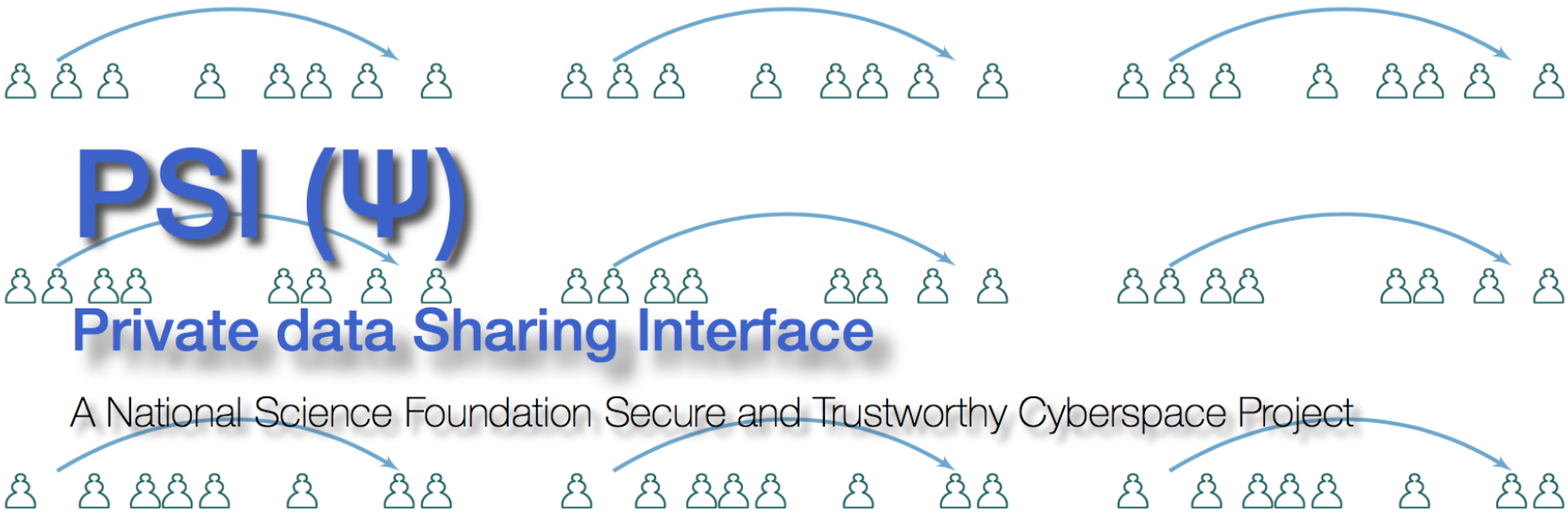
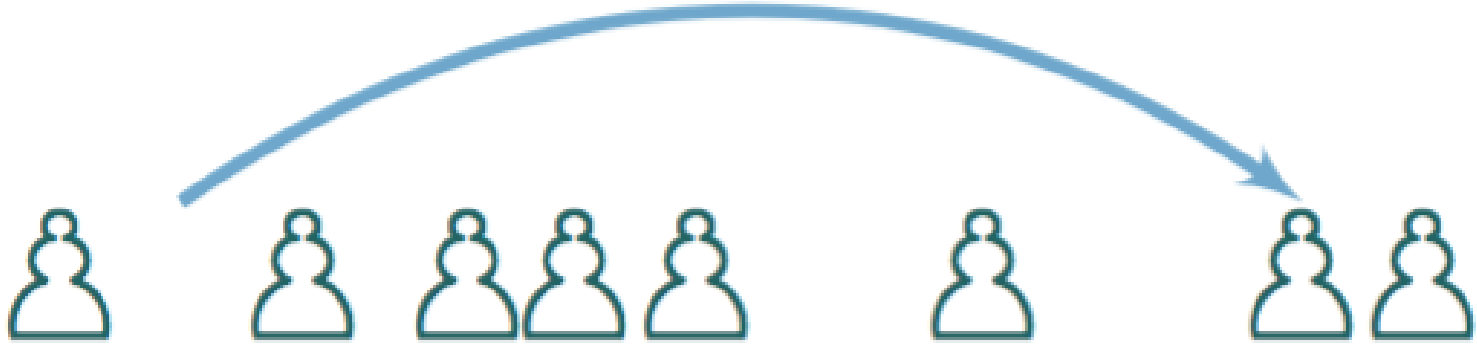


PSI (Ψ)

Private data Sharing Interface

A National Science Foundation Secure and Trustworthy Cyberspace Project



PSI (Ψ): a Private data Sharing Interface

Privacy Tools for Data Sharing
Lessons Learned and Directions Forward

December 11, 2017

James Honaker
james@hona.kr

Overview

GOALS:

- **Accessibility:** work for researchers without privacy expertise
- **Generality:** work on any received datasets across social science
- **Workflow-Compatibility:** work within familiar research tools

Overview

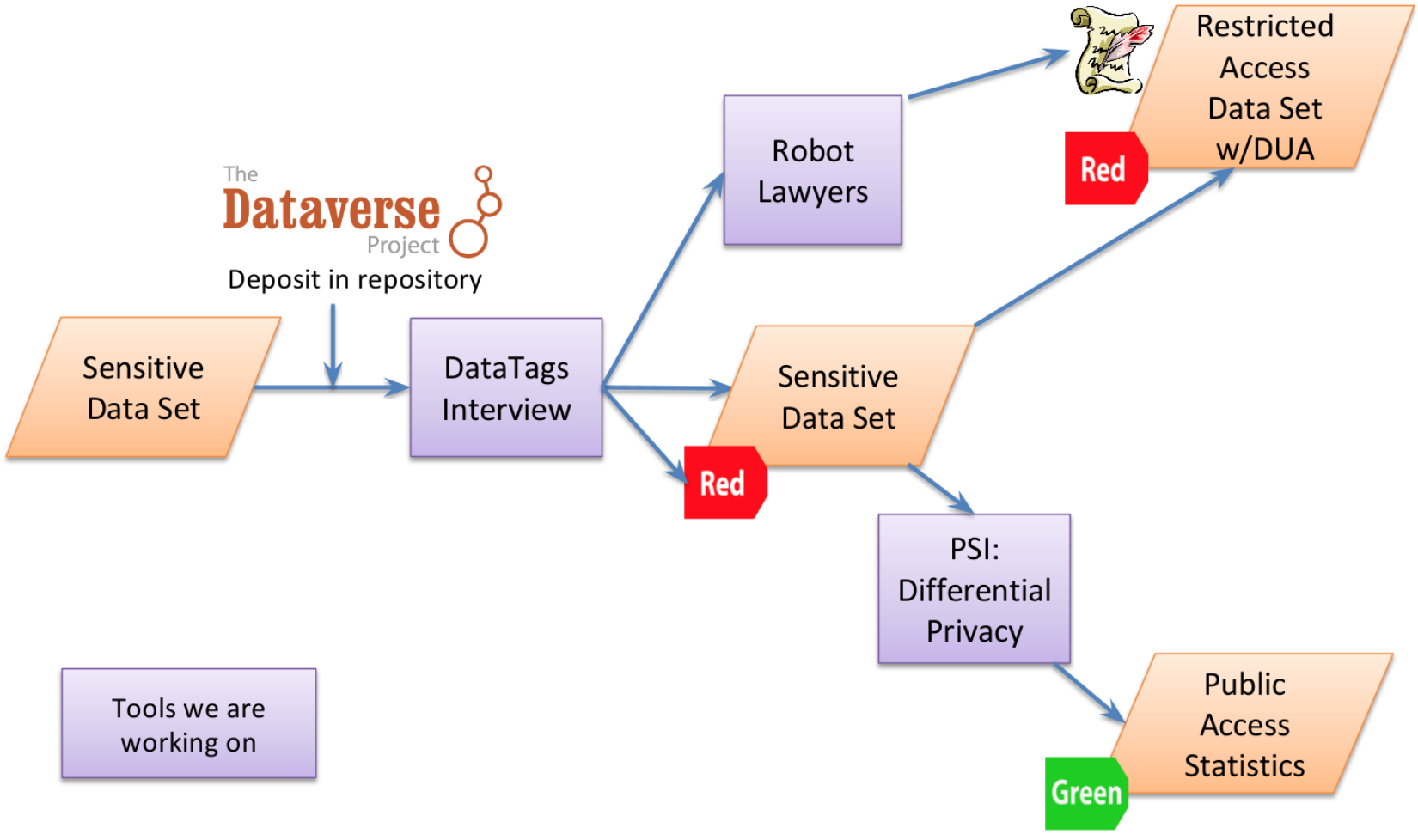
GOALS:

- **Accessibility:** work for researchers without privacy expertise
- **Generality:** work on any received datasets across social science
- **Workflow-Compatibility:** work within familiar research tools

INCENTIVES FOR USE:

- **"DP works great"** in some circumstances, the results of differentially private analyses are virtually indistinguishable from non-private analyses.
- **"Access is wide"** when data sharing to a wide community, we should be increasingly concerned about attacks from individuals with malicious intent.
- **"Data is currently unavailable"** when data is unavailable, *any* useful statistical information that DP can offer is a benefit

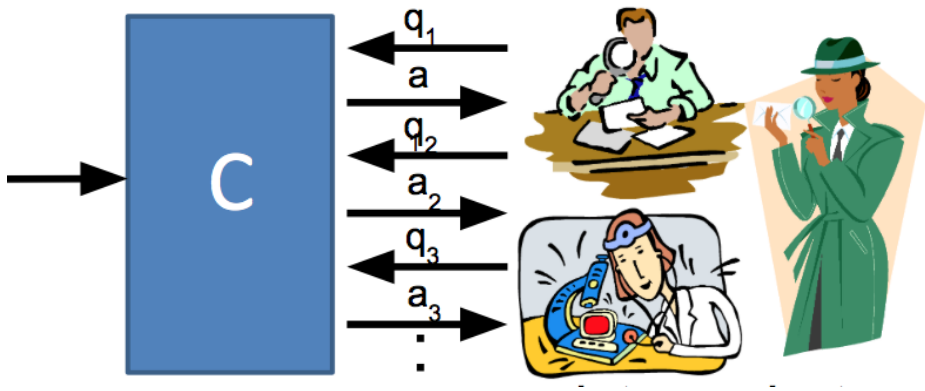
Integrated Privacy Tools



Differential Privacy

[Dinur-Nissim '03,+Dwork, Dwork-Nissim '04,
Blum-Dwork-McSherry-Nissim '05, Dwork-McSherry-Nissim-Smith '06]

Sex	Blood		HIV?
F	B		Y
M	A		N
M	O		N
M	O		Y
F	A		N
M	B		Y

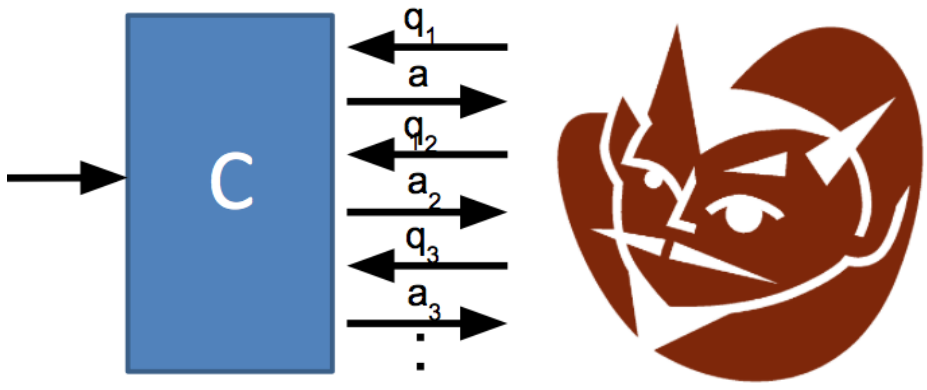


Data Curator Analysts

Differential Privacy

[Dinur-Nissim '03,+Dwork, Dwork-Nissim '04,
Blum-Dwork-McSherry-Nissim '05, Dwork-McSherry-Nissim-Smith '06]

