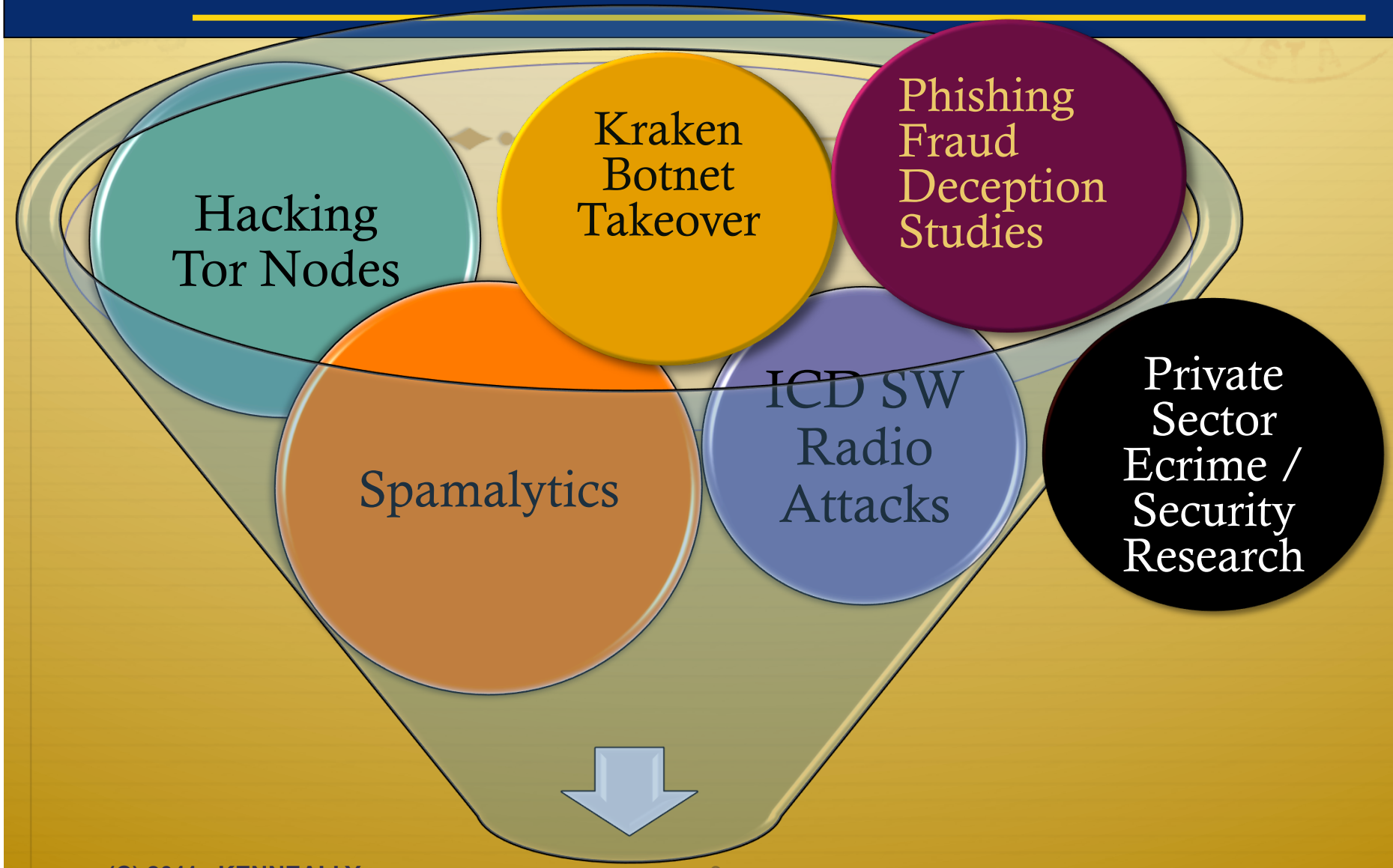
The Need for Community Standards for Ethical Behavior in E-Crime Research

Erin Kenneally, M.F.S., J.D.
Elchemy
Cooperative Association for Internet Data Analysis, UC San Diego

Overview

- Motivations & Context
- Problem Statement: Building a Community Ethics Ethos
- The Menlo Principles: Restatement of Belmont Principles in the ICTR Context
- Applying and Implementing Menlo Principles
  - Respect for Persons
  - Beneficence
  - Justice
  - Respect for Law and Public Interest
- Ethical Impact Assessment (EIA) Tool

Motivations



Ethics Guidelines

Context: Do the Right Thing

- Researchers **want to help**, to benefit the *internet community*
- …but oh, the **temptations**!

  First to publish; do something new; show how 31337 you are; fight for funding; ends justify the means
- …and the **conflicts**

  Affecting other research; impacting LE investigations; thwarting mitigation efforts; protecting rights; helping the bad guys; less risky (and less sexy) options?

THIS IS WHERE ETHICS COME IN…

Context: Existing Ethics Standards

- The IEEE, ACM, etc: **Codes of Ethics**
- **The Belmont Report**, the National Research Act, and Institutional Review Boards (IRB); Common Rule (45 CFR 46)
- **"Rules of Engagement"**
  - The Law of Armed Conflict; Active Response Continuum
- **Other Organizational Codes** (Universities, Corporations, etc.)

Context: Existing Ethics Standards

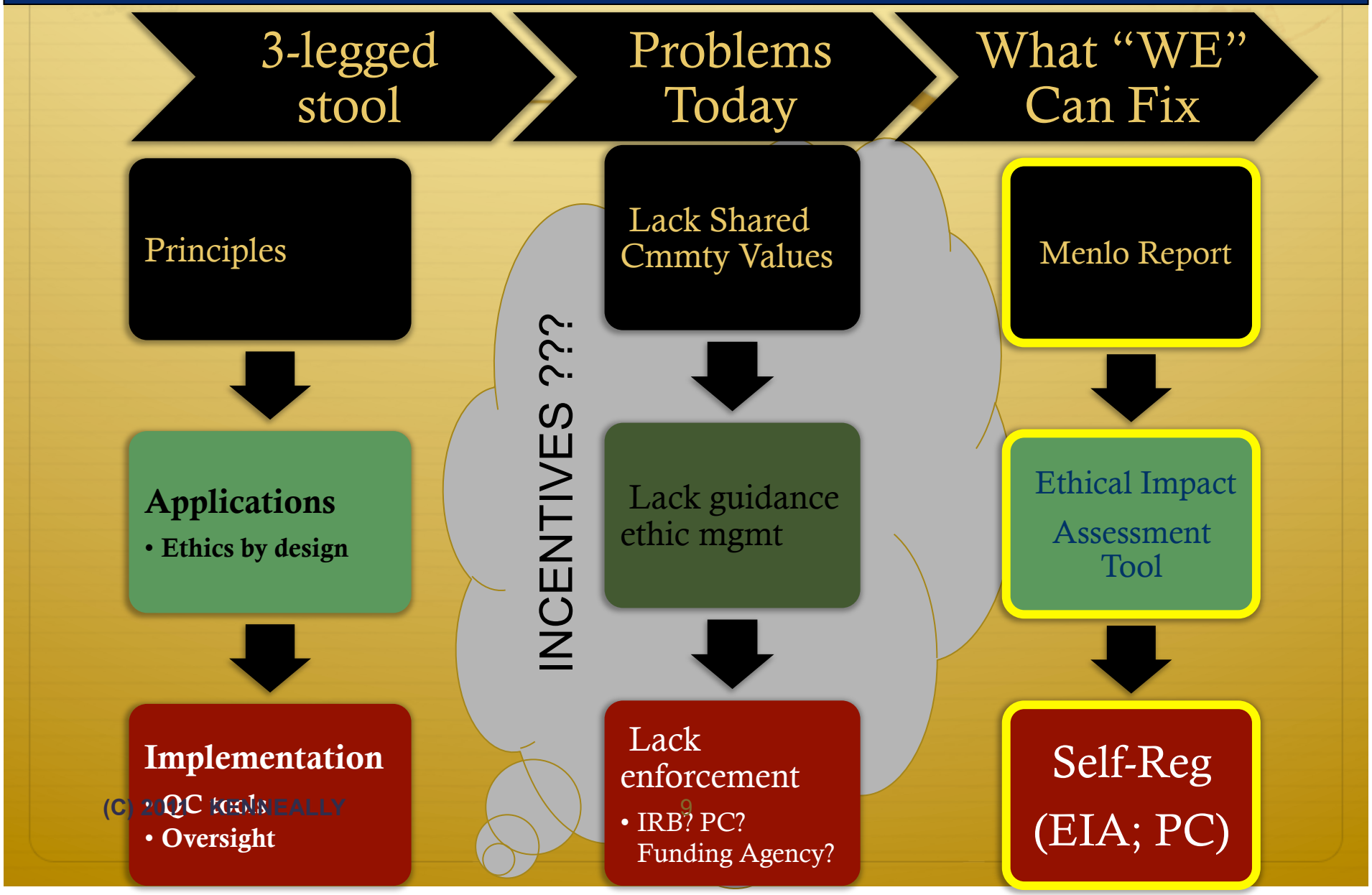
- *Ethical Principles and Guidelines for the Protection of Human Subjects of Research* US HEW 1979 (Belmont Report)
  - Set up: Institutional Review Board (IRB)- institutional assurance that for research involving human subjects, the rights and welfare of the subjects are protected.
  - **Respect for persons**
    - Individuals should be treated autonomously (stakeholders)
    - Informed consent
  - **Beneficence**
    - Do no harm
    - Maximize possible benefits/minimize risks
  - **Distributive Justice**
    - Equitable selection of research subjects

BUT…. El Problemo →

Motivation: Need for Principles in Context

- What does fundamental terms such as ***Human Subject*** mean in E-Crime Research?
  - What is a *research subject / living individual* in the context of large-scale, data-intensive research?
- How does a researcher obtain ***informed consent*** when interacting with thousands, millions of persons behind the machines/network traffic?

Problem: State of Affairs Today



What We Need: Build a Community Ethics Ethos

If we don't get our act together, someone will do it for us.

Key to Enabling E-Crime Research

- **"Ethically-Defensible Research"**
  - **Building decision making capabilities**
  - **Consistency**
  - **Self Governance**
- Reward Ethical Behavior

Self Governance: Menlo Report

- **DHS Working Group on Ethics in ICTR**
  - Inaugural workshop May 26th-27th, 2009 in Washington, DC
  - Lawyers, Computer Scientists, IRB Members, Ethicists
- Goal is to create an **updated Belmont** report for the field of ICTR
- Initial feedback on draft report out for comments next month
- Public forum for discussion at **IEEE Security and Privacy (Oakland): "*Community Workshop on Ethical Guidelines for Security Research*"**

  http://www.ieee-security.org/TC/SP2011/workshops.html

Self-Governance:
Ethical Impact Assessment (EIA) Framework

- **What:**
  - Help design and evaluate the ethical impact of research.
  - Within framework of lifecycle of research Collection, Use and Disclosure.
- **So What?:**
  - 'unfunded mandates' are a disservice to all stakeholders
  - make ethics 'embraceable' lower costs and increase motivation for researchers (especially technical mindsets) to engage
  - consistency

EIA and Respect For Persons

- ICT Researchers
- Human Subjects
  - Data Subject / End User
  - Network / Platform / Service Provider
  - Intermediary in Network
- Society
- Gov't / Law Enforcement
- Others

Stakeholder Assistive Questions

- Are the stakeholders who are potentially put at risk from research activities reasonably identifiable and potentially approachable in order to obtain informed consent?
- Can you identify the relationships between all of the stakeholders in terms of rights, responsibilities, and duties?
- If the research involves ICT itself, have you adequately considered the primary and secondary effects of impacts to the ICT on stakeholders?
- If the research involves data collection or use of previously collected data, is it easy to identify humans via IP addresses, URLs, content, or any other attributes of the data?
- Have you determined who owns, controls, or authorizes the collection, use and disclosure of the data?

EIA and Beneficence Principle

- **Applied**:
  - Do no harm
  - Minimize possible harms (& max benefits)
- **Applied in E-Crime context**:
  - 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
  - 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: Example Framing Questions

- **Confidentiality**.
  - What policies and practices assure confidentiality of information?
- **Anonymity**.
  - Is data attributable to human subjects de-identified/anonymized where reasonably possible?
- **Proportionality**.
  - Does the ICTR consider only collecting and maintaining personal data that are adequate, relevant and not excessive in relation to the research purposes for which they are collected and/or further processed?
- **Minimization**.
  - If ICTR involves human subjects surveillance, are minimization techniques and processes used (e.g., limited collection, purpose specification, limited data use, limited data retention, etc.)?

EIA and Beneficence: Example Framing Questions

- **Fairness.**
  - Does the ICTR promote fairness for human subjects by considering data quality, notice, individual participation, transparency and accountability?
- **Data Security.**
  - Is data secured, and how is it secured, against threats to privacy & data integrity (or, disclosure and use risks)?
- **Administrative and Technical Controls.**
  - Is the research design, methods and implementation vetted by by internal and/or external authorities (e.g., IRBs, sponsor agency, conference program committee, program managers)?

EIA: Stakeholders

Ethics Principles Considered	ICT Researchers	Human Subjects			Society	Gov't / Law Enforcement	Other
		Data Subject / End User	Network/ Platform/ Service Provider	Intermediary in Network			
1. Identification of Stakeholders - Identify relevant individuals and organizations who are involved in the propsed research activity, including computer systems and data	UCSD research team; other academic researchers analyzing the Storm botnet.	Users of computers infected with the Storm bot (worker machines).	*Nework provider for proxy hosts in botnet *Internet service providers (ISPs) of users with infected computers *Webmail platform provider *Registrar of fake phishing site	* Owners of networks where botnet Command and Control (C&C) servers are located; * the Overnet P2P network community.	Users whose computers are infected with the Storm bot.	Law Enforcement Agencies (LEAs) in multiple countries.	* Other non-academic, non-gov't actors involved in mitigation and research efforts related to the Storm botnet; * AV vendors?

EIA: Consent

Ethics Principles Considered	ICT Researchers	Human Subjects		
		Data Subject / End User	Network/ Platform/ Service Provider	Intermediary in Network
		Research Collection		
2. Consent- obtain informed consent to collect data; must be specifically obtained for each research purpose	n/a	* Worker machines- no consent to participate in Storm botnet, but researchers' proxy not responsible for initiating contact with and inserting spam workloads (spam templates, email delivery list, URL dictionaries) into worker or user machine; Obtaining informed consent would negate entire purpose of research * Question: informed consent of users visiting phished site due to deception?	• Network provider for proxy collectors informed and consented • Webmail platform provider informed and consented • Registrar informed and consented	• Proxy hosts (in botnet) owned by researchers • Fake pharma and ecard sites owned by researchers

EIA: Compliance

Ethics Principles Considered	ICT Researchers	Human Subjects			Society
		Data Subject / End User	Network/ Platform/ Service Provider	Intermediary in Network	
3.Compliance – engage due diligence for respecting laws, contracts, etc. to protect individuals and orgs	• No violation of CFAA, ECPA, IP laws, private agreements • IRB approval?	* no CFAA claims (no unauthorized access, damages); no ECPA (no interception of traffic, party to communication, questionable though if two-party consent needed);	• No agreement/K associated nodes in Storm network; no circumvent mediating device; adherence to Overnet protocols and resources • No unauthorized access to webmail platform • Unlikely violate ToS prohibiting sending of spam, since webmail accounts received spam responses to redirected target hosts	* authorization to log (capture, manage, store) traffic to own website; no protocol manipulation of received traffic	(see other stakeholders)

EIA: Harms

Ethics Principles Considered	ICT Researchers	Human Subjects			Society
		Data Subject / End User	Network/ Platform/ Service Provider	Intermediary in Network	
4. Harms- consider full spectrum of harms to persons and information systems (systems assurance, privacy, reputation, physical, psychological, economic)	* none	• Researchers actions (CC rewriting, interposing Spam delivery, interposing user click-thru) did not diminish the performance or usability of the worker machines. • No recruitment of new worker bots; * no privacy harm- researchers did not collect, store or transmit any sensitive personal information from worker systems, or via mimicked sites	Network and webmail providers: Researchers actions (CC rewriting, interpose Spam delivery, interpose user click-thru) did not diminish the performance or usability, create resource pressures, cause corrective action effort or compromise their systems, services or network.	* Researcher actions (CC rewriting, Interpose Spam delivery, Interpose user click-thru) did not tamper with new or existing machines in the network beyond researcher-owned proxy hosts	• Potential chilling effects involved in knowing a third party redirecting observing activity, * de minimis compared to chilling effects from knowing they are unwitting participants in malicious, C&C controlled botnet

EIA: Benefits

Ethics Principles Considered	ICT Researchers	Human Subjects			Society
		Data Subject / End User	Network/ Platform/ Service Provider	Intermediary in Network	
6. Benefits Considered - design and conduct to maximize benefits and minimize harms	Publication, funding, internal reputation and access.	Reduced risk of infection and data loss.	More effective techniques for building risk profiles. Removal of or patching of insecure hosts.	Reduced risk of infection and data loss.	More effective techniques for building risk profiles. Removal of or patching of insecure hosts.

EIA: Mitigation

Ethics Principles Considered	Human Subjects		
	Data Subject / End User	Network/ Platform/ Service Provider	Intermediary in Network
7. Mitigation controls- notify appropriate parties if research causes harm, consider if harm is revealed	• Eliminate any harm to integrity or functionality of user's systems- redirection to de-fanged fake phished site, replace link to Storm malware with benign executable served on demand from user not via any system exploit; • stripped out the exploit functionality of page, logged the user-agent string (to determine if the exploit would have likely worked) and always asked the user to download file, but did not actually provide them with an executable to download, • present 404 error upon user click to download;	n/a (no harms)	n/a (no harms)

What are we waiting for?

Erin Kenneally
Erin @ Elchemy.org