Opt-In Statistical Disclosure Protections

Empowering Survey Respondents to Improve Data Quality

Aaron R. Williams   *Jennifer Andre*
August 2023

URBAN INSTITUTE · ELEVATE · THE · DEBATE

Table of contents

Executive Summary

Body Text style or Chapter Intro Para style here (text shown is in Chapter Intro Para). If you do not have an executive summary, remove this section.

First-Level Heading in Title Case (Heading 2 style)

Body Text style for first paragraph under a heading.

Body Text First Indent style for all subsequent paragraphs. To add an endnote, use the Insert Endnote function. Endnotes will automatically appear in the Notes section after the appendixes.[1]

Second-Level Heading in Title Case (Heading 3 style)

Body Text style for first paragraph under a heading.

Body Text First Indent style for all subsequent paragraphs.

Third-level heading; all caps is built into style (heading 4 style)

Body Text style for first paragraph under a heading.

Body Text First Indent style for all subsequent paragraphs.

Opt-In Statistical Disclosure Protections

Introduction

People generate and share data about themselves every day when they browse the web, purchase goods and services, and respond to surveys, and they should be empowered to make decisions about how these data are accessed and used. Currently, disclosure protection policies at the US Census Bureau do not allow for such empowerment – respondents to surveys like the decennial census and the American Community Survey are all subjected to disclosure protections. Data for all respondents are, by default, masked with some form of statistical disclosure control, and those who may wish to see themselves accurately reflected in the data are unable to do so. These data quality distortions may have greater impact for certain groups, such as smaller race and ethnicity groups, relative to others.

In this brief, we explore a new framework for disclosure protections that would require respondents to actively opt in to disclosure protections. Responses for those who opt in would be treated with disclosure protections, while responses for those who forego protections would remain unchanged in statistical product outputs. We present two demonstration studies, the first using an opt-in local differential privacy approach for the decennial census, and the second using an opt-in synthetic data approach for the American Community Survey. In both cases, we seek to explore the impact of varying the rate of opting in to disclosure protections on data quality, along with the associated privacy consequences. We especially examine the impact for small racial/ethnic groups, including the impact on quality and privacy if some groups opt in at higher rates than others.

We aim to test the feasibility of this potential solution path, contributing to ongoing public discussions and debate about disclosure protections and public data quality involving researchers, public data users, and other stakeholders. This solution would have wide-ranging implications, including operational changes, new outreach strategies, and many complex legal questions about Title 13 and other regulations. The findings we present here provide early evidence on the impact of turning privacy disclosure choices over to participants.

Background

Data Privacy

Utility & privacy tradeoff

Formal privacy/DP

Privacy loss budget

Traditional SDC

Synthetic data

The US Census Bureau and Disclosure Avoidance

The US Census Bureau is tasked with providing high quality data about the US and its people. These data are of enormous consequence for the public, serving as the basis for political representation, community funding and planning, and key research. Given these use cases, the accuracy and quality of Census Bureau products is crucial.

Decennial census statistical products are used for congressional apportionment, redistricting, federal funding allocations, planning and decision-making for government and business organizations, and informing many other surveys (Mather and Scommegna 2019). The American Community Survey (ACS) is used to inform federal agencies for policymaking and program delivery, state and local agencies for services like roads and schools, and nongovernmental organizations for research and analysis (United States Census Bureau 2017). In fiscal year 2015, 132 federal programs used Census Bureau data to allocate more than $675 billion in funds to state and local communities (Hotchkiss and Phelan 2017). Decennial census and ACS data are also foundational to racial equity analytics, enabling researchers to answer important research and policy questions (Axelrod, Ramos, and Bullied 2022).

In addition to conducting surveys and releasing high quality public data, the Census Bureau is also obligated to protect the confidentiality of individual respondents reflected in these data products. The Census Bureau's approach to safeguarding the identities of respondents in publicly released data is informed by its interpretation of Section 9 of Title 13 of the U.S. Code, enacted in 1954. This approach has evolved over the years, especially in response to advances in computing technologies and attack methods (Hotz and Salvo 2022). In 2018, the Census Bureau announced its intention to "modernize how we protect respondent confidentiality," including the adoption of Differential Privacy (DP) (J. M. Abowd 2018). This move was motivated by certain benefits of DP over traditional disclosure limitation, including more robust protections and greater transparency (J. Abowd et al. 2022).

