Towards a Modern Approach to Privacy-Aware Government Data Releases

Micah Altman
MIT Libraries

David O’Brien & Alexandra Wood
Berkman Center for Internet & Society

Open Data: Addressing Privacy, Security, and Civil Rights Challenges
19th Annual BCLT/BTLJ Symposium
April 2015
Disclaimer

These opinions are our own. They are not the opinions of MIT, Brookings, Berkman any of the project funders, nor (with the exception of co-authored previously published work) our collaborators.
Collaborators

- The Privacy Tools for Research Data Project
  <privacytools.seas.harvard.edu>
- Research Support from Sloan Foundation; National Science Foundation (Award #1237235); Microsoft Corporation
Related Work


Preprints and reprints available from: informatics.mit.edu
Goals

1. Examine critical use cases

2. Develop a framework for systematically analyzing privacy in releases of data

3. Produce a guide for selecting among new legal and technical tools for privacy protection
Use Cases for Government Data Releases

- Freedom of Information Act/Privacy Act
- Traditional Public and Vital Records
- Official Statistics
- Open Government/E-Government Initiatives
Public Release of Workplace Injury Records
OSHA’s Form 301
Injury and Illness Incident Report

This Injury and Illness Incident Report is one of the first forms you must fill out when a recordable work-related injury or illness has occurred. Together with the Log of Work-Related Injuries and Illnesses and the accompanying Summary, these forms help the employer and OSHA develop a picture of the extent and severity of work-related incidents.

Within 7 calendar days after you receive information that a recordable work-related injury or illness has occurred, you must fill out this form or an equivalent. Some state workers’ compensation, insurance, or other reports may be acceptable substitutes. To be considered an equivalent form, any substitute must contain all the information asked for on this form.

According to Public Law 91-556 and 29 CFR 1904, OSHA’s recordkeeping rule, you must keep this form on file for 5 years following the year to which it pertains.

If you need additional copies of this form, you may photocopy and use as many as you need.

Information about the employee

1) Full name _______________________________________________________________________

2) Street ___________________________________________________________________________

3) City __________________________ State _______ ZIP _______________

4) Date of birth _______/_____/______

5) Date hired _______/_____/______

6) Male [ ] Female [ ]

Information about the physician or other health care professional

7) Name of physician or other health care professional ____________________________________________________________________________________

8) If treatment was given away from the worksite, where was it given?

   Facility __________________________________________________________________________

   Street ___________________________________________________________________________

   City __________________________ State _______ ZIP _______________

9) Was employee treated in an emergency room?

   Yes [ ] No [ ]

10) Was employee hospitalized overnight as an inpatient?

    Yes [ ] No [ ]

11) Case number from the Log ____________ (Transfer this case number from the Log after you record the case.)

12) Date of injury or illness _______/_____/______

13) Time employee began work _______/_____/______ AM / PM

14) Time of event _______/_____/______ AM / PM

   Check if time cannot be determined [ ]

15) What happened? Tell us how the injury occurred. Examples: “When ladder slipped on wet floor, worker fell 20 feet”; “Worker was sprayed with chlorine when gasket broke during replacement”; “Worker developed serious in wrist over time.”

16) What was the injury or illness? Tell us the part of the body that was affected and how it was affected; be more specific than “burn,” “pain,” or score. Examples: “Strained back”; “chemical burn; hand;” “carpal tunnel syndrome.”

17) What object or substance directly harmed the employee? Examples: “concrete floor”; “chlorine”;

   “radial arm saw.” If this question does not apply to the incident, leave it blank.

