Erin Kenneally
University of California San Diego
Center for Evidence-based Security Research (CESR)
Cooperative Association for Internet Data Analysis (CAIDA)

How to Throw the Race to the Bottom – Harmonizing Ethical & Legal Issues with ICT Research Using Online Data

Throwing the Race Plan

- Issue Space (Ordering Forces – Expectations gap)
- Common Scenarios Exposing Gaps
- Fractures Manifest
  - Ethical
  - Legal
  - Standards
- Closing the Gap- Solution Dimensions
  - Deriving Signals from New Models
  - Applying Signals- Expectation Impact Assessment (EIA)

Issue Space - ordering forces and expectations Gap

- Trust online reflects gap between individual and collective **EXPECTATIONS** (law, ethics) and their CAPABILITIES (technology)
- Law and ethics online and offline are **ORDERING FORCES**→ inform the acceptability of behaviors and relationships with persons & orgs
- Migration of analog activities online has exposed **GAP** between expectations and capabilities
- Manifest as **ambiguity between asserted rights, interests, and threats to**

Issue Space - ordering forces and expectations Gap

- What characterizes the ability to anonymously observe, collect and use new and existing online data without directly interacting with the subject of the data?
  - (a) cyber espionage and surveillance by corporations and nation-states
  - (b) online advertising and data brokering by industry
  - (c) network and security research
  - (d) all of the above

- Common thread : opaque acts + potentially harmful data collection and usage + no normative or proscriptive procedures and disclosures to the entities whose rights or interests may be negatively impacted
- What motivates attention to these harms & differentiates acts:
  - Law and Ethics → Ordering Forces
  - When silent / unclear, the risk of harms may be unattended or conflated
  - Revisit the legal and ethical calculus

Issue Space - ordering forces and expectations Gap

- **Uncertainty** over the collection, use and disclosure of online data **exposes gaps** and deficiencies in law and ethics.
- Goals of **network and security research remain** -- theoretic and applied knowledge of networks, malicious threats & vulnerabilities; development of new and improved cyber security products and strategies
- What is **changing & challenging legal and ethical ordering forces**?
  - **Character of the data** available to R to achieve goals:
    - Data that is openly available online, sensitive private, confidential or whose original acquisition or disclosure online illicit/unclean hands
    - What are R responsibilities re: sensitive information online that is a product of malicious, negligent, or ignorant collection or disclosure?
  - **R use** of collection (scanners, crawlers) and analysis (data mining, probabilistic reasoning) tools magnify sensitivities?

- **Goal**: initial model to understand, evaluate, address ethical and legal issues surrounding the use of 'online public data' for research
  - **Foster** novel (network and cyber security) research
  - **Discourage** opportunistically exploiting or engineering logical vulnerabilities in our ordering forces for research

Common Scenarios Exposing Gaps

- (1) **Network layer information** (maps, traffic, M2M communications) about Internet-wide consumer and industrial vulnerabilities (open embedded devices in the energy, telco and transportation networks) is readily **searchable and downloadable** from a **website** as a **result of** port scanning from a distributed **botnet** of poorly protected embedded devices.

- (2) **Location information** of individuals and business data (subnets, hosts, open ports and banners) from different **public sources** (search engines, databases, public archiving tool, e.g., Wayback Machine) are accessible using **free open source tools**

- (3) **Personal private data** (email addresses, names, device identifiers, financial account credentials, user name/password combinations, disease information) and **business confidential** manuals/technical docs **leaked** by negligent employees, fraudulent insiders or malicious hackers onto a publicly-accessible website and then **collected by an automated script** and posted openly on an **open chatroom**

- (4) **Links** to a readily downloadable dumps of stolen credentials, corporate financial ledgers and billing data, goods & services pricelists (stolen credit cards, accounts, botnets, cash out services) posted on **underground forums**

