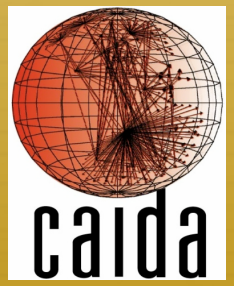
Workshop on Ethics in Computer Security Research (WECSR)
Tenerife, Canary Islands, Spain
28 January 2010

Framework for Understanding and Applying Ethical Principles in Network and Security Research

- Erin Kenneally, M.F.S., J.D.
  University of California San Diego, CAIDA
- Michael Bailey, Ph.D, University of Michigan
- Douglas Maughan, Ph.D., U.S. Dept. of Homeland Security



Overview

- Motivations
- The Belmont Report
  - Respect for Persons
  - Beneficence
  - Justice
- Professional Ethical Codes
- Ethical Impact Assessment (EIA) Framework: Applying Traditional Principles to ICT Research
- Up Next

Motivations

- Rapid changes in effects of enabling technologies on human welfare
- Novel ethical challenges arise in gap between expectations and capabilities
- ICT research catalyst: computer & network research for cyber security R&D
  - lack of practical, reproducible scientific results via gap between ops and research
  - DHS PREDICT effort
  - But, sharing challenges
    - Network traffic privacy and confidentiality
    - Legal gray areas in collecting, disclosing data for research
- Botnets, Vulnerability disclosure, Antiphishing studies, oh my!
- Ops abuses : ⇧ barrier to entry & BOP

Launch Pad: Belmont Report & '202' Report

= Ethical Principles and Guidelines for Research Involving Human Subjects

Authority: National Research Act 1974 → Nat'l Commission for the Protection of Human Subjects of Biomedical & Behavioral Research
-- ID basic ethical principles for human subjects research
-- Develop guidelines to assure compliance with principles

- **Belmont Drivers:**
  - Nuremburg Code- post WWII Nuremburg War Crime Trials standard
  - other codes: Helsinki Declaration 1964, US HEW Guidelines 1971 (codified 45 CFR 46)
- **Role of principles**: prescriptive basis for formulating, interpreting, critiquing the rules; purpose to provide framework to guide resolution of ethical problems.

- DHS Ethics Working Group to apply Belmont to ICTR = **202 Report**

Launch Pad: Professional Ethical Codes

- IEEE Code of Ethics (2006)
- ACM Code of Ethics and Professional conduct (1992)

- The Good: "do good" imperative for membership
- The Bad: limited domain- workplace and employment
- The Ugly: still a gap; how does "do good" apply to ICT human research & experimentation?

Lift-Off: Ethical Impact Assessment (EIA) Framework

- **What**: PIA analog; v.1 prototype
- **Why**:
  - 'unfunded mandates' are a disservice to all stakeholders
  - make ethics 'embraceable' lower costs and increase motivation for researchers (especially technical mindsets) to engage
- **How**: intellectual tool to apply abstract principles to practice

Applying Respect for Persons Principle

- **Applied:**
  - 1. individuals should be treated as autonomous agents
  - 2. persons with diminished autonomy entitled to protection
- **Applied in cyber security context:**
  - (**A**) should include both individuals and society, should consider organizations; realize tight coupling of humans w/ data and systems
  - Yeah, But → identity :: network artifacts disjointed; hard to ID potentially at-risk populations in network traces

EIA and Respect for Persons

- **Framing Questions:**
  - Can the network artifacts (IPA, URL) be reasonably linked to an identifiable human? (or, automated device or human-operated device level)
  - Does the data collected concern the 'substance, purport or meaning of a communication' from an identifiable person?
  - Does data reveal behavioral data that could link to identifiable person?

Applying Respect for Persons (mas)

- **Applied in cyber security context:**
  - **(B)** obtain consent to use data and info systems for specific research purposes
  - Yeah, But → in vivo research in cyber environment – size, scope, provenance, rights – introduce legal, strategic, economic factors

EIA and Respect for Persons (mas)

- **Framing Questions**:
  - If individuals are identifiable in network and security data, have they consented?
  - Can they decline participation in the research, or uses of collected data?
  - If the purpose of data use has changed, has renewed consent been obtained?
  - Is consent possible, or does it directly and substantially impede research goals? (ref Beneficence)

Applying Beneficence Principle

- **Applied**:
  - 1. Do not harm
  - 2. Minimize possible harms (& max benefits)
- **Applied in cyber security context**:
  - (**A**) researchers should systematically assess both risks and benefits of research on privacy, civil rights, well-being of persons
  - Yeah, But → RBA challenging with gaps, grayness of laws, professional codes, IRBs
  - **(B)** researchers should consider the full spectrum of risks of harms to persons and information systems (reputational, emotional, financial, physical)
  - Yeah, But → normative social immaturity re: harms (qualitative & quantitative)

EIA and Beneficence

- **Framing Questions:**
  - What are effects of research on all stakeholders: researchers, human subj, society?
  - What are possible unintended consequences? E.g., privacy harms
  - What is nature and source of collected data?
  - What is purpose of collecting data?
  - What is intended use of data?
  - Will research be disseminated to 3rd parties and used consistent with purpose?
  - What are the administrative and technical controls to enforce obligations?
  - What is risk of re-identification (law trigger, data quantity, threat perspective, time/effort required)
  - What categories of activity have strong reasons for involving HSR?