Sex	Blood		HIV?
F	B		Y
M	A		N
M	O		N
M	O		Y
F	A		N
M	B		Y

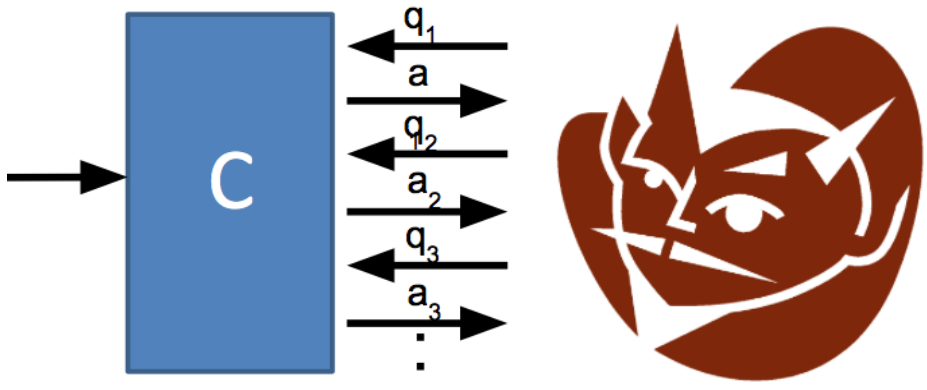


Data Curator Adversary

Differential Privacy

[Dinur-Nissim '03,+Dwork, Dwork-Nissim '04,
Blum-Dwork-McSherry-Nissim '05, Dwork-McSherry-Nissim-Smith '06]

Sex	Blood		HIV?
F	B		Y
M	A		N
M	O		N
M	O		Y
F	A		N
M	B		Y

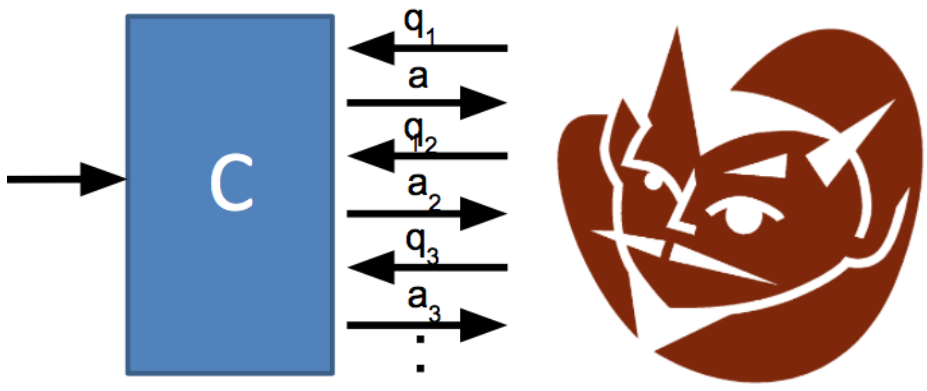


Data Curator Adversary

Differential Privacy

[Dinur-Nissim '03,+Dwork, Dwork-Nissim '04,
Blum-Dwork-McSherry-Nissim '05, Dwork-McSherry-Nissim-Smith '06]

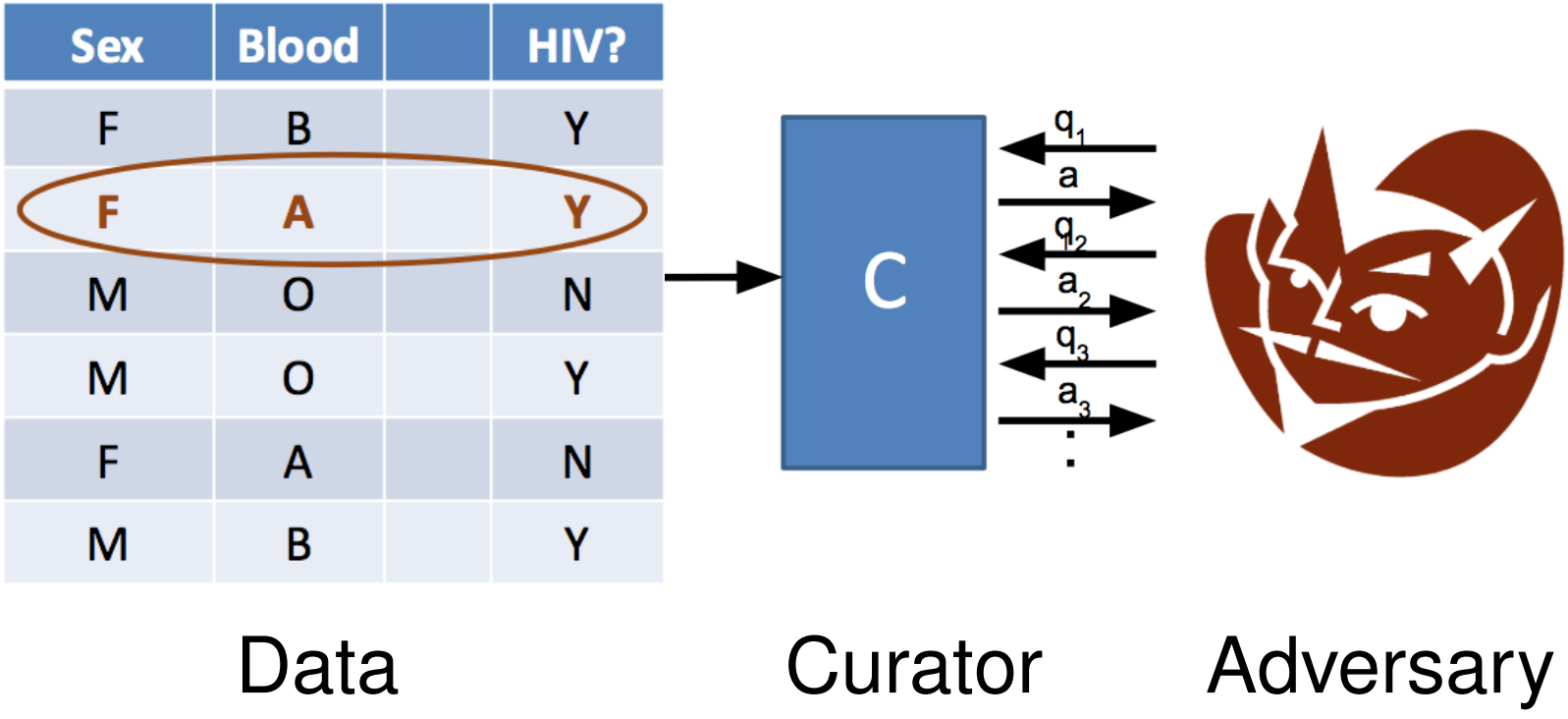
Sex	Blood		HIV?
F	B		Y
M	O		N
M	O		Y
F	A		N
M	B		Y



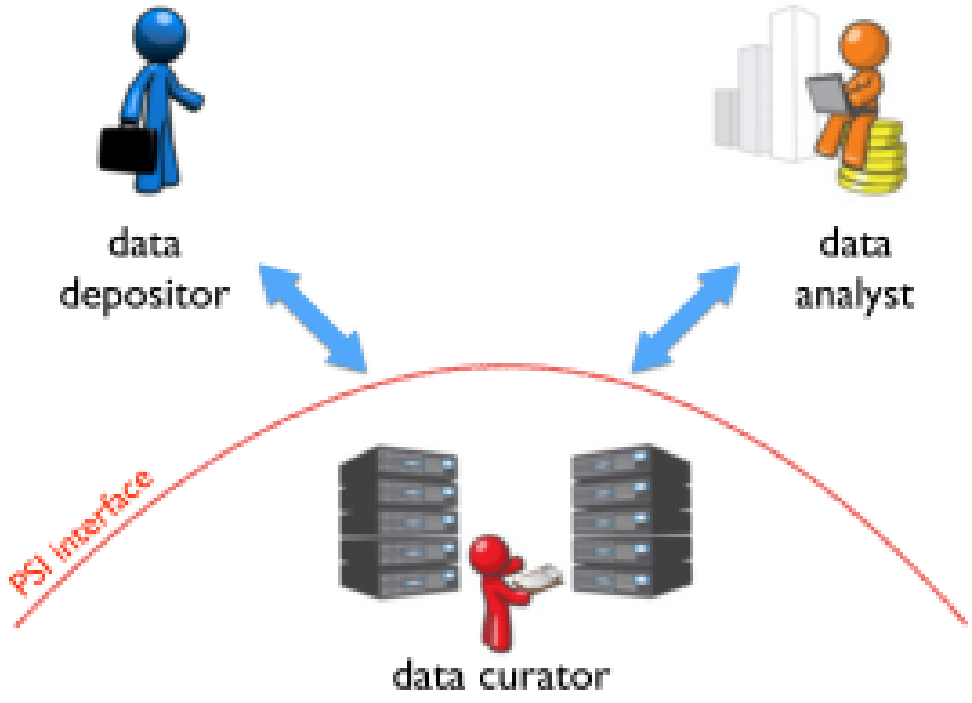
Data Curator Adversary

Differential Privacy

[Dinur-Nissim '03,+Dwork, Dwork-Nissim '04,
Blum-Dwork-McSherry-Nissim '05, Dwork-McSherry-Nissim-Smith '06]



Actors

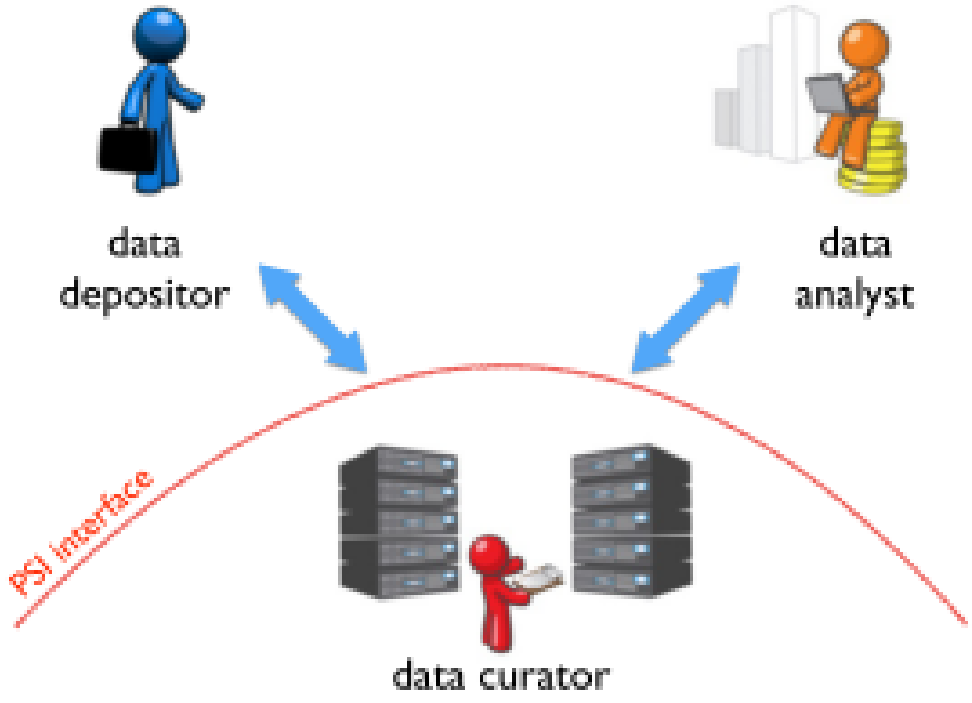


data depositors: Come to deposit their sensitive dataset in a repository, and may wish to make DP access available.

data curators: Maintain the hardware and software on which PSI runs and the accompanying repository infrastructure