18) If the employee died, when did death occur? Date of death _______/_____/______
Benefits from Public Data Availability

- Transparency as a democratic principle
- Accountability of institutions
- Economic and social welfare benefits
- Data for research and scientific progress
Scope of Information Made Public

- All collected data not protected by FOIA, the Privacy Act, or OSHA reporting regulations
- Redaction of names, addresses, dates of birth, and gender
- Information to be released includes job title, date and time of incident, and descriptions of injury or illness and where and how it occurred
<table>
<thead>
<tr>
<th>Case number from the Log</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of injury or illness</td>
<td>9 17 2008</td>
</tr>
<tr>
<td>Time employee began work</td>
<td>8:30 AM</td>
</tr>
<tr>
<td>Time of event</td>
<td>10:45 AM</td>
</tr>
</tbody>
</table>

What was the employee doing just before the incident occurred? Describe the activity, as well as the tools, equipment, or material the employee was using. Be specific. Examples: “climbing a ladder while carrying roofing materials”; “spraying chlorine from hand sprayer”; “daily computer key-entry.”

Lifting boxes on shelves while restocking products.

What Happened? Tell us how the injury occurred. Examples: “When ladder slipped on wet floor, worker fell 20 feet”; “Worker was sprayed with chlorine when gasket broke during replacement”; “Worker developed soreness in wrist over time.”

Worker developed sharp pains in back while lifting a particularly heavy box.

What was the injury or illness? Tell us the part of the body that was affected and how it was affected; be more specific than “hurt,” “pain,” or “sore.” Examples: “strained back”; “chemical burn, hand”; “carpal tunnel syndrome.”

Worker strained his back and noted considerable pain and limitation of movement.
Unaddressed Challenges and Risks

Re-identification Risks

- Individuals can be identified despite redaction of directly identifying fields or attributes
- Robust de-identification of microdata is a very difficult problem, and free-form text fields are especially challenging

Information Sensitivity

- OSHA identifies “privacy concern cases” as injuries or illnesses related to sexual assault, mental health, or infectious diseases
- There are other situations in which details regarding an injury or illness may be sensitive, such those related to drug or alcohol abuse, that are not included
Unaddressed Challenges and Risks

Review, Reporting, and Accountability

- Lack of review mechanisms, such as systematic redactions of sensitive information before release
- Lack of accountability for harm arising from misuse of disclosed data
Framework for Modern Privacy Analysis
Observation 1

Privacy is not a simple function of the presence or absence of specific fields, attributes, or keywords in a released set of data.

Other factors, including what one can learn or infer about individuals from a data release as a whole or when linked with other information, may lead to harm.
Observation 2

Redaction, pseudonymization, coarsening, and hashing, are often neither an adequate nor appropriate practice, and releasing less information is not always a better approach to privacy.

Simple redaction of information that has been identified as sensitive is often not a guarantee of privacy protection and may also reduce the usefulness of the information. In addition, the act of redacting certain fields of a record may reveal the fact that a record contains sensitive information.
Observation 3

Naïve use of any data sharing model, including a more advanced model, is unlikely to provide adequate protection.

*Thoughtful analysis with expert consultation is necessary in order to evaluate the sensitivity of the data collected, to quantify the associated re-identification risks, and to design useful and safe release mechanisms.*
Framework for Privacy Analysis

- Benefits from data availability
- Scope of information made available
- Re-identification (learning) risks
- Information sensitivity (harm in context)
- Information transformation (aggregation, redaction)
- Post-disclosure control mechanisms: review, reporting, and information accountability
Privacy Interventions at Any Stage
Data Sharing Models
## Types and Targeting Interventions

<table>
<thead>
<tr>
<th></th>
<th>Procedural</th>
<th>Economic</th>
<th>Informational</th>
<th>Legal Mechanisms</th>
<th>Technical Mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retention</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transformation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post-Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Where do proposed interventions fit?

<table>
<thead>
<tr>
<th></th>
<th>Procedural</th>
<th>Economic</th>
<th>Informational</th>
<th>Legal Mechanisms</th>
<th>Technical Mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptance</td>
<td>Informed consent</td>
<td></td>
<td>Informed consent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retention</td>
<td>Right to examine</td>
<td>Property Rights Assignment; Fees;</td>
<td>Safe harbor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transformation</td>
<td>Right to correct</td>
<td>Fines</td>
<td>Breach reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access</td>
<td>Restrictions on use</td>
<td></td>
<td>Individual right of action</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post-Access</td>
<td>Tethering</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Formal Policies**
- PBD #2, 3, 7
- PBD #4, 7
- PBD #6, 78