For the 2020 Decennial Census, the Census Bureau updated their Disclosure Avoidance System (DAS) from traditional swapping algorithms to the differentially private TopDown Algorithm (TDA) (Bowen, Williams, and Pickens 2022). As a formally private method, the privacy protections can be quantified. In contrast, the Census Bureau has conceded that the "science does not yet exist to comprehensively implement a formally private solution for the ACS" (Daily 2022). Instead, they are currently exploring the feasibility of a fully synthetic public-use microdata file and accompanying validation server. In both cases, all respondents

are subjected to disclosure protections, even those who might otherwise prefer to see their data accurately reflected.

Opt-In Privacy Framework and Implications

In our demonstrations, we imagine a framework for disclosure protection in which respondents would be asked to actively opt in to statistical disclosure control methods. Those who do not opt-in would simply contribute their true data to statistical products. We make various simplifying assumptions and decisions, described in detail later in this report.

Such a change in framework would have significant legal ramifications such as X, Y, Z.

There are also various ethical considerations. For one, an opt-in framework would require significant outreach efforts and plain-language explanations to ensure that respondents understand what they are or are not opting into. Further, careful attention must be paid to the impact of one respondent choosing to forego protections on the privacy risks of respondents who do opt in.

Demonstration 1: Local Differential Privacy for the Decennial Census

The Census Bureau deployment of DP for the 2020 Decennial Census uses a global privacy approach in which tabulated cells of confidential responses in a series of data tables are infused with noise by a central curator (the Census Bureau). All census respondents are automatically subjected to the DAS, even those who might otherwise wish to see their data reflected accurately, without any noise. Further, the noise that is injected into tabulated data cells is independent of the size of the population in the cell. In effect, there is more relative error added for small groups than for larger ones. This could lead to worse data quality for small groups such as some racial/ethnic groups and, as a result of inaccurate representation in the data, these groups could receive inadequate funding and incorrect research findings.

A primary benefit of a formal privacy approach like the DAS is that the overall privacy loss budget can be transparently quantified with the metric . Further, the mathematical properties of DP allow for some individuals to forego privacy protections without decreasing other respondents' protections.

Local Differential Privacy

To allow for individual-level opt-in, we move from a central DP approach, in which the Census Bureau as a data curator would add noise to all respondents, to a local DP approach, allowing for some respondents to opt in and others to forego disclosure protections. Typically, a local model assumes that a central curator cannot be trusted, and so a respondent adds noise to their data before sending it to the curator. For this use case, we can imagine a slight variation on this approach in which the trusted Census Bureau still receives all data in its confidential form, and then infuses noise only for respondents who opt in.

Many local DP mechanisms are based on the concept of Randomized Response, first proposed by S. L. Warner in 1965 (Warner 1965). The central idea is that a survey respondent flips a coin, and the result of the coin flips determines if they answer a yes/no question with the true answer or not. The randomization of the coin flip infuses the noise that grants disclosure protections (Near and Abuah 2022).

We use Generalized Random Response (GRR) for our use case, allowing us to move from a binary coin flip to a setting with higher cardinality. With GRR, we turn the entire domain of potential responses into a histogram and randomly switch observations based on a rate determined by the privacy loss budget, . We then tabulate a resulting histogram of counts and apply an adjustment to account for the randomly perturbed responses (Wang et al. 2020).

Data

For this demonstration, we use person-level records from the 2010 Decennial Census Stateside Public Use Microdata Sample. This sample contains records representing 10 percent of housing units, and the people residing in them, along with 10 percent of people living in group quarters. We restrict our sample to Washington, DC and Iowa because the former has two large racial/ethnic groups, while the latter is more homogeneous. These data contain demographic and household characteristics about respondents, including age, race, ethnicity, and sex.

Simulations

For our simulation approach, we run iterations of a disclosure mechanism to generate noisy histograms of counts for a set of defined attributes. We focus on two disclosure mechanisms to compare a standard global approach to a local opt-in approach. The first is a Laplace sanitizer, a global method in which cells are infused with noise from a Laplace distribution. The Laplace distribution is centered at zero and the variability is the ratio of the privacy loss budget, , over the l_1-global sensitivity of the statistic [Dwork et al. (2006)](Williams and Bowen 2023). The second is the previously described GRR method, a local method in

which individuals who opt in to disclosure protections report a true response with probability $p = \frac{e}{e+d1}$.
Otherwise, the record is randomly replaced with another combination of fields.