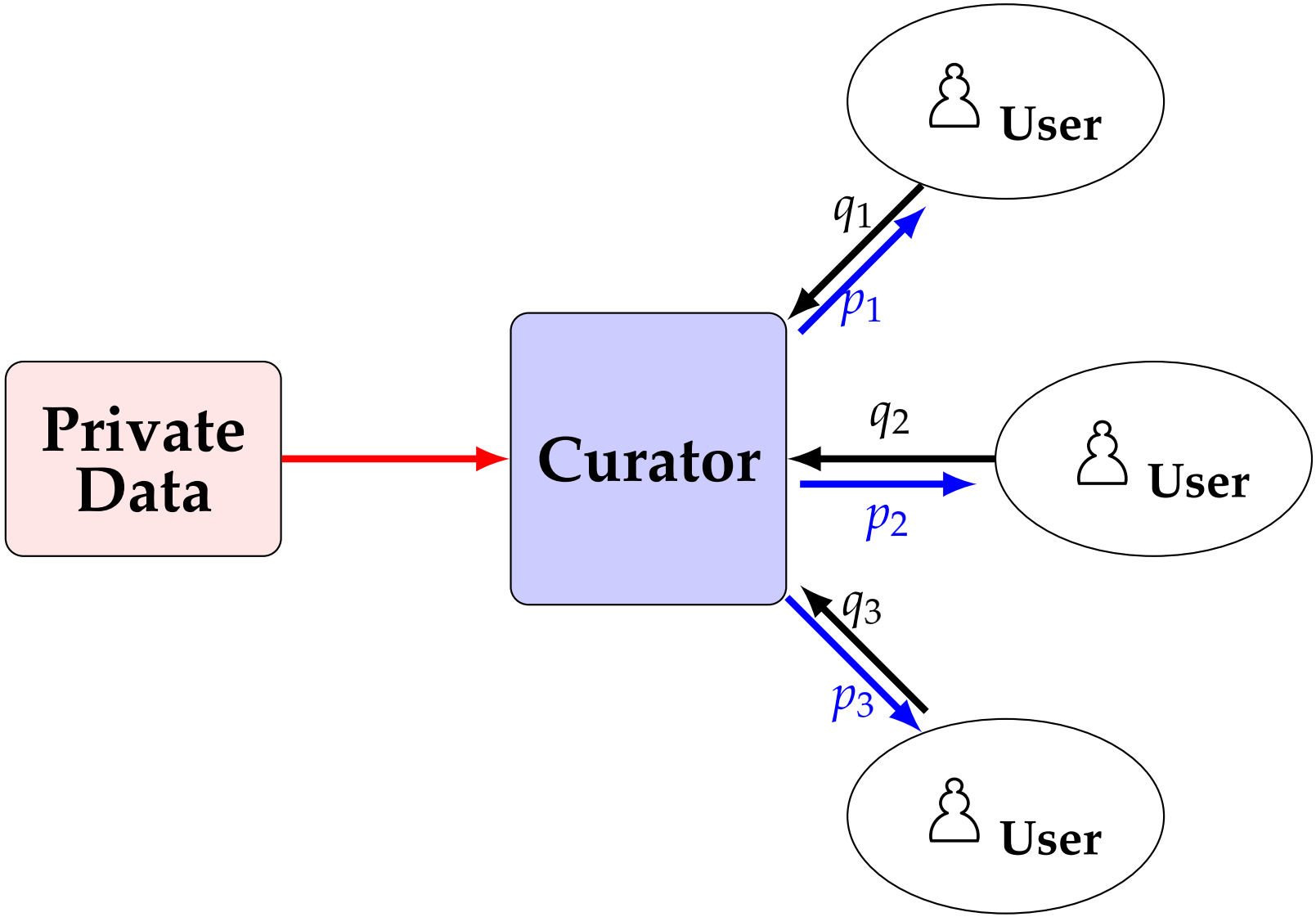
data analysts: Come to access sensitive datasets in the repository, often with the goal of data exploration

Actors



	Level of Trust	DP Expertise
data depositors:	Trusted	None
data curators:	Trusted	Modest
data analysts:	Untrusted	None
	Semi-Trusted	None

Curator Model



The curator architecture for data privacy.

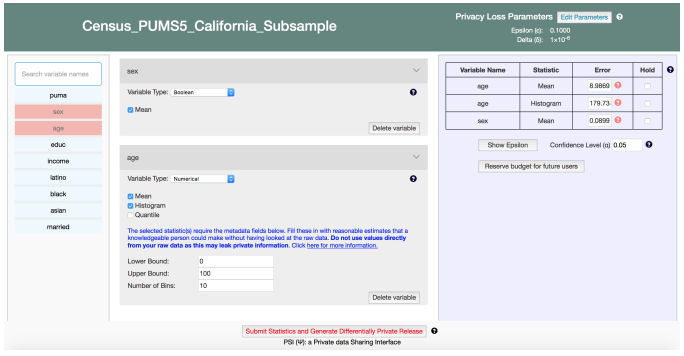
PSI (Ψ): a Private Data Sharing Interface

Key and Novel Features

- Exploratory Statistics
- Regression: Linear, Probit, Logit, Poisson
- Causal Inference: Matching and Difference of Means
- Formal Verification of Transformations
- Missing Data
- Tiered Access

PSI (Ψ): a Private Data Sharing Interface

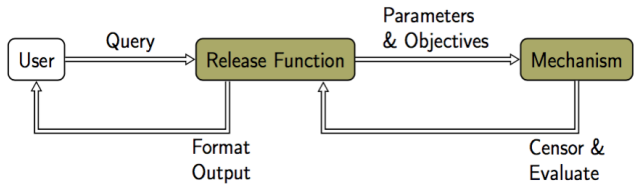
PSI (Ψ): a Private Data Sharing Interface



Budgeter

TwoRavens

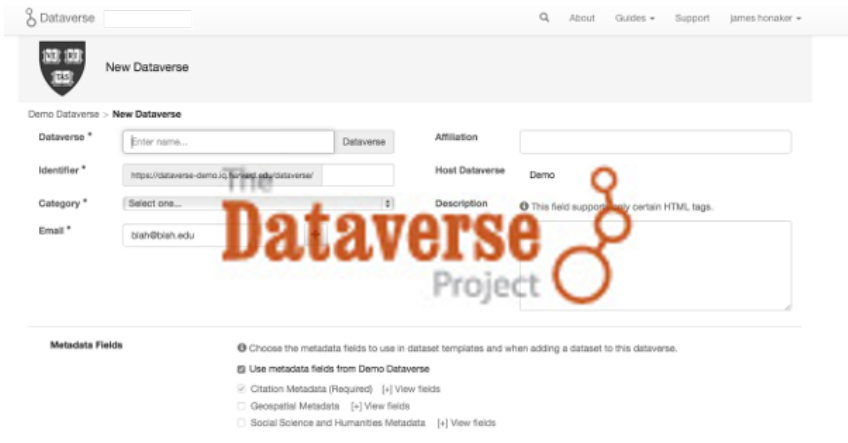
The Dataverse Project

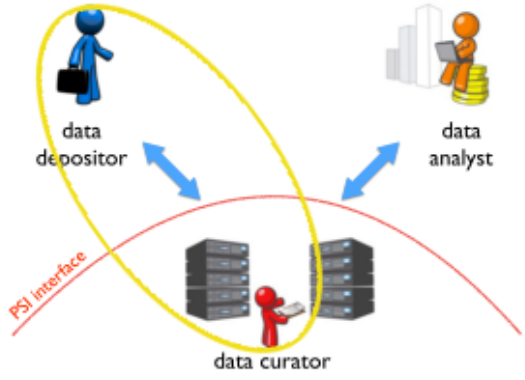


Psilence R Library

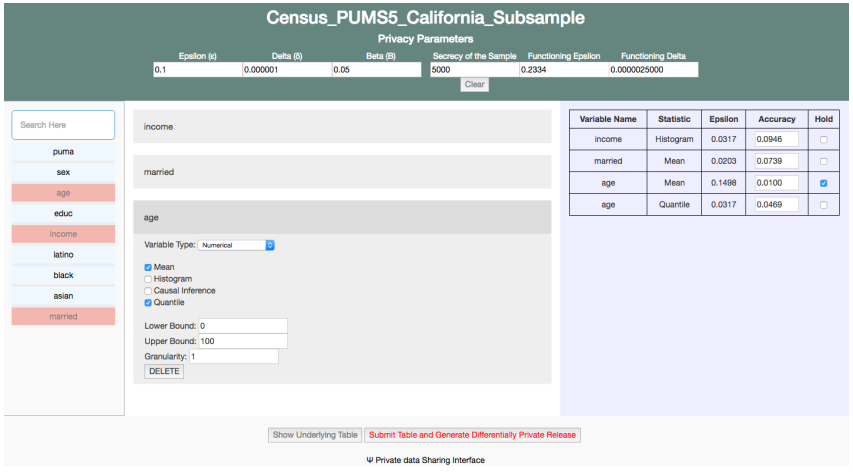
http://privacytools.seas.harvard.edu/psi

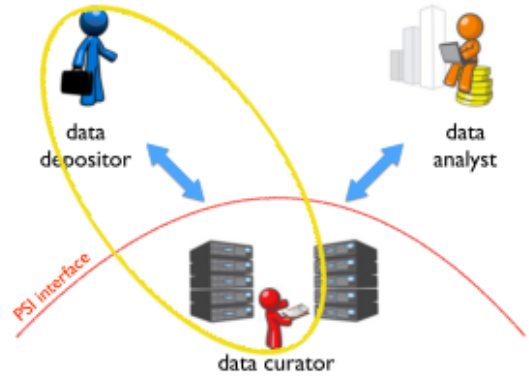

Upload
Budget
Release
Explore
Query


Dataverse
About
Guides
Support
james honaker
New Dataverse
Demo Dataverse > New Dataverse
Dataverse *
Identifier *
Category *
Email *
Affiliation
Host Dataverse
Demo
Description
Metadata Fields
Use metadata fields from Demo Dataverse
Citation Metadata (Required)
Geospatial Metadata
Social Science and Humanities Metadata

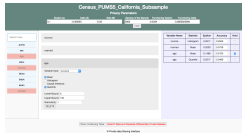

data depositor
data analyst
PSI interface
data curator


Upload
Budget
Release
Explore
Query


Census_PUMS5_California_Subsample
Privacy Parameters
Epsilon (ε)
Delta (δ)
Beta (β)
Secrecy of the Sample
Functioning Epsilon
Functioning Delta
0.1
0.000001
0.05
5000
0.2334
0.0000025000
Clear
Search Here
puma
sex
age
educ
income
latino
black
asian
married
income
married
age
Variable Type: Numerical
Mean
Histogram
Causal Inference
Quantile
Lower Bound: 0
Upper Bound: 100
Granularity: 1
DELETE
Variable Name
Statistic
Epsilon
Accuracy
Hold
income
Histogram
0.0317
0.0946
married
Mean
0.0203
0.0739
age
Mean
0.1498
0.0100
age
Quantile
0.0317
0.0469
Show Underlying Table
Submit Table and Generate Differentially Private Release
Ψ Private data Sharing Interface