Ethical Fractures Manifest

- **Ethical parameters for collecting information in online public spaces:**
  - ambiguous & contested; IRBs don't know what protections should apply to online research
- **Signals are over- & under-inclusive**:
  - **Signals**: "human subject" = "identifiable" "private" "interactions/ intervention" … expedite review if "minimal risk"
  - **Bypass** signals if 'observe public behavior + collect non-identifiable + disclosure no cause harm' or 'collect existing data, docs, records + publicly available/recorded non-identifiable':
    - **Fingerprinting** practices proliferate, device IDs may come to represent users in databases, instead of PII
    - Entity covered (private sector not bound)
    - **Scope**: HS-centric, no address human-harming: systems and data that are distanced from HS
  - **Notice & Consent** ill-fitting: Object is the publication/system, not the individual person …. procedure, purpose, risk-benefit, withdrawal n/a with 2ndry info

Ethical Fractures Manifest

- NPRM Common Rule:
  - **Public Information is not HSR/Exclude public info from oversight**

  (Est Reasonable Expectations as basis for exempting public info, but begs question about how to determine REP!!!!!!)
  - **Minimal Risk** Def → Rec 3.1: probability and magnitude of phys/psych harm does not exceed what encountered in daily life or in routine medical, psychological, or educational examinations, tests, or procedures of the general population
  - **Consent** → Rec 4.5: should not require re-consent for future use of pre-existing, de-identified non-research or research data

- **IRB attempts** to manage gap:
  - create public-use datasets but inconsistent treatment and definitional disagreement across IRBs

Legal fractures Manifest

- **Confidential data** : Common Law duty on regulated contexts (doctor/patient, atty/client); core principles but not WHEN (caseXcase)
- Invasion of Privacy (Common Law Tort): R is not source/first order actor so trigger is absent/strained:
  - 1. Intrusion upon seclusion/private affairs 2. Public disclosure of embarrassing private facts 3. Publicity placing one in a false light in the public eye 4. Appropriate one's likeness for the advantage of another
- **Private Agreements**: NDA loophole- no privity in a secondary use context + excepts info that 'was publicly known and made generally available in the public domain prior to the time of disclosure

- **Sector-specific laws**:
  - Many data protection laws N/A → R not covered entity (HIPAA, GLBA, Fed and State Data Breach Laws)
  - Relevant privacy/computer trespass laws definition application challenges:
    - CFAA "unauthorized" "access" "damages"
    - ECPA "interception" & consent issue (transitive/distance)
    - Measuring Expectations : ToS? Assumed obscurity?
  - Damages/harm hurdle for privacy and identity-related : Increased Risk (fear of future injury not good enough)
- **Consent & notice** impracticable in the context of benefit/utility needs

Legal fractures manifest

- **Balancing of rights/interests**
  - 1st A rights (R, Commercial Co.), censorship, academic freedom, institutional accreditation if restrict
  - /eg/ Two major private LPR firms—sue Utah's governor and AG: 1st A right to collect data on license plates, displayed in public on open roads

- **Ancillary legal risk:**
  - Mere possession of sensitive info (pwds) not illegal
  - Trafficking not if no intent to transfer
  - Conspiracy and aiding & abetting fails: lack of knowledge whether source collection was illegal; mere possession of account numbers (unauthorized access device) is illegal under 1029 Access Device Fraud, but need intent to defraud

Standards Fractures Manifest

	Traditional	Now
Threat model	More bounded	New threats to privacy (data implicates ++indiv)
Collection	Trigger, provided, active	Use, generated, passive from automated, M2M transactions
'Personal Data'	Pre-determined, static	Context +++variables, dynamic w/ shifting norms
Purpose	Specific, static	Emergent, econ value and innovation derived from combining and subsequent use
Policy	Focus on individual, Start w/ hypothesis	> Expectations compete (balance innovation, growth), Opportunistic
Access & Correction	Bounded	Impracticable, N/A, Distance
Data quality	Bounded	Reliability & provenance problems

Closing the Gap- Solution Dimensions

- **1st/** galvanize the common dimensions across ethics and law
  - **WHAT** (nature of the data)
  - **WHERE/HOW** (place and method proxy for expectation)
  - **IMPACT** (type of harm, mitigation, purpose)

- **2nd/** reassess 'signals of expectations' using models from informal ordering forces
  - more nimble responding to change (compared to institutionalized law and ethics)

Deriving Expectation Signals from New Models

- **Fed & State Data Breach Laws** cover privacy incidents of electronic PII
  - What- PII
  - Impact- Risk of Harm triggers –"that compromises the security, confidentiality, or integrity of personal information"

- **The Menlo Report & Companion**

http://ssrn.com/abstract=2445102

- **HIPAA :**
  - exempts de-identified data
  - "Risk of harm" standard replaced with 4 factor test : nature and extent of the PHI; unauthorized person involved; whether PHI was actually acquired or viewed; extent to which any risk has been mitigated.