We then evaluate these results using bias and accuracy metrics, comparing the noisy histograms to the true values. We use mean percent error to evaluate bias, or the tendency for noisy estimates to systematically move in one direction relative to the true values. We use absolute mean percent error to evaluate accuracy, or the closeness of noisy estimates to the true values.

The specifications for our simulations are as follows. For each combination of specifications, we run 100 iterations of each disclosure mechanism.

- Scenarios: the set of grouping attributes for the resulting histogram frequencies
  » Scenario 1 (cardinality = 2)
    * Hispanicity: Hispanic or Latino, Not Hispanic or Latino
  » Scenario 2 (cardinality = 24)
    * Age bucket: Child (0-17), Adult (18-64), Senior (65+)
    * Race/Ethnicity: White alone, Black or African American alone, Other alone, or Hispanic or Latino (any race)
    * Sex: Male, Female
- Privacy loss budget,
  » 1
  » 5
  » 10
  » 20
- Opt-in rate: the probability that respondents opt in to disclosure protections
  » 0.01
  » 0.1
  » 0.5
  » 0.9
  » 1

Results and Discussion

Local DP Methods Result in Overall Lower Accuracy than Global Methods

For Scenario 1, we focus primarily on results allowing us to compare the performance of the local GRR method to the central Laplace method. With a cardinality of just 2 (Hispanic or Latino, Not Hispanic or Latino), this scenario allows for the most similar comparison with the global method (in which epsilon is

allocated to just one statistic).

Figure 1 shows the distribution of bias metrics from our simulations at the defined levels of and opt in rate. Both the local and central methods are unbiased, with the distribution of mean percent error values centered around zero.
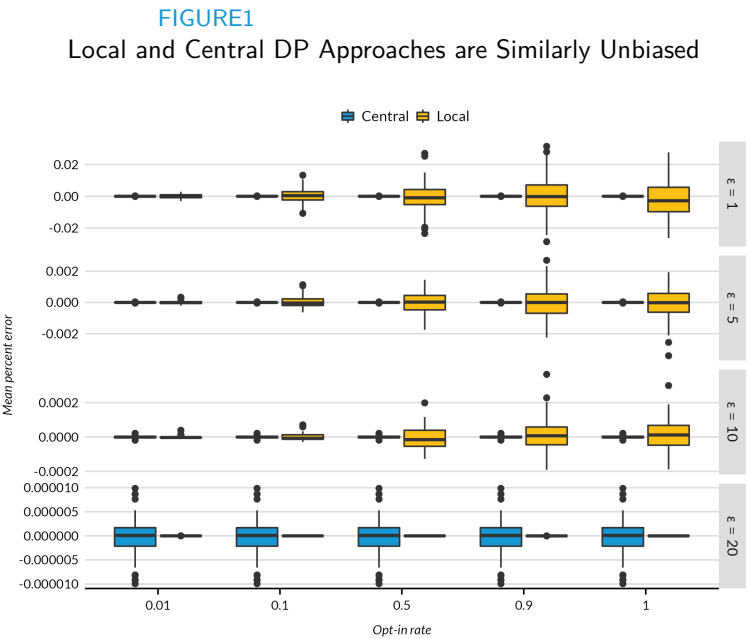
FIGURE1

Local and Central DP Approaches are Similarly Unbiased

Figure 2 shows the distribution of accuracy metrics from our simulations at the defined levels of epsilon and opt in rate.

FIGURE2

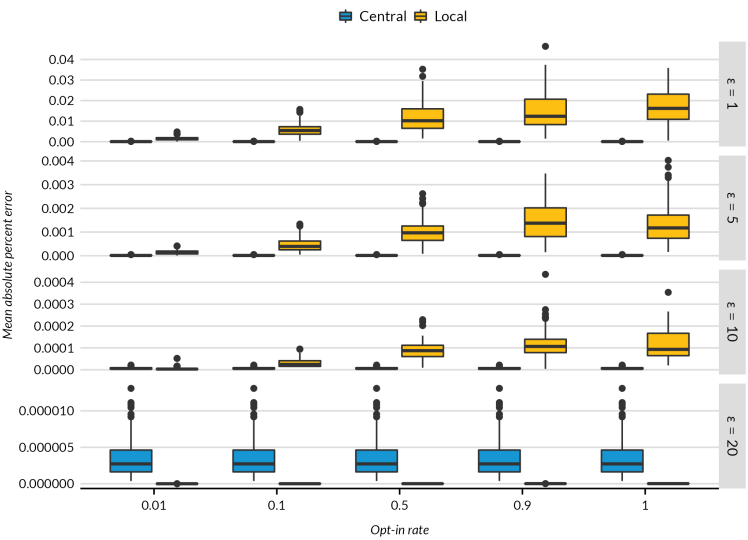Local Method Outperforms Central Method Only with Very High Privacy Loss Budget