data depositor
data analyst
PSI interface
data curator

Upload

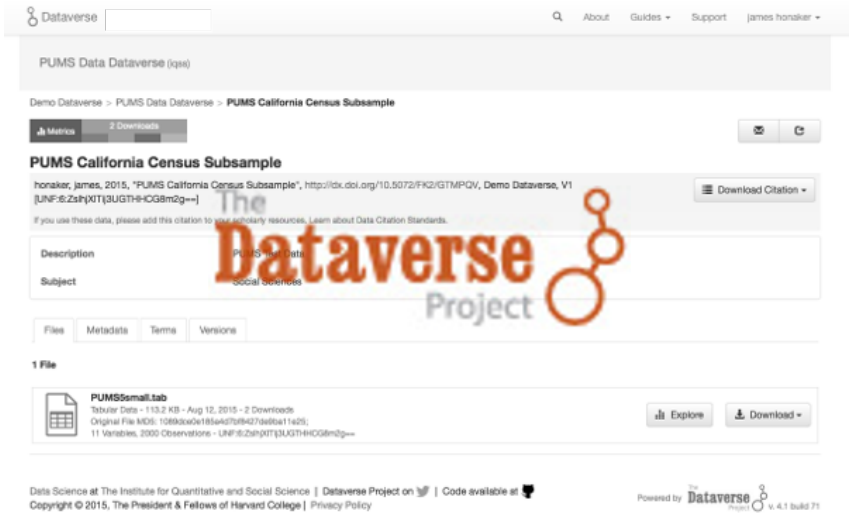


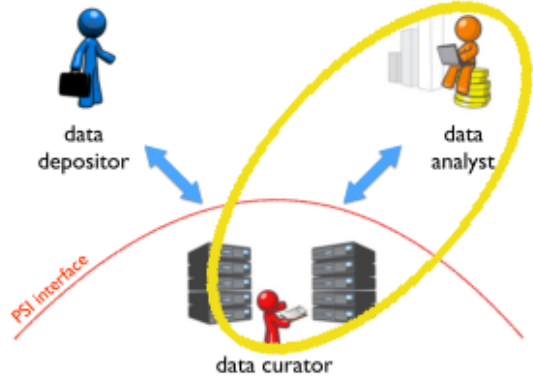
Budget

Release

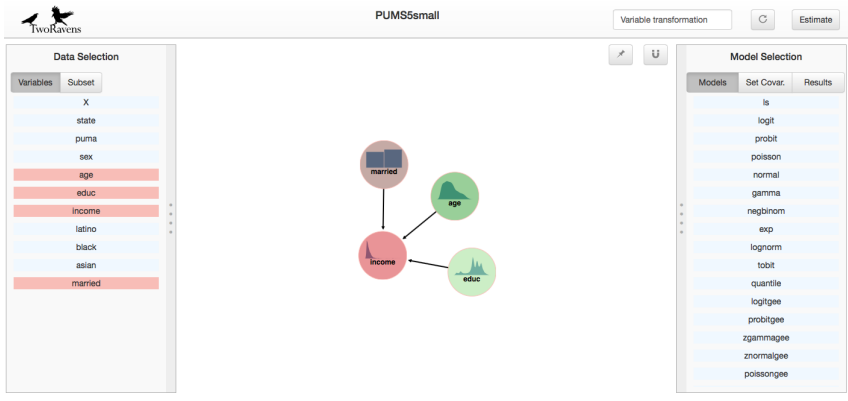
Explore

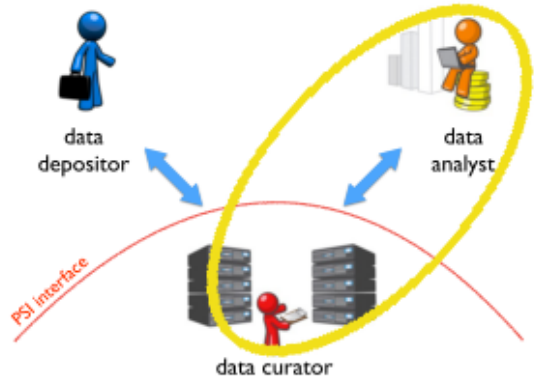
Query



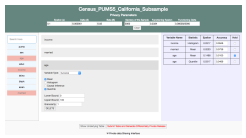



Upload
Budget
Release
Explore
Query


TwoRavens
PUMS5small
Variable transformation
Estimate
Data Selection
Variables
Subset
X
state
puma
sex
age
educ
income
latino
black
asian
married
married
age
income
educ
Model Selection
Models
Set Covar.
Results
ls
logit
probit
poisson
normal
gamma
negbinom
exp
lognorm
tobit
quantile
logitgee
probitgee
zgammagee
znormalgee
poissongee


