

Reviewing Sensitive Data with Differential Privacy



JEDI Workshop, November 20, 2020. Organized by Data-PASSS Alliance.

As Open as Possible, As Closed as Necessary: Empowering Transparency in Publications
Based on Sensitive Research Data

Mercè Crosas, Ph.D., Harvard University

scholar.harvard.edu/mercecrosas @mercecrosas



The Institute for Quantitative Social Science



HARVARD
UNIVERSITY

Differential Privacy tools to explore sensitive data

- A **differentially private** algorithm introduces a minimum amount of noise to released statistics to mathematically guarantee the privacy of any individual in the dataset
- **OpenDP** (<https://opendp.org>) is a **community effort** to build a trustworthy and open-source suite of **differential privacy tools** to explore sensitive data
- We are currently working on the first release of **OpenDP and Dataverse integration**

What will this mean:

- Opens up sensitive data to the research community
- Sensitive datasets findable in a Dataverse repository will be explorable through **differentially private statistics**, without ever accessing the original dataset
- Statistics included: mean, histogram, quantile, median, variance, OLS regression, logistic regression, probit regression, difference of means, unbiased privacy

Openly findable data, secure computation and storage, differentially private releases

Public Repository

Sensitive datasets discoverable via repository (only metadata open)

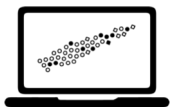
Dataverse

Blue

Green

Yellow

Data Reviewer



Differential Privacy release

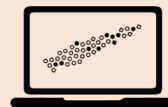
Notary Service



Digitally signed attestations
confirming DUA compliance

Data owner/depositor

Approved Secure Compute Environment to
run differential privacy statistics



OpenDP



Trusted Remote Storage Agents (TRSA) or
data enclaves



Orange

Red

Impact: Infrastructure for Privacy-Assured Computation
<https://cyberimpact.us/>

Journals' Dataverse collections will be able to support discovery, citation, and review of sensitive data

The screenshot displays the Harvard Dataverse homepage. At the top, the Harvard Dataverse logo is on the left, and navigation links (Add Data, Search, About, User Guide, Support, Sign Up, Log In) are on the right. Below the logo, a metrics bar shows '22,958,371 Downloads'. A search bar contains the text '(categoryOfDataverse:"Journal" OR dvCate' with a 'Find' button and a link to 'Advanced Search'. On the left sidebar, there are filters for 'Dataverses (92)', 'Datasets (6,424)', and 'Files (78,686)'. Below these are filters for 'Dataverse Category' (Journal (92)) and 'Publication Year' (2020 (17), 2019 (7), 2018 (13), 2017 (7), 2016 (14)). Further down are filters for 'Subject' (Social Sciences (57), Arts and Humanities (22), Medicine, Health and Life Sciences (17), Computer and Information Science (16), Law (15)). The main content area shows '1 to 10 of 92 Results'. The first five results are highlighted with red boxes: 'Executive Agreements Database (Harvard University)' (Nov 13, 2020), 'Harvard Law Review Database (Harvard University)' (Nov 13, 2020), 'Negotiation Journal (Harvard University)' (Sep 30, 2020), 'Journal of Political Institutions and Political Economy Database' (Sep 29, 2020), and 'Review of Corporate Finance Studies Database' (Sep 25, 2020). The next two results are 'Comparative Political Studies Database (University of Minnesota)' (Aug 5, 2020) and 'Journal of Slavery and Data Preservation Database (Michigan State University)' (Jul 24, 2020).

- **92 journal Dataverse collections** in Harvard Dataverse repository
- Replication datasets currently contain non-sensitive data
- With **OpenDP-Dataverse integration**, sensitive datasets will be archived in a secure storage
- **Data reviewers and users** will have **access to differential privacy statistics** of the sensitive datasets