Figure 2 demonstrates two key takeaways about the accuracy of these methods. First, the opt-in framework approach does improve the overall accuracy of the local GRR method. As we decrease the level of opt in, the width of the mean percent error distribution shrinks and moves closer to zero. However, the second key takeaway is that the central method significantly outperforms the local method in terms of accuracy at nearly every tested level of and opt in rate, even with very small opt in rates. The local method only outperforms the central method with a very high privacy loss budget of = 20, and the errors for both methods are very small for that level of privacy loss anyway.

While the opt-in local approach does improve the accuracy of estimates with lower levels of opt in, this improvement alone is unfortunately not enough to justify a switch from a central model to a local model. Existing local DP methods cannot offer the same level of accuracy as central methods, especially for datasets with even higher cardinality. However, the potential to improve data quality results with a local method and opt-in framework motivates greater focus on developing local DP methods in the future.

Opt-in Privacy Offers the Potential to Improve Data Quality for Small Groups

Although existing local DP methods may be disappointing for overall accuracy, an opt-in local DP framework still offers the potential to improve data quality for small groups. Data quality may be especially improved for groups that opt-in at relatively lower rates than others. For Scenario 2, we focus on results allowing us to compare differences in data quality by racial/ethnic group.

Figures 3 and 4 show the distribution of accuracy results for the specified opt in rates for each racial/ethnic group (using = 1), separately by state.

FIGURE3
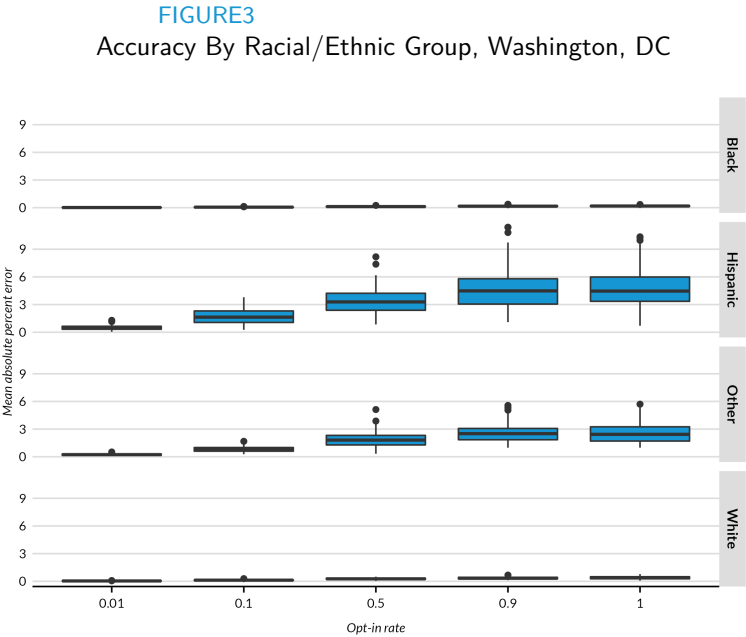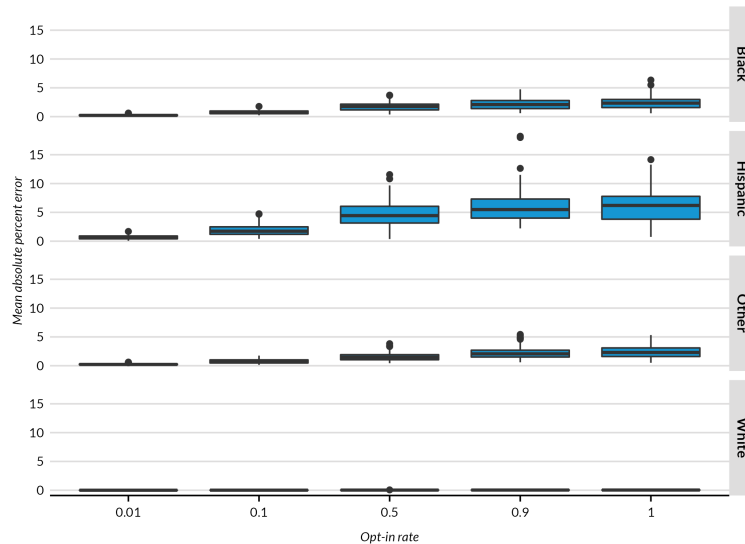Accuracy By Racial/Ethnic Group, Washington, DC