data depositor
data analyst
PSI interface
data curator

Upload

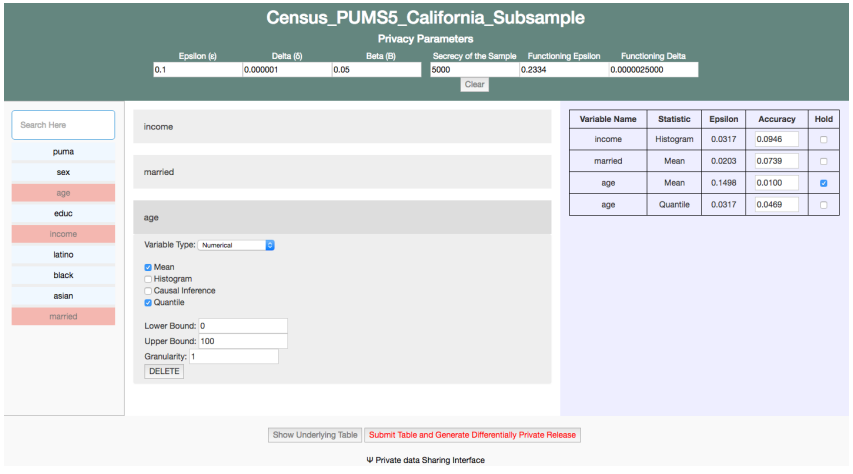


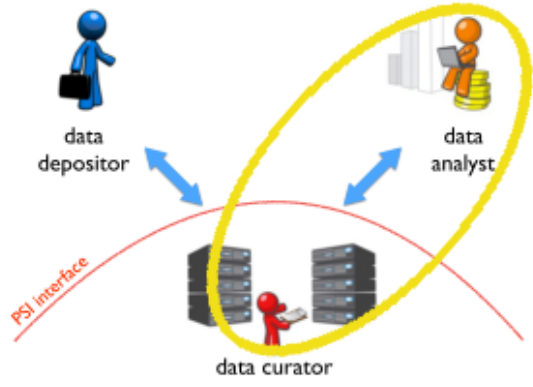
Budget

Release

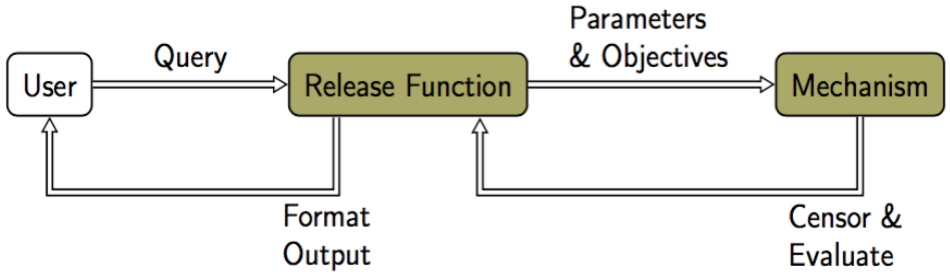
Explore

Query

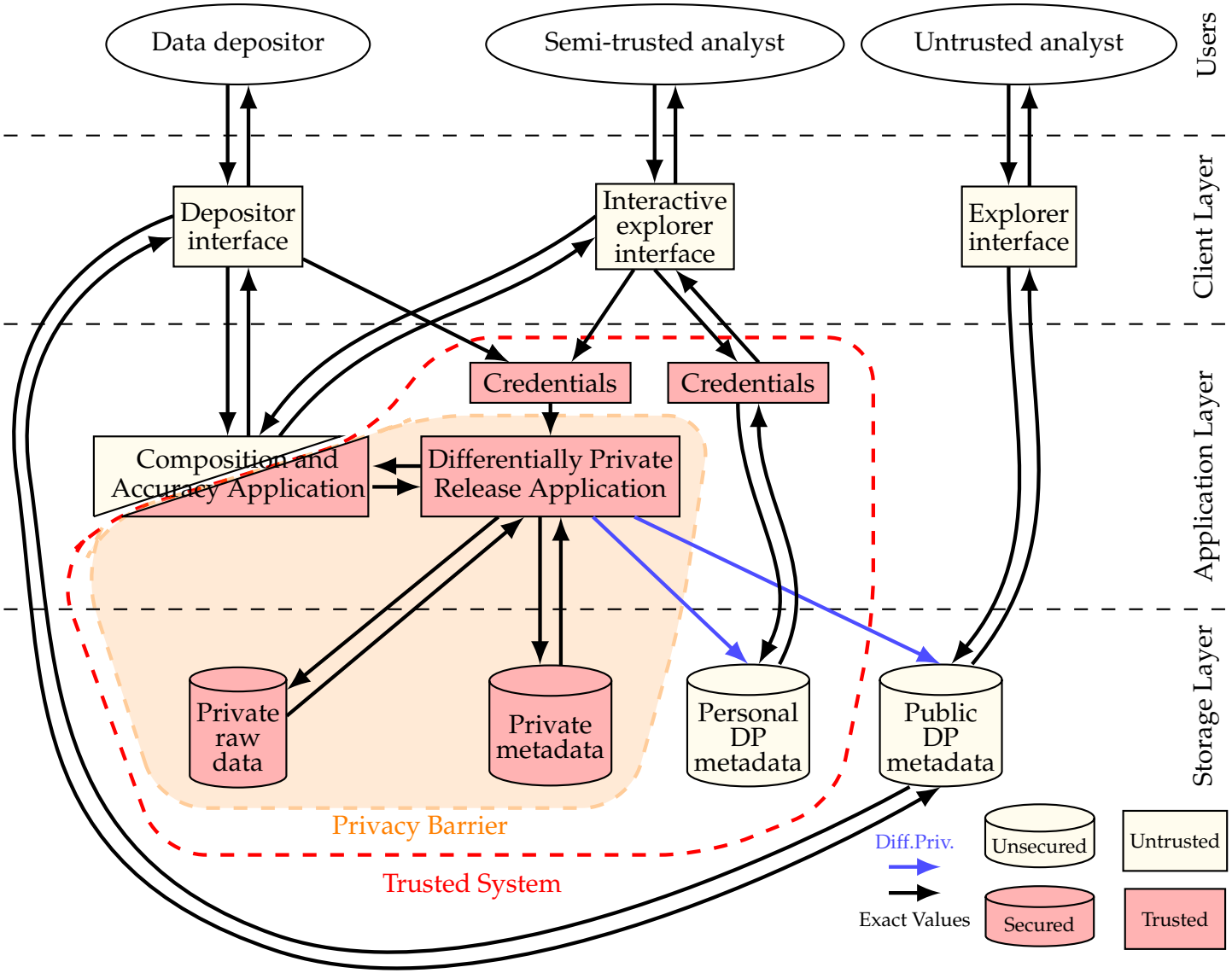


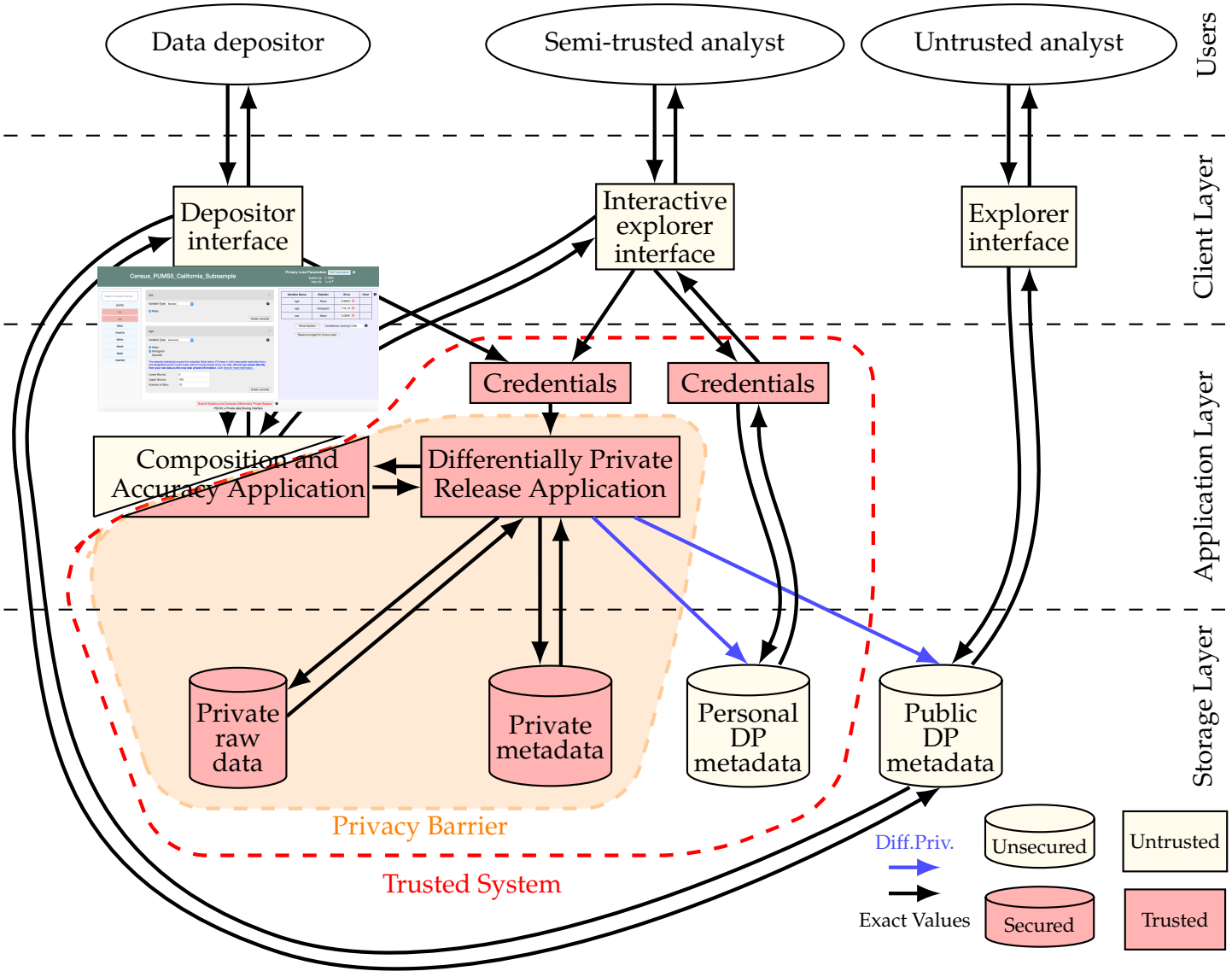


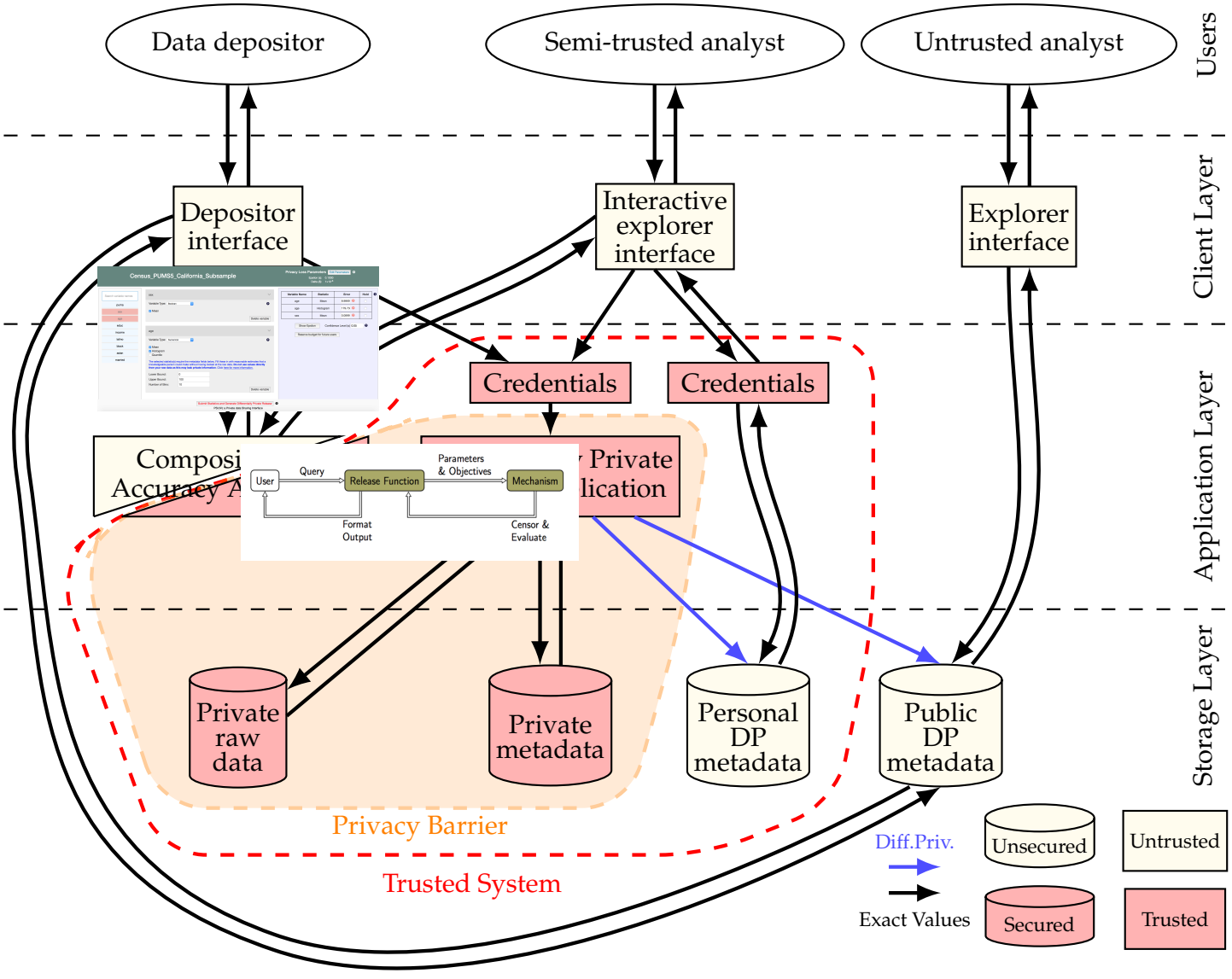
PSI Library

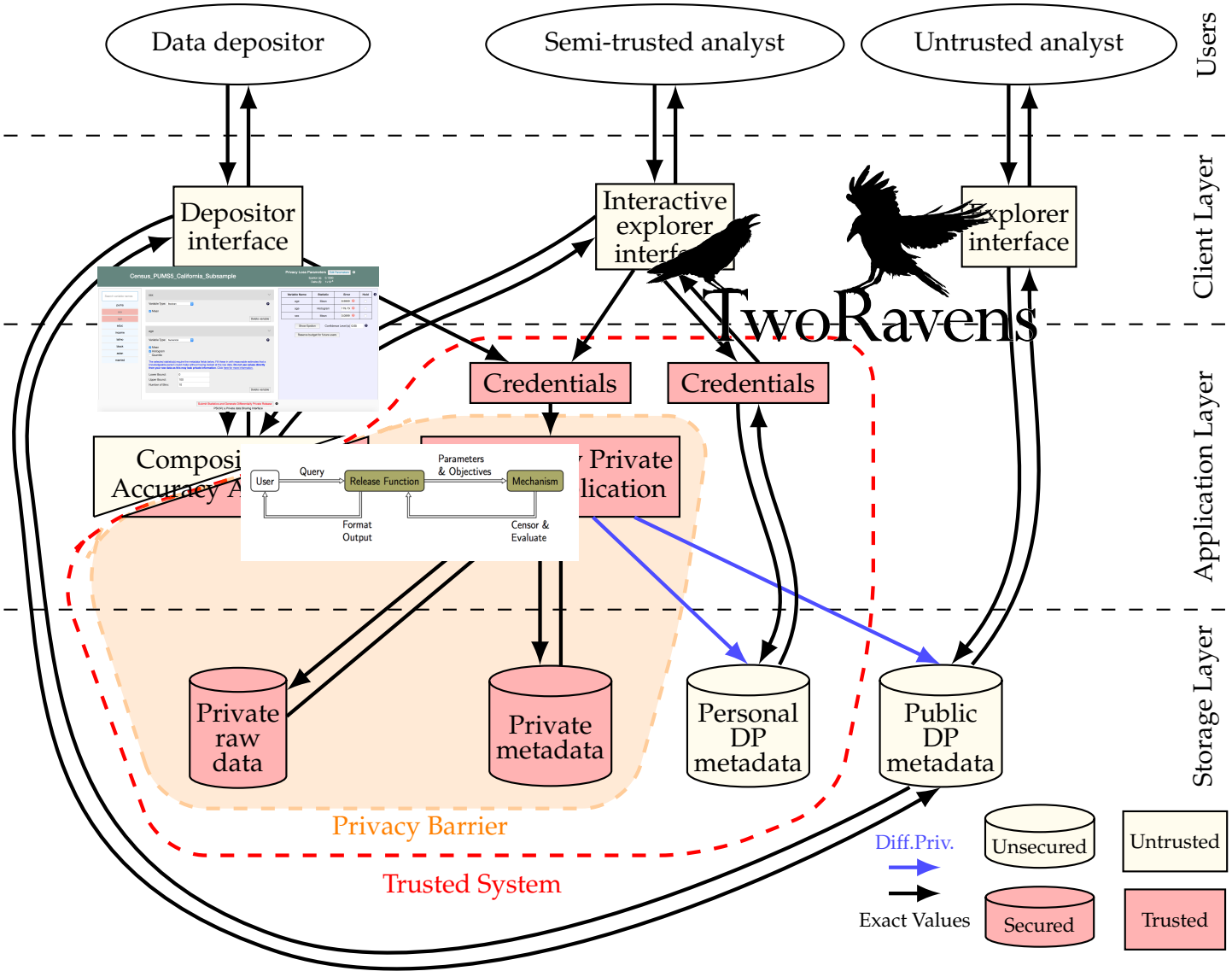


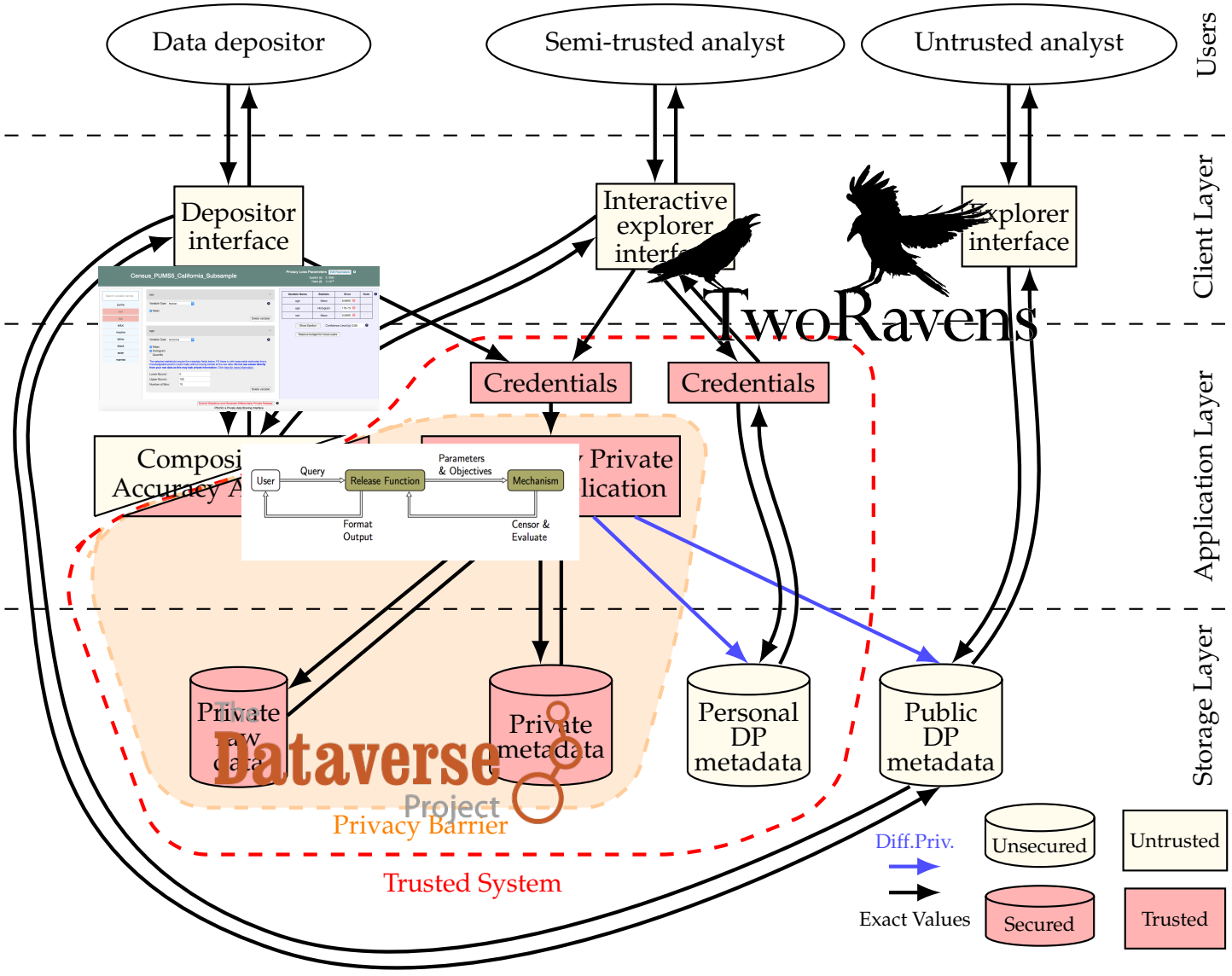
- Modular architecture
- Class based, using R
- Contains common exploratory statistics
  - Univariate descriptive statistics, such as means, quantiles, histograms, and approximate cumulative distribution functions.
  - Basic statistical estimators, matching algorithms and difference-of-means tests for causal inference, and low-dimensional linear, logit, probit and poisson regression.
- Reusable

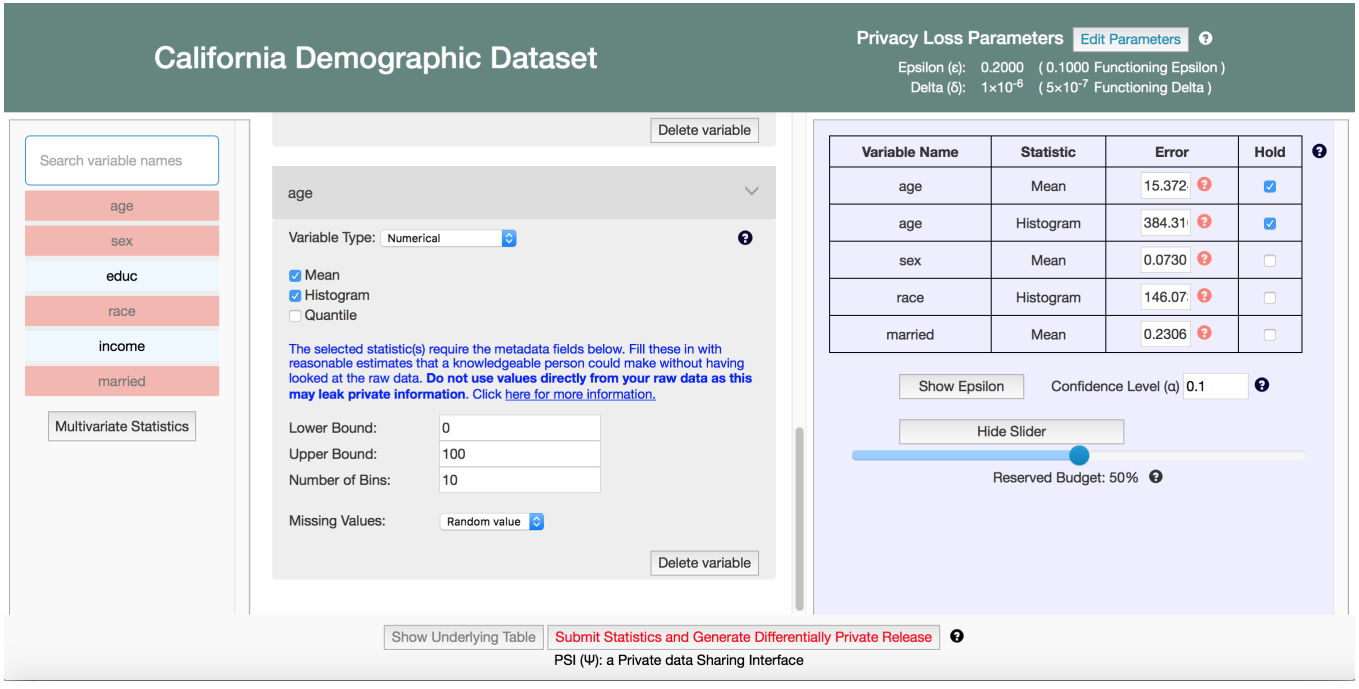

Data depositor
Semi-trusted analyst
Untrusted analyst
Users
Depositor interface
Interactive explorer interface
Explorer interface
Client Layer
Credentials
Credentials
Composition and Accuracy Application
Differentially Private Release Application
Application Layer
Private raw data
Private metadata
Personal DP metadata
Public DP metadata
Storage Layer
Privacy Barrier
Trusted System
Diff.Priv.
Exact Values
Unsecured
Secured
Untrusted
Trusted


Data depositor
Semi-trusted analyst
Untrusted analyst
Users
Depositor interface
Interactive explorer interface
Explorer interface
Client Layer
Credentials
Credentials
Composition and Accuracy Application
Differentially Private Release Application
Application Layer
Private raw data
Private metadata
Personal DP metadata
Public DP metadata
Storage Layer
Privacy Barrier
Trusted System
Diff.Priv.
Exact Values
Unsecured
Secured
Untrusted
Trusted

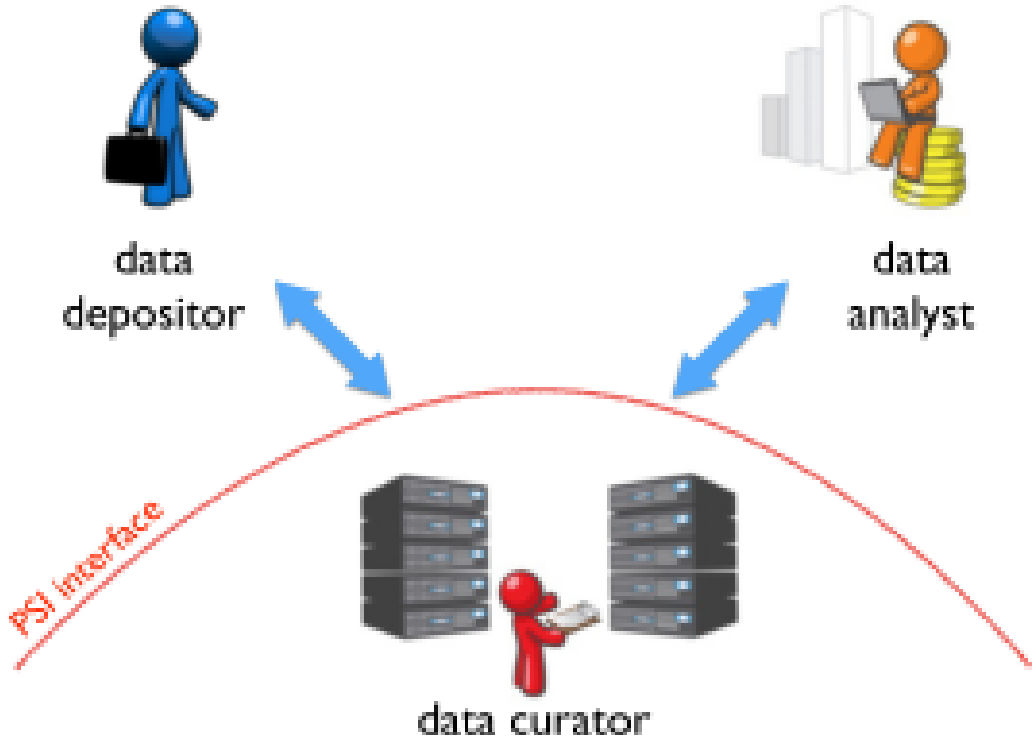

Data depositor
Semi-trusted analyst
Untrusted analyst
Users
Depositor interface
Interactive explorer interface
Explorer interface
Client Layer
Credentials
Credentials
Composi
Accuracy A
Private
lication
User
Query
Release Function
Parameters & Objectives
Mechanism
Format Output
Censor & Evaluate
Application Layer
Private raw data
Private metadata
Personal DP metadata
Public DP metadata
Storage Layer
Privacy Barrier
Trusted System
Diff.Priv.
Exact Values
Unsecured
Secured
Untrusted
Trusted

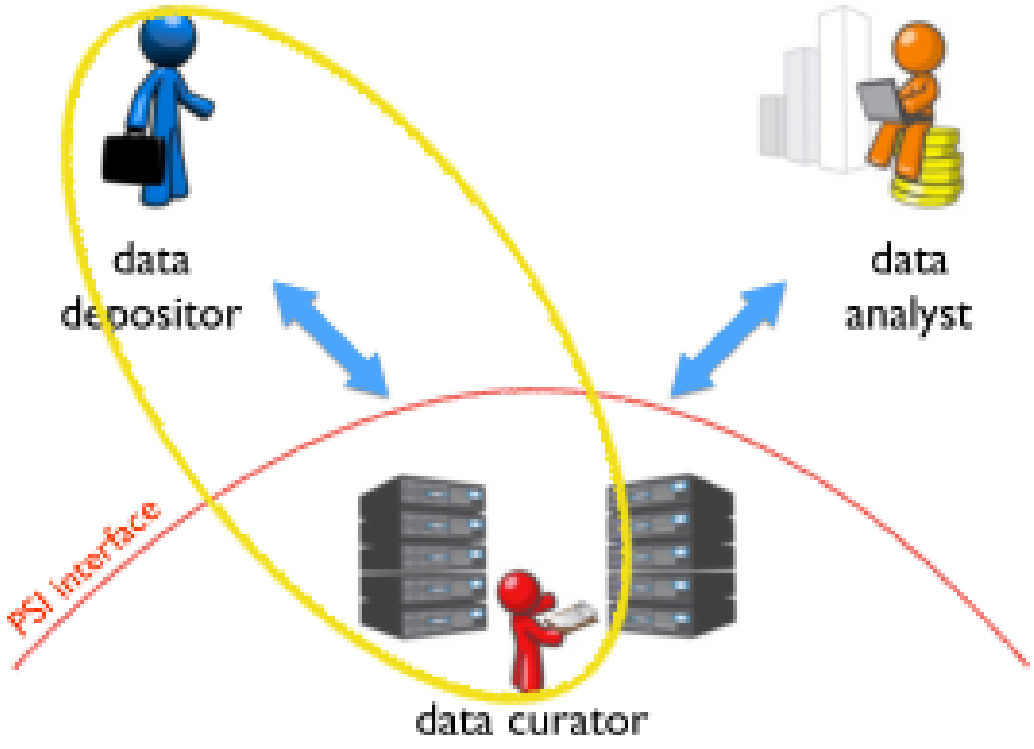

Data depositor
Semi-trusted analyst
Untrusted analyst
Users
Depositor interface
Interactive explorer interface
Explorer interface
Client Layer
TwoRavens
Credentials
Credentials
Application Layer
Private application
User
Query
Release Function
Parameters & Objectives
Mechanism
Format Output
Censor & Evaluate
Private raw data
Private metadata
Personal DP metadata
Public DP metadata
Storage Layer
Privacy Barrier
Trusted System
Diff.Priv.
Exact Values
Unsecured
Secured
Untrusted
Trusted

