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
- Open Government/E-Government Initiatives
- Traditional Public and Vital Records
- Official Statistics
Recent Examples

- E-Government Data
  Occupational Safety and Health Administration release of workplace injury records

- Open Government Data
  Open cities data
Public Release of Workplace Injury Records
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
Case number from the Log 4 (Transfer the case number from the Log after you record the case.)

Date of injury or illness 9 17 2008
Month Day Year

Time employee began work 8:30 AM PM

Time of event 10:45 AM PM Check if time cannot be determined

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.
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 as those related to drug or alcohol abuse, that are not included.
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
Observations

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.
Observations

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.*
Observations

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 public data availability
- Scope of information made public
- Re-identification risks
- Information sensitivity
- Review, reporting, and information accountability
Privacy Interventions at Any Stage
Data Sharing Models
Data Management Approaches

- 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
Statistical & Computational Approaches

- Contingency tables
- Synthetic data
- Data visualizations
- Interactive mechanisms
- Multiparty computations
- Functional and homomorphomic encryption
## Selecting Appropriate Controls

### Data Structure
- Logical Structure (e.g., single relation, multiple relational, network/graph, semi-structured, geospatial, aggregate table)
- Source
- 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, total error)

### 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)
References


Questions

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

Privacy Tools for Sharing Research Data
A National Science Foundation Secure and Trustworthy Cyberspace Project

with additional support from the Sloan Foundation and Google, Inc.