend them)

• Limitations
  – Individual consent hard to get
  – Blanket consent (e.g., as part of a network’s terms of service) may provide little information about data collection, use
  – Provider exception requires collaboration with operational IT staff
Other Privacy Issues

• State laws
  – “Two-party” rule in state wiretap laws

• International laws
  – EU member nations generally have stricter privacy laws

• Interaction with human subjects regulations
How ECPA Affects Cybersecurity Research (1)

• **Activity:** Collecting full-packet traces in real-time
  – Relevant law: Wiretap Act
  – Applies to *any* network (government, enterprise, WiFi, university, etc.)
  – Need consent or sufficient link to operational network protection for provider exception
  – Wiretap Act continues to cover traces after they are recorded ➔ If collection violates law, disclosure probably does too.
How ECPA Affects Cybersecurity Research (2)

- Activity: Collecting packet-header traces in real-time
  - Relevant law: Pen/Trap statute
  - Consent, provider exceptions available
  - Also an exception for network “operation, maintenance, and testing”
  - Legally stored data become subject to SCA
How ECPA Affects Cybersecurity Research (3)

- **Activity:** Sharing or publishing packet traces
  - **Relevant law:** SCA
    - Applies only to “public” service providers: commercial ISPs but not businesses
  - **Full-packet traces:** disclosure prohibited without consent, subpoena
  - **Packet header traces:** disclosure allowed unless given to “governmental entity”
    - Much broader than law enforcement; hampers some public releases
COMPUTER FRAUD & ABUSE ACT (CFAA)
CFAA & Network Research

• Botnet infiltration (and response?)
• Running malicious code in testbeds
• Collecting data from online services
• Running honeynets to interact with attackers
CFAA Elements

• “Protected computer”
  – Any computer connected to the Internet
• “Access”
  – Not defined in statute
• “Authorization”
  – Not defined in statute
• “Obtaining information” / causing “loss”
  – Penalties scale with type, value of information obtained
  – “Loss” is not defined
Is the CFAA as Broad as It Sounds?

• Perhaps . . .

• United States v. Lori Drew (2009)
  – “Access” means “to obtain information from”
  – “Authorization” may be set by Terms of Service
  – But U.S. Const. limits criminal application of CFAA in TOS breach cases.
    • Insufficient clarity + arbitrary enforcement = unconstitutional vagueness
Testbeds: Legal Issues

• Concern: What if worms, viruses escape testbed containment?

• CFAA prohibits (1) knowingly causing transmission of code and (2) intentionally or recklessly causing damage
  • Unclear whether accidents meet this standard of intent
ETHICAL ISSUES
Overview

1. Basic ethical principles / theories

2. Human subjects research and ethical “compliance”
Ethical Frameworks

• Consequentialism
  – The moral rightness of an act depends only on its consequences.

• Deontological theories
  – Morality is prescribed by individual rights, duties.
Research Ethics

- “Belmont Report” crafted principles for human subjects research (HSR)
  - Respect for persons
  - Beneficence
  - Justice
- “Common Rule” codifies Belmont principles
  - Defines “research,” “human subject,” “consent,” “institutional review board” (IRB)
  - Applies to any HSR at an organization receiving federal research funding
Navigating Human Subjects Review

Copyright 2009 Aaron Burstein. Some rights reserved: http://creativecommons.org/licenses/by-nc-nd/3.0/us/.
Chart 1: Is an Activity Research Involving Human Subjects Covered by 45 CFR part 46?

Start here.

Is the activity a **systematic** investigation designed to develop or contribute to **generalizable** knowledge? [45 CFR 46.102(d)]

- **NO** Activity is not research, so 45 CFR part 46 does not apply.
- **YES** Activity is research. Does the research involve **obtaining** information about living **individuals**? [45 CFR 46.102(f)]

- **NO**
  - The research is not research involving human subjects, and 45 CFR part 46 does not apply.
  - Is the information **individually identifiable** (i.e., the identity of the subject is or may readily be ascertained by the investigator or associated with the information)? [45 CFR 46.102(f)(2)]
  - **NO**
    - **BUT**
    - **YES**
      - Go to Chart 2

- **YES**
  - Activity is research involving human subjects. Is it **conducted or supported by HHS**? [45 CFR 46.101(a)(1)]
  - **YES**
    - Unless exempt under 45 CFR 46.101(b), 45 CFR part 46, subpart A requirements apply to the research. As appropriate, subpart B, C, and D requirements also apply.
  - **NO**
    - Is the research covered by an applicable OHRP approved assurance created under 45 CFR 46.103?
      - **YES**
        - Go to Chart 2
      - **NO**
        - Other Federal, State and local laws and/or regulations may apply to the activity. [45 CFR 46.101(f)]

September 24, 2004

Copyright 2009 Aaron Burstein. Some rights reserved: http://creativecommons.org/licenses/by-nc-nd/3.0/us/.
Ethical Trouble Spots for Network Research

• Is it HSR?
• Waiver of Informed Consent
  – May be waived if “impracticable” to obtain
• Deception
  – Minimal risk
  – No adverse effect on subjects’ rights, welfare
  – Non-deceptive research design impracticable
IRB Review: Easing the Pain

• Exemptions
  – Studies of existing, publicly available data
  – Studies of data recorded so that “subjects cannot be identified, directly” or through IDs
  – Note: IRB decides whether research is exempt.

• Expedited review
  – Research involves “no more than minimal risk”
  – Allows quick(er) protocol approval
Ethics Beyond HSR Issues

• Harm to the researcher’s organization (e.g., university)
• Harm to other users
• Accelerating the arms race
• Confusing researchers’ roles
  – When to report malicious activity to . . .
    • Victims?
    • Law enforcement?
Law & Ethics in Research Frontiers

• Studies of security-related behavior
  – Downloading malware
  – Checking binary signatures
  – Ignoring A/V warnings
  – “Conditioning” users to ignore security
• Infiltrating cybercrime organizations
• DMCA “take down” studies
• Active probes
Security Analysis of Software
Software Analysis: Legal Issues

• Issues
  – Finding software vulnerabilities
  – Publishing results

• Relevant laws:
  – Contract law (EULAs, clickwrap/shrinkwrap licenses)
  – Digital Millennium Copyright Act (DMCA)
Software Analysis: Contract Issues

• EULAs typically prohibit reverse engineering, other processes that reveal vulnerabilities
• Courts usually enforce them . . .
• . . . but important issues remain unsettled:
  – Pre-emption by patent law
  – Tension with First Amendment
Software Analysis: DMCA Issues

• “No person shall circumvent a technological measure that effectively controls access to a work protected” by the Copyright Act

• But: courts, U.S. DOJ have found that the DMCA does not prohibit conducting research on or publishing papers about software vulnerabilities.

• Caveats:
  – Publishing actual circumvention software might violate DMCA.
  – Restrictions in EULAs still apply.
Ethical Issues in Software Analysis

• Whether (and when) to notify software vendor

• How much detail to publish
Resources

• Legal Information Institute (http://www.law.cornell.edu/)
  – Open access to US Constitution, US Code
• Common Rule
• Samuelson Clinic at UC Berkeley School of Law (http://www.samulesonclinic.org/)
• Reforming the ECPA to Enable a Culture of Cybersecurity Research (http://jolt.law.harvard.edu/)
  – In-depth analysis of applicable privacy laws and proposal for a research exception to the ECPA