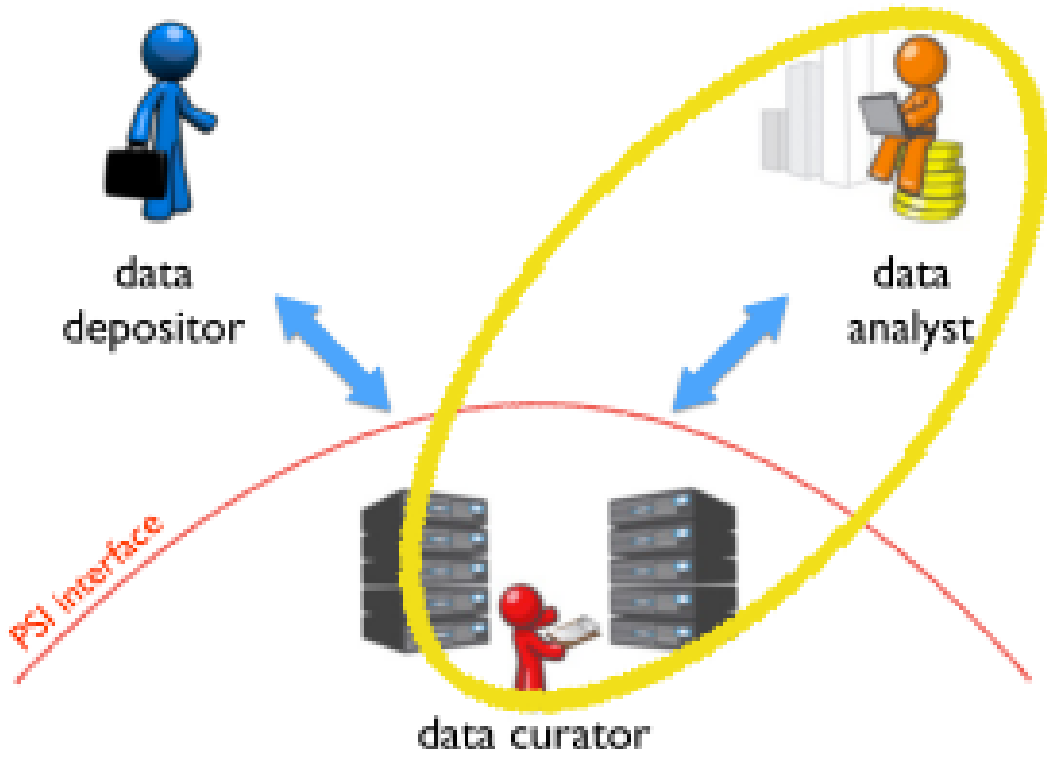

Data depositor
Semi-trusted analyst
Untrusted analyst
Users
Depositor interface
Interactive explorer interface
Explorer interface
Client Layer
TwoRavens
Credentials
Credentials
Application Layer
Query
Release Function
Parameters & Objectives
Mechanism
User
Format Output
Censor & Evaluate
Private Application
Private Raw Data
Private metadata
Personal DP metadata
Public DP metadata
Storage Layer
Dataverse Project
Privacy Barrier
Trusted System
Diff.Priv.
Exact Values
Unsecured
Secured
Untrusted
Trusted


California Demographic Dataset
Privacy Loss Parameters
Edit Parameters
Epsilon (ε): 0.2000 (0.1000 Functioning Epsilon)
Delta (δ): 1×10^-6 (5×10^-7 Functioning Delta)
Search variable names
age
sex
educ
race
income
married
Multivariate Statistics
Delete variable
age
Variable Type: Numerical
Mean
Histogram
Quantile
The selected statistic(s) require the metadata fields below. Fill these in with reasonable estimates that a knowledgeable person could make without having looked at the raw data. Do not use values directly from your raw data as this may leak private information. Click here for more information.
Lower Bound: 0
Upper Bound: 100
Number of Bins: 10
Missing Values: Random value
Delete variable
Variable Name
Statistic
Error
Hold
age
Mean
15.372
age
Histogram
384.31
sex
Mean
0.0730
race
Histogram
146.07
married
Mean
0.2306
Show Epsilon
Confidence Level (α) 0.1
Hide Slider
Reserved Budget: 50%
Show Underlying Table
Submit Statistics and Generate Differentially Private Release
PSI (Ψ): a Private data Sharing Interface

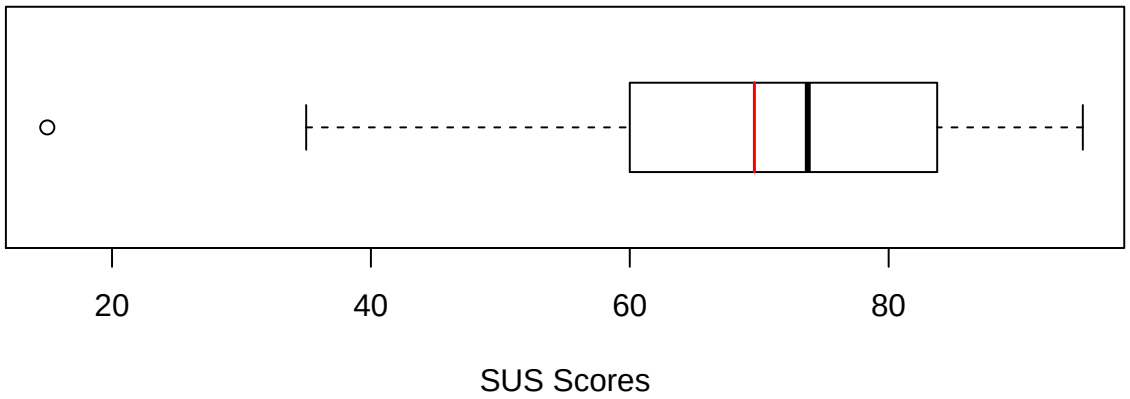
http://


data
depositor
data
analyst
PSJ interface
data curator


data
depositor
data
analyst
PSI interface
data curator


data
depositor
data
analyst
PSI interface
data curator

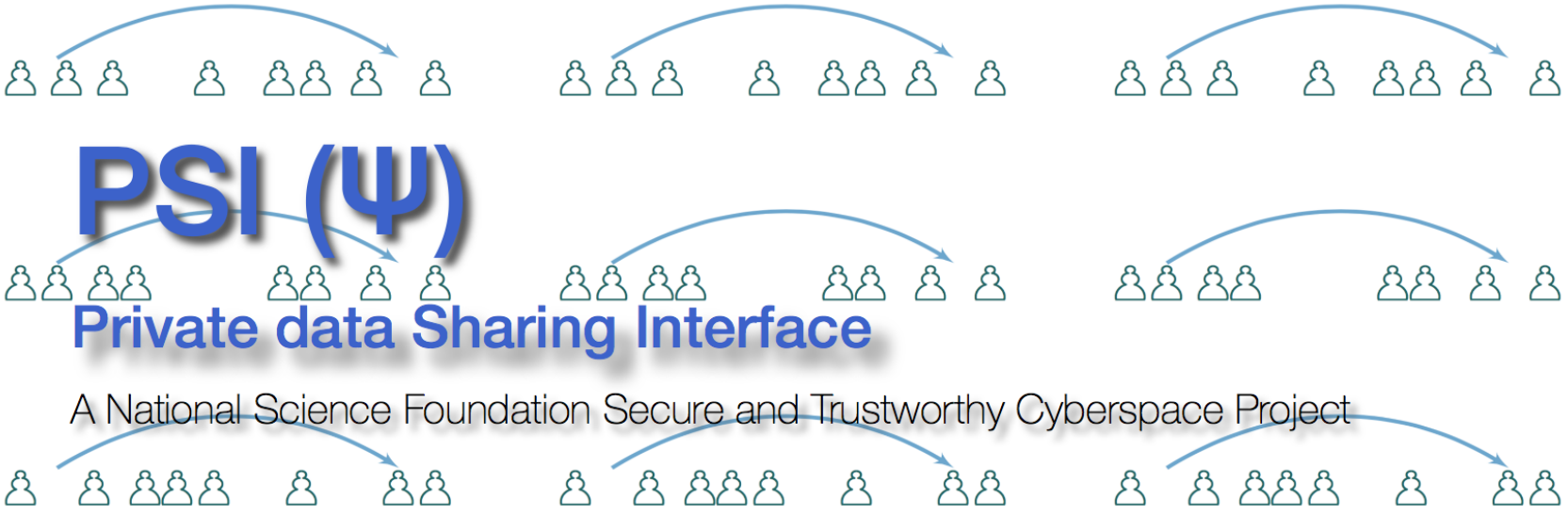
Usability



- 28 subjects over three phases
- 11 tasks over the course of an hour
- Excel 56.5; GPS 70.8; ⟵ PSI ⟶; iPhone 78.5

Conclusion

- **Accessibility:** Successful usability studies (and replication analyses)
- **Generality:** Growing library of algorithms for data exploration of social science data
- **Workflow:** Integrated via Dataverse into the data life cycle



Live Demo and Paper available at:

`http://privacytools.seas.harvard.edu/psi`

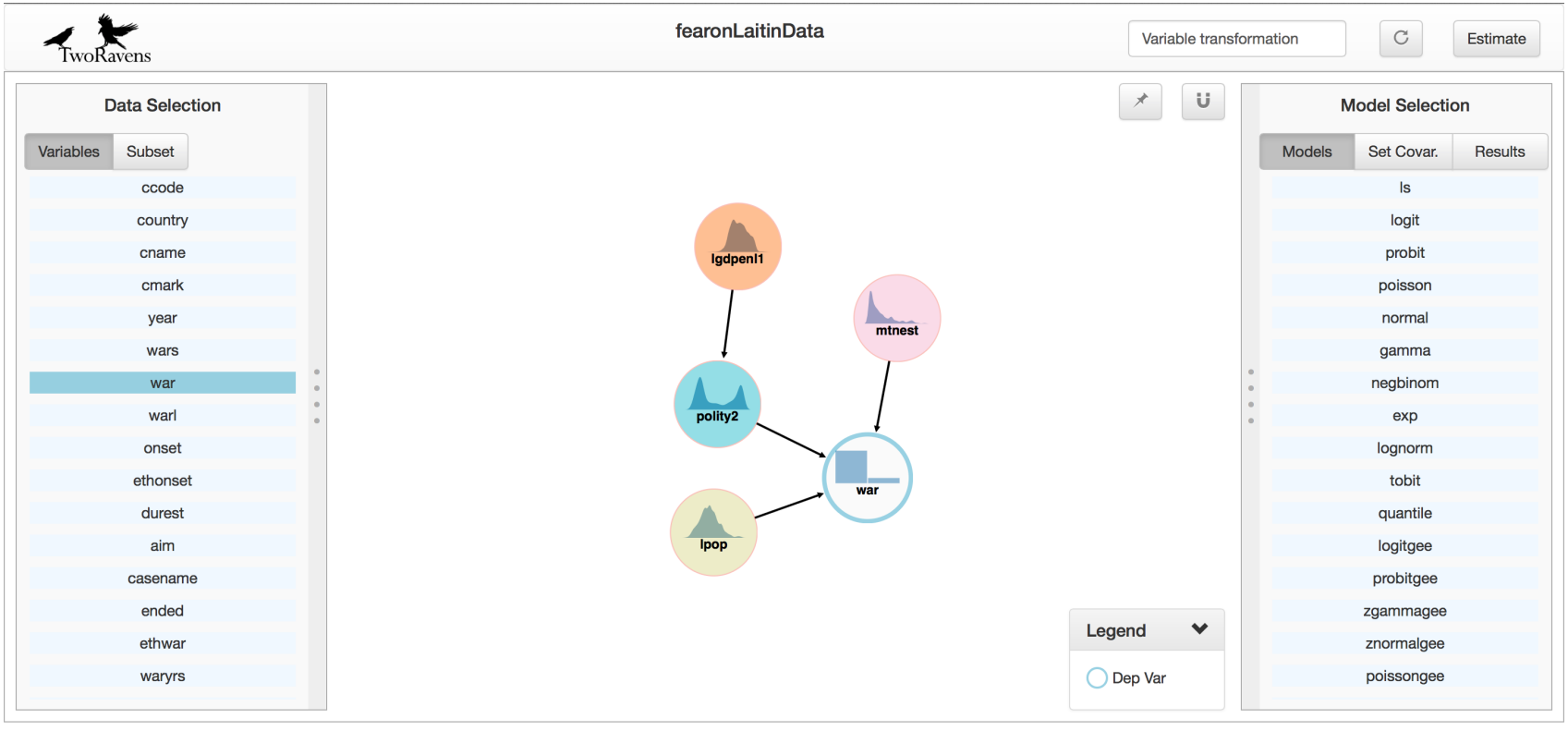
Thanks

Extra Materials

Goals and Design Principles

- Thin Client
- Graphical Representation
- Gesture Driven
- Browser Based
- Device Independent

The TwoRavens Interface



Project: `http://2ra.vn`

Example: `http://bit.ly/29Epijc`

Differential Privacy: A Primer for a Non-technical Audience*

(Preliminary version)

Kobbi Nissim[†1], Thomas Steinke[2], Alexandra Wood[3], Micah Altman[5], Aaron Bembenek[6], Mark Bun[2], Marco Gaboardi[4], David R. O'Brien[3], and Salil Vadhan[2]

[1]Department of Computer Science, Georgetown University.
kobbi.nissim@georgetown.edu.
[2]Center for Research on Computation and Society, Harvard University.
{tsteinke|mbun|salil}@seas.harvard.edu.
[3]Berkman Klein Center for Internet & Society, Harvard University.
{awood|dobrien}@cyber.law.harvard.edu.
[4]State University of New York at Buffalo.
gaboardi@buffalo.edu.
[5]Program on Information Science. Massachusetts Institute of Technology.
escience@mit.edu.
[6]School of Engineering and Applied Sciences. Harvard University.
bembenek@g.harvard.edu.

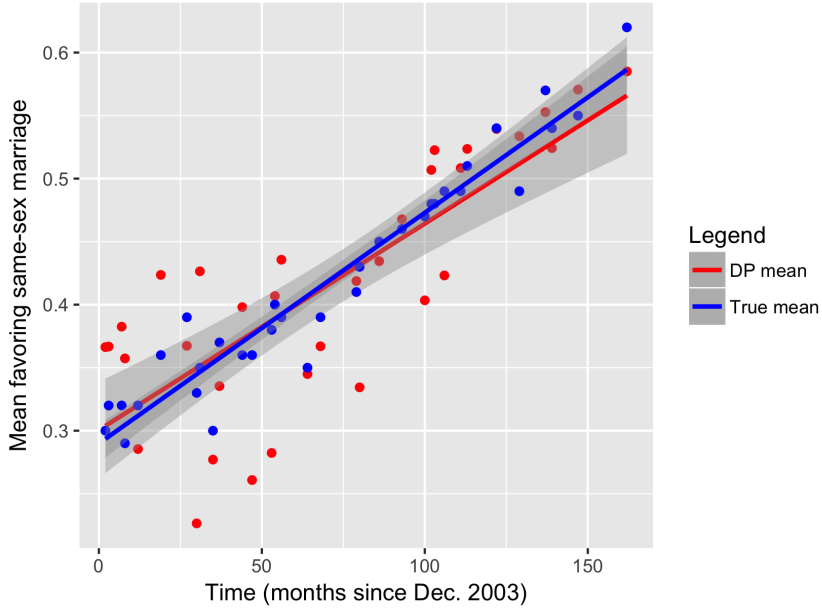
October 17, 2017

Keywords: differential privacy, data privacy, social science research

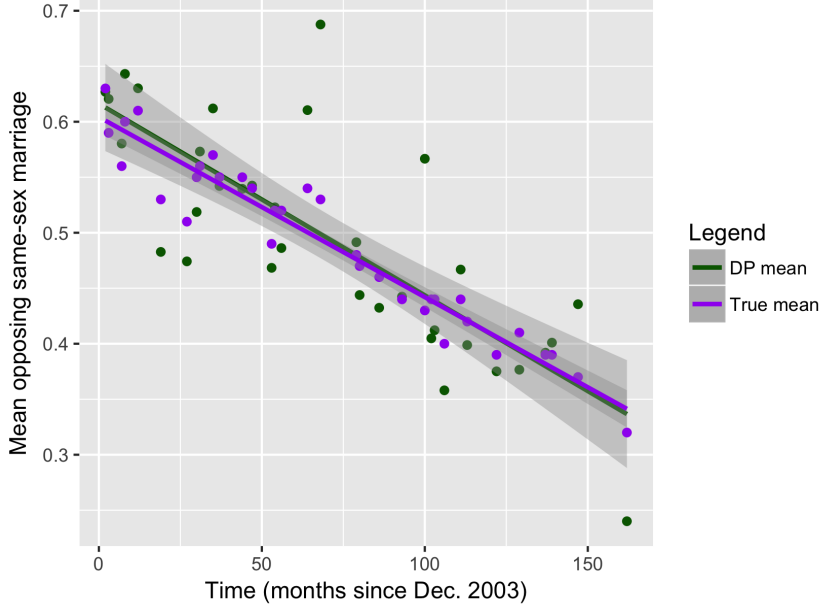
*This document is the product of a working group of the *Privacy Tools for Sharing Research Data* project at Harvard University (http://privacytools.seas.harvard.edu). The working group discussions were led by Kobbi Nissim. Kobbi Nissim, Thomas Steinke, and Alexandra Wood were the lead authors of this document. Working group members Micah Altman, Aaron Bembenek, Mark Bun, Marco Gaboardi, Kobbi Nissim, David R. O'Brien, Thomas Steinke, Salil Vadhan, and Alexandra Wood contributed to the conception of the document and to the writing. We thank Scott Bradner, Cynthia Dwork, Caper Gooden, James Honaker, Deborah Hurley, Rachel Kalmar, Georgios Kellaris, Daniel Muise, and Michel Reymond for their many valuable comments on earlier versions of this document. A preliminary version of this work was presented at the 9th Annual Privacy Law Scholars Conference (PLSC 2017), and the authors thank the participants for contributing thoughtful feedback. This material is based upon work supported by the National Science Foundation under Grant No. 1237235, as well as by the Alfred P. Sloan Foundation.

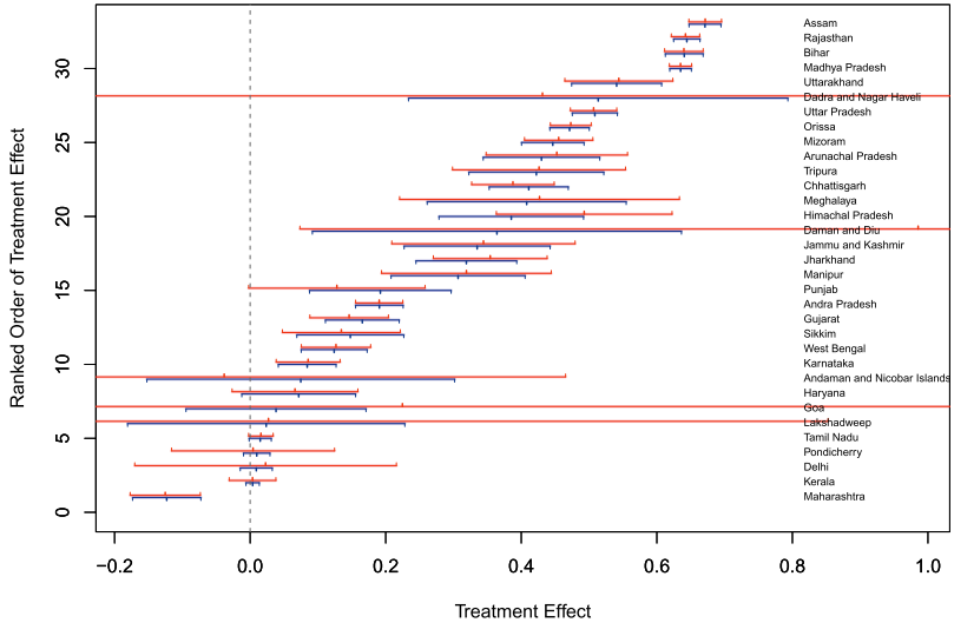
[†]Work towards this document was completed while the author was at the Center for Research on Computation and Society at Harvard University.

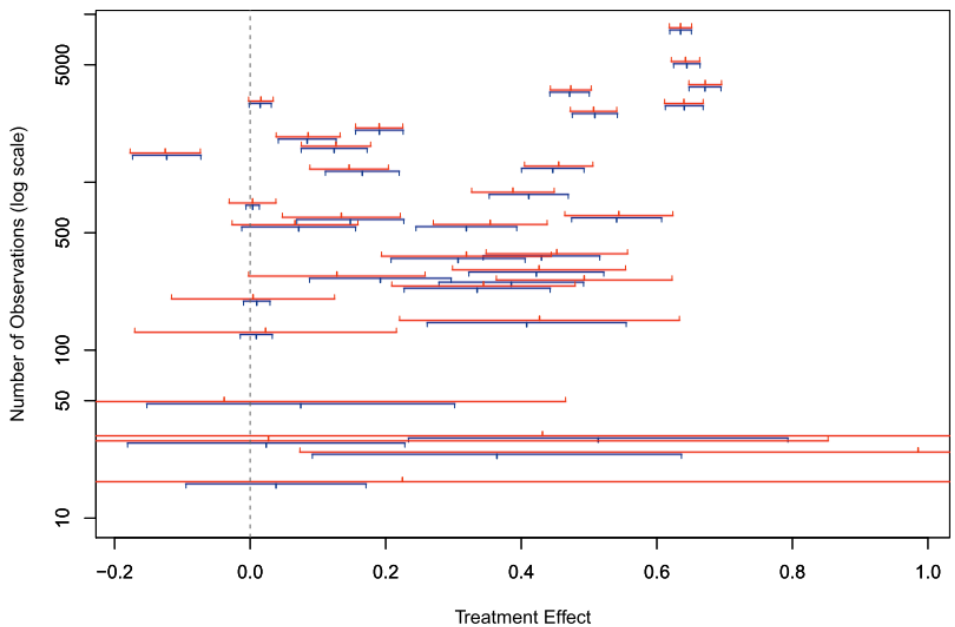
Support of same-sex marriage over time (2004-2017)



Opposition to same-sex marriage over time (2004-2017)




Ranked Order of Treatment Effect
0
5
10
15
20
25
30
−0.2
0.0
0.2
0.4
0.6
0.8
1.0
Treatment Effect
Assam
Rajasthan
Bihar
Madhya Pradesh
Uttarakhand
Dadra and Nagar Haveli
Uttar Pradesh
Orissa
Mizoram
Arunachal Pradesh
Tripura
Chhattisgarh
Meghalaya
Himachal Pradesh
Daman and Diu
Jammu and Kashmir
Jharkhand
Manipur
Punjab
Andra Pradesh
Gujarat
Sikkim
West Bengal
Karnataka
Andaman and Nicobar Islands
Haryana
Goa
Lakshadweep
Tamil Nadu
Pondicherry
Delhi
Kerala
Maharashtra


Number of Observations (log scale)
10
50
100
500
5000
−0.2
0.0
0.2
0.4
0.6
0.8
1.0
Treatment Effect