**Encryption-Based**
- Data Blurring
- PDS
Technical Approaches: Statistical & Computational

- Contingency tables
- Synthetic data
- Data visualizations
- Interactive mechanisms
- Multiparty computations
- Functional and homomorphic encryption
Technical Approaches: Information Security

- Access controls (including tiered access models)
- Secure data enclaves
- Personal data stores
- Audit systems
- Information accountability/operational policy
- Risk assessments
Legal & Regulatory Approaches

- Notice and consent
- Data sharing agreements
- Transparency and audit requirements
- Data minimization requirements
- Accountability for misuse, including civil and criminal penalties and private rights of action
Observation 4

Current approaches to evaluating risk and data utility and selecting appropriate controls is largely ad-hoc and inconsistent across organizations and sectors.
## Risk and Harm

### Identifiability (learning potential)
- Direct identifiers
- Quasi-identifiers (personal, externally readily observable characteristics)
- Indirect-linkages
- Statistical reidentification risk
- Individual learning risk
- Social learning risks

### Information Sensitivity
- Types of harms: e.g., loss of insurability, loss of employability, market discrimination, criminal liability, psychological harm, loss of reputation, emotional harm, and loss of dignity (dignitary harm); social harms to a vulnerable group (e.g., stereotyping), price discrimination against vulnerable groups, market failures; chilling of speech and action; potential for political discrimination; potential blackmail and other abuses
- Expected magnitude of harm, if identification occurs (e.g., minimal, moderate, severe)
- Number of people exposed to harm
Selecting Controls: Risk & Harm Factors
## Information Factors

### Data Structure
- Logical Structure (e.g., single relation, multiple relational, network/graph, semi-structured, geospatial, aggregate table)
- Unit of observation
- Attribute measurement type (e.g., continuous/discrete; ratio/interval/ordinal/nominal scale; associated schema/ontology)
- Performance characteristics (e.g., dimensionality/number of measures, number of observation/volume, sparseness, heterogeneity/variety, frequency of updates/velocity)
- Quality characteristics (e.g., measurement error, metadata, completeness)

### Analysis Type
- Form of output (e.g., summary scalars, summary table, model parameters, data extract, static data publication, static visualization, dynamic visualization, statistical/model diagnostics)
- Analysis methodology (e.g., contingency tables/counting queries, summary statistics/function estimation, regression models/GLM, general model-based statistical estimation/MLE/MCMC, bootstraps/randomization/data partitioning, data mining/heuristics/custom algorithms)
- Analysis goal (e.g., rule-based, theory formation, existence proof, verification, descriptive inference, forecasting, causal inference, mechanistic inference)
- Utility/loss/quality measure (e.g., entropy, mean squared error, realism, validity of descriptive/predictive/causal statistical inference)
## Stakeholder Factors

### Disclosure Scenarios
- Source of threat (e.g., natural, unintentional, intentional)
- Areas of vulnerability (e.g., data, software, logistical, physical, social engineering)
- Attacker objectives, background knowledge, and capability (e.g., “nosy neighbor,” “business competitor,” “muckraking journalist,” “panopticon,” “intrusive employer/insurer”)
- Breach criteria/disclosure concept

### Stakeholders
- Stakeholder types (e.g., consumer, producer, funder, host institution, researcher, regulator, subject, citizen, journal)
- Stakeholder capacities/resources (e.g., technical expertise, infrastructural capacity, budget, staffing resources)
- Trust relationships
- Incentives and payoffs
- Stakeholder range of actions in each lifecycle stage
Selecting Controls: OSHA Example

- Tiered access model with embedded review, audit, and accountability mechanisms
  - Public access to contingency tables and data visualizations, for a quick review and comparison of different employers
  - Interactive query access via a privacy-aware model server, for enabling access to more fine-grained information
  - Restricted access to raw data via a secure data enclave, subject to data use agreement, for vetted researchers
References


Questions

E-mail: Micah Altman, escience@mit.edu
Web: privacytools.seas.harvard.edu