- **MLA Mobile Location Analytics** (smartstoreprivacy.com): self-regulatory framework for the services provided in the US to Retailers by MLA companies
- COLLECTION LIMITED- what is needed for analysis;
- USE LIMITED- no used in adverse manner (eligibility employment/credit, promotion, retention, pricing, terms);
- ONWARD TRANSFER- principles transitive to 3rd ptys
- RETENTION LIMITED- internal policies for storing and deleting unique-sensitive data;
- CONSUMER EDUCATION
- EXCEPTIONS: not identifiable (personal info linked to an identifier; person can be contacted based on that info) or, aggregated & not retained, or, affirmative consent

Deriving Expectation Signals from New Models

- **EU Data Protection Act principles** : 2ndary data can be processed if:
  - not to "support measures or decisions with respect to particular individuals." eg, not using research data for investigating benefit fraud
  - processed so no substantial distress to data subject
  - research results/stats must be disclosed so no individual ID'd.
- **EU Court of Justice** (05/14) ruling recognizes the expectations about privacy, autonomy, dignity
  - declares that EU Data Protection Dir est "Right to be Forgotten" - search engines must purge if "inadequate, irrelevant or no longer relevant" data from its results when a member of the public requests it, even if the material was previously published legally

- **2ndry Use health data for research model (SHIP)** (http://www.scot-ship-toolkit.org.uk/)
  - Researcher responsibilities
  - ID privacy risks/ likelihood of breach
  - Impact of privacy breach
  - Reputational impact on Researcher
  - Researcher motive
  - Public expectation and Public interest
  - Data handling- in ways that comply with the legal and ethical requirements
  - Transparent policies about collection & use

Deriving Expectation Signals from New Models

- **"Fair Use"** model for Researchers?
  - **Purpose** (and character of use eg, commercial/educ)
  - **Amount**/Most significant part (used in relation to whole data)
  - **Effect** (of use upon potential market /value of data)
  - **Nature of the data** (Factual works < protection than creative works)
  - Helps reduce a tension between © law and 1st A guarantee of freedom of expression

- **"Fairness" standard for Subjects viz FTC Sec 5**:
  - Act or practice unfair if (1) cause/likely harm to consumers (2) not reasonably avoidable by consumers and (3) not outweighed by countervailing benefits to consumers or to competition (15 U.S.C. § 45(n))
- Calls for **shifted Focus on Responsible Use, NOT Notice & Consent**: Allow collection of identifiable, restrict use and disclosure

Signals Applied- Expectation Impact Assessment

Dimensions	Signals / Predictors	Ethics		Law	
		Collection	Use/Disclosure	Collection	Use/Disclosure
WHAT (Nature of Data)	What is the nature and sensitivity of the information to be disclosed?				
	What is the reasonable expectations of the individual whose information it is?				
	Is it reasonably probable that the information was obtained through deceit, theft or without the owner's authorization?				
	Is it reasonable to believe it was protected by Confidentiality when originally collected/ disclosed?				
	Is it reasonable to obtain authorization?				
	Would Disclosure Control render original consent/confid restrictions (irrelevant)?				
HOW/WHERE	Availability of Alternatives? If source is illegal, must be no other alternative source from which to gain info				
	Can R publish general conclusions but exclude methodology & other detail that could enable replication; publish limited/ redacted?				
	Citations/Attribution - does it have a statement about where data acquired and admonition about illicit source acquisition?				
IMPACT (Type of Harm, Mitigation, WHY/ Purpose)	Are the risk control measures (security, anon) documented and made known?				
	What is the confidentiality and security arrangements in place to protect the information from further disclosure?				
	Has R obtained advice of expert advisor not directly connected with the use for which the disclosure is being considered (Research Ethics Committee, Privacy Advisory Committee)?				

Your Attention: Appreciated!

Erin Kenneally

erin@caida.org