Applying Beneficence and EIA (yet mas)

- **Applied in cyber security context** (including Professional Codes)
  - (**C**) Research should not violate laws, operator agreements, K obligations, or other private arrangements
  - Yeah, But → legal due diligence hard, uncertain applications and interpretations of laws
- **Framing Questions**:
  - If the research conflicts with law/policy, is there an exception or valid agreement otherwise permitting?
  - If gov't involved, will there be int'l or bilateral diplomatic ramifications?
  - Should research methodology be modified or abandoned?
  - Have you engaged legal guidance?

Applying Beneficence Principle (mas)

- **Applied in cyber security context**:
  - **(D)** Design & conduct research to maximize probable benefits and minimize harms to persons and organizations
  - Yeah But → estimating scale at which risks and benefits can occur; ability to attribute research data and results to individuals; increasing availability of data

EIA and Beneficence (mas)

- **Framing Questions**:
  - Does research impact CIA of info systems (including originating and transiting)?
  - Does research design include controls to minimize harms (ie, using in vitro, anonymization or other disclosure controls)?
  - Are there exigent circumstances that should be factored into the evaluation of harm from research?
  - Will research result in no > harm than what would occur in its absence?
  - What checks and balances to prevent/repeat harms?
    - chill 1st A. rights to speak, associate, surf anonymously
    - target groups based on sex, religion, politics
    - Impair data quality & integrity
    - Surveillance harms – id theft, gov't persecution, alter behavior re: counter-surveillance
  - Could the research make the targeted problem (eg, infosec) worse, or undermine research goals?

Applying Beneficence and EIA (yet mas)

- **Applied in cyber security context**:
  - **(E)** If research causes risk or harm to a person, the person should be notified
    - If research reveals but does not cause unanticipated harm, strongly consider responsible disclosure (sponsor organization, IRB, LE)
  - Yeah, But → what about risk held in abeyance?
- **Framing Questions**:
  - When notification of persons is not possible or appropriate, can harm be mitigated by notifying other appropriate parties?
  - Is notification and response tailored to the causes and extent of risk exposure?

EIA – Applying Justice

- **Applied in cyber security context**:
  - (**A**) Benefits and burdens of research should be shared fairly between research target subjects and beneficiaries of research results
  - Yeah, But → selection of subjects is challenging in cyber context (e.g., attribution/provenance, projection)
- **Framing Questions**:
  - Does the research raise fairness and discrimination concerns?
  - Will the research undermine cooperation from the community whose participation is needed/targeted?
  - Is the research methodology and results transparent?

EIA – Applying Justice (mas)

- **Applied in cyber security context**
  - **(B)** selection of research subject should be equitable (with exceptions to balance benefits), and should adhered to internationally accepted best practices
  - Yeah, But → variance in nation-states' cyberlaws & rights

- **Framing Questions**:
  - To what extent does research violate legal and ethical principles of equality?
  - How should research design be altered to decrease inequality or mitigate its effects?
  - Is the standard against which research measured that of reasonable researcher, not strict liability?

Are We There Yet?

- **Must explicitly justify reasoning to all stakeholders if we claim low risk :: benefit of research**

- **V. 1** of EIA… will evolve in parallel and in concert with The 202 Report
  - Subsequent meetings 9/09, 11/09, 3/10, 6/10

EIA Tool Prototype

ICT Research Activity: _____

Ethics Assessment Considerations	Comments & Examples	Research Component			Benefits Considered	Controls	Risk Remarks
		Collection	Mgmt & Use	Disclosure/ Sharing			
ETHICAL PRINCIPLE: (A) Respect for Persons							
1. Relevant Parties- consider individuals and organizations, including computer systems and data	[insert bullet questions]						
2. Consent- obtain informed consent to collection, use or disclose data and systems; consent does not transfer for research purposes unless specifically obtained	[insert bullet questions]						
3.Compliance – engage due diligence for respecting laws, contracts, etc. to protect individuals and orgs	[insert bullet questions]						
ETHICAL PRINCIPLE: (B) Beneficence							
4. Harms- consider full spectrum of harms to persons and information systems	Legal, systems assurance, privacy, reputation, physical psychological, economic						
6. Maximize Benefits- design and conduct to maximize benefits and minimize harms	[insert bullet questions]						
7. Migration- notify appropriate parties if research causes harm, consider if harm is revealed	[insert bullet questions]						
	[insert bullet questions]						
ETHICAL PRINCIPLE: (C) Justice							
8. Fairness & Equity– benefits and burdens should be apportioned fairly	[insert bullet questions]						
9. Transparency	[insert bullet questions]						

Props

- Much grey matter feedback by the DHS Working Group on Ethics in ICTR
  - inaugural workshop May 26th-27th, 2009 in Washington, DC
- Estimated completion of working group and publication of authoritative guidance in Summer 2010.

….and Thank-You

erin@caida.org