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

	Content	Non-content
Real-time	Wiretap Act	Pen/Trap
Stored	Stored Communications Act	

Electronic Communications Privacy Act (ECPA)

- Wiretap Act (18 U.S.C. § 2510-22)
  - 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

	Voluntary disclosure OK?	Internal use OK?
Real-time, contents	No	No
Stored contents	No	Yes
Real-time, non-content	No	Yes
Stored, non-content	Yes (to non-govt recipient)	Yes

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

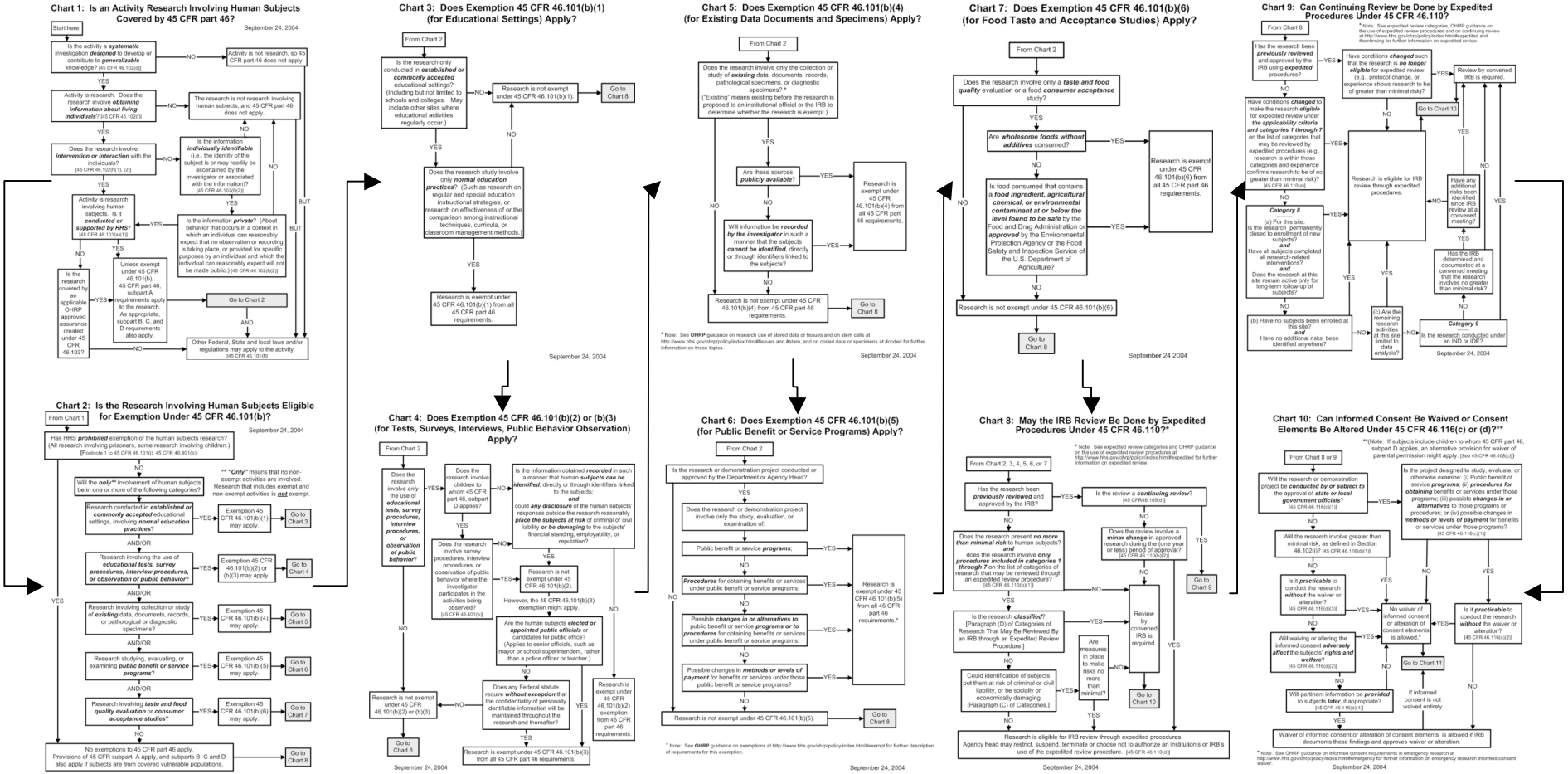
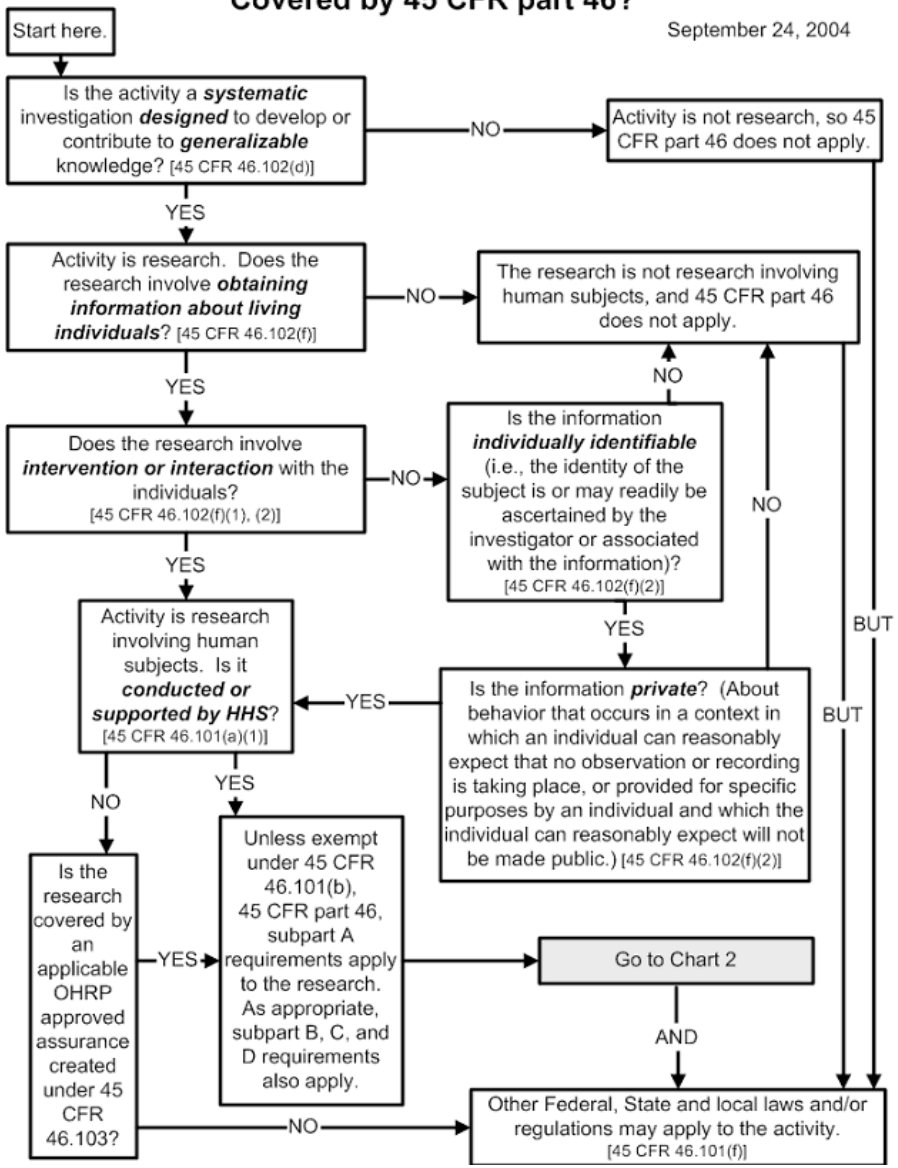


Chart 1: Is an Activity Research Involving Human Subjects Covered by 45 CFR part 46?



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
  - Go to http://ecfr.gpoaccess.gov/, select title 45, part 46.
- 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