FIGURE4

Accuracy By Racial/Ethnic Group, Iowa

According to the 2010 Census Redistricting Data (Public Law 94-171) Summary File, the population of Washington DC was 38% white, non-Hispanic and 51% Black, non-Hispanic, and the population of Iowa was 91% white, non-Hispanic. For both states, mean percent error is smallest for these relatively large groups, reflecting the larger sample sizes. Error tends to be relatively larger, and with larger spreads, for the smaller groups in both places.

The opt-in framework offers a solution path to improve data accuracy for these smaller racial/ethnic groups. For example, the median absolute percent error for the Hispanic group is roughly 3.5% in Washington, DC and 6% in Iowa when there is 100% opt in, or when all respondents are subjected to disclosure protections. These error values shrink to about 1.5% and 2%, respectively, with a group opt-in rate of 10%. Given the properties of formal privacy, the privacy protections afforded to those who opt-in are unaffected by those who choose to forego protections.

With an opt-in disclosure framework, the US Census Bureau and community groups could engage in outreach efforts, especially to smaller groups, to help respondents understand the implications of foregoing disclosure protections, both for their privacy but also for the wide-ranging impacts of improving their data quality. This type of outreach could result in better data quality for these groups, with positive downstream impacts on representation and funding allocations to communities.

All in all, existing local DP methods generate protected data of overall lower accuracy than data generated by central models. However, this demonstration shows the potential of local DP to improve data accuracy for small groups, while still protecting privacy, with an opt-in DP framework. This use case motivates further development of local DP methods and opt in experimentation to improve accuracy results.

Demonstration 2: Synthetic Data for the American Community Survey

Synthetic Data

Data

Simulations

Results and Discussion

Conclusion

Appendix Letter. Appendix Title in Title Case

Use the same text styles you used in the main report.

Notes

[1] Endnotes should appear automatically under the Notes heading. If theyre showing up somewhere else, ask your editor or your centers Word expert for assistance.

About the Authors

Aaron R. Williams but the rest of the text lightface. Use Author Bios–First style for the introductory paragraph of each bio. You can paste your bio from your author page on the Urban website (and condense it if needed) here.

If your bio is more than one paragraph long, use Author Bios–Additional for any subsequent paragraphs. This style suppresses spacing between paragraphs.

Author bios no longer include photos.

Jennifer Andre but the rest of the text lightface. Use Author Bios–First style for the introductory paragraph of each bio. You can paste your bio from your author page on the Urban website (and condense it if needed) here.

If your bio is more than one paragraph long, use Author Bios–Additional for any subsequent paragraphs. This style suppresses spacing between paragraphs.

Author bios no longer include photos.

Abowd, John M. 2018. "Protecting the Confidentiality of Americas Statistics: Adopting Modern Disclosure Avoidance Methods at the Census Bureau."

https://www.census.gov/newsroom/blogs/research-matters/2018/08/protecting_the_confi.html.

Abowd, John, Robert Ashmead, Ryan Cumings-Menon, Simson Garfinkel, Micah Heineck, Christine Heiss, Robert Johns, et al. 2022. "The 2020 Census Disclosure Avoidance System TopDown Algorithm." *Harvard Data Science Review*, no. Special Issue 2 (June). https://doi.org/10.1162/99608f92.529e3cb9.

Axelrod, Judah, Karolina Ramos, and Rebecca Bullied. 2022. "Opportunities and Challenges in Using Private-Sector Data for Racial Equity Analysis."

Bowen, Claire McKay, Aaron R Williams, and Madeline Pickens. 2022. "Decennial Disclosure: An Explainer on Formal Privacy and the TopDown Algorithm."

Daily, