Ethics Research & Development Summary
Cyber-security Research Ethics Decision Support (CREDS) Tool

Workshop on Ethics in Networked Systems Research
Co-located with ACM SIGCOMM'15
August 21st 2015
London, UK

Erin Kenneally
UC San Diego
Center for Applied Internet Data Analysis
erin@caida.org

Marina Fomenkov
UC San Diego
Center for Applied Internet Data Analysis
marina@caida.org

This research & development summary addresses the workshop's call for ethical, social scientific or legal research that reflects on - or aims to guide - technical research and projects in the field of computer and data communication networks, especially an analysis to minimize the potential harm while enabling a broad range of Internet research to be conducted.

Motivation and Objectives

With research using data available online, researcher conduct is not fully prescribed or proscribed by formal ethical codes of conduct or law because of ill-fitting "expectations signals" – indicators of ethical and legal risk. We are researching and developing a conceptual model (framework) and an interactive online decision support tool to understand, evaluate and address ethical and legal issues surrounding online cyber risk research.[1]

Our applied research is motivated by the pragmatic needs of present day researchers that presage the negative impacts on academic and industrial R&D and public trust. More specifically, network and security researchers routinely encounter a multitude of research-relevant, yet sensitive information along the network stack: from application layer personal health, financial or behavioral data, usernames and passwords lists, corporate confidential documents, and email and voice communications databases; to lower layer network traffic traces, system vulnerabilities, and machine- to-machine communications. This information is found in various online locations ranging from normal websites and social networks to underground criminal forums, Internet relay chat rooms, and server drop zones on publicly-obscured/hidden sites. What are researchers' responsibilities when they come across sensitive information online that is a product of malicious (criminal theft or illicit fraud), negligent, or ignorant (data that were poorly secured or protected from public browsing) acquisition or disclosure? Does the calculation change when their collection (scraping, harvesting) and analysis (data mining, probabilistic reasoning) tools magnify either the quantity or

[1] For purposes of our project we use the term "online research" to encompass the various aspects of the use of the Internet as both a tool and a source of data for research, but it will not address those specific study procedures where data is collected from individuals in social networks or otherwise, such as is involved in behavioral manipulation, surveys, clinical interviews, structured tests, self-reports, deception, or ethnographic interviews.

quality of the sensitivities? These are open questions for which there are no immediate answers or community-wide, normative decision support tools.

The CREDS project seeks to outline and reach a common understanding and conduct for ethical and legal cyber risk research online in an effort to prevent unattended harm, diminished public trust, and reputational blowback by association arising from undifferentiated comparisons to public or private surveillance and cyber opportunism. We aim to help jumpstart collective dialogue and pave a path forward to harmonizing ethical and legal expectations for research using online data for researchers, oversight entities, policymakers and society. By arming researchers and risk advisors with a tool to realize more effective avoidance of risk, our approach will help researchers and overseers to identify and respond to these gray areas in a legally- and ethically-justified manner. It recognizes the need for immediate guidance by jumpstarting the solution, yet allows for shared understanding (best practices) to evolve and converge through the exchange of experiences among and between stakeholders as the tool and its underlying model gets socialized.

The vast majority of efforts to guide cyber research risk policies underway are focused on raising community dialogue about ethics principles and applications and not on ways to implement those foundational elements into research practice. Our project breaks new ground by implementing novel substantive ethics guidance via a scalable and accessible online risk decision support tool. Further, many efforts are exclusively focused on information risk, neglecting to consider risk related to research activity that impacts networks and systems as well. By enabling stakeholders with a risk decision support tool, our project uniquely attempts to create a tool to integrate the knowledge developed from years of compartmentalized dialogue and scholarship on Internet research risk, as well as to invoke models from other domains that are engaging similar issues.

Research & Development Approach

We propose to develop a framework facilitating risk assessment and ethics decisions in cyber research, implement it as an interactive wizard-style tool and make it available online to promote broad use by network and cybersecurity researchers and other relevant stakeholders such as oversight entities.

Against the backdrop of motivations and objective, the CREDS tool conceptual framework is necessarily principle-based rather than rule-based. To formulate the decision support tool foundation, we derive the principles and their applications (collectively, the *signals*) from a galvanization of legal and ethical models that have emerged in response to various technology-induced social issues in both research and non-research domains such as consumer protection law, Ethical Review Board regulations, financial and healthcare regulations, copyright law, and environmental law. We will engage multidisciplinary knowledge first from available literature (peer reviewed journals, law review articles, case law, news reports, conference papers, government reports, standards and regulations) and next from collaboration and information exchange with related efforts via workshops, focus groups, surveys and interviews. We will seek close interaction with the Networking and Security Ethics Feedback panel [1], SIGCOMM Workshop on Ethics in Networked Systems Research [2], and the Department of Homeland Security PREDICT Ethics Advisory group [3].
To refine and codify the developed foundation, we will use the cyber risk research activities at the Center for Applied Internet Data Analysis (CAIDA) and the Center for Evidence-based Security Research (CESR) at the University of California San Diego as case study test beds. Upon completion of tool development and usability testing, we plan to make it freely and publicly available online.

Intended Benefits

Ultimately, our decision tool will integrate a conceptual framework, methodology, and reference model for: estimating and communication of uncertainty and risk, understanding the process of analysis and potential

impacts of technology, and measuring and improving judgment and reasoning. Its widespread use will foster a shared understanding of cyber risk research and encourage the use of uniform, sustainable, lightweight decision support between and among researchers and oversight authorities.

The outcomes of iterative community feedback on the decision framework and tool may serve as a foundation for ongoing discussions, investigations and promotion of prescriptive norms for network and cybersecurity research online, such as what is "minimal risk" in this research context.

Specific benefits of this methodology/framework/tool include:

- develop a better understanding of network research collection, use and disclosure techniques, the suitability of their use in particular situations, and the comparative strengths and weaknesses;
- improve decision making processes when researcher's rights and interests conflict/vary with those of users or intermediaries who are impacted by research risk;
- reduce questions, complaints and disputes about research collection, use and publication/disclosure involving raw or derived sensitive information;
- improve public authority (funding agencies; institutional review boards; program review committees) accountability with a standardized process for evaluating reasoning and outcomes; and,
- advance analytic (predictive and descriptive) research that relies on the availability of information online while enhancing transparency, confidence and data sharing.

REFERENCES

[1] Ethics Feedback Panel for Networking and Security. https://www.ethicalresearch. org/efp/netsec.

[2] "Workshop on ethics in networked systems research," August 2015. London, UK. http: //conferences.sigcomm.org/sigcomm/2015/netethics.php.

[3] Protected Repository for the Defense of the Infrastructure against Cyber Threats (PREDICT). Advisory Activities Ethics of Cyber Security. https://predict.org/Default.aspx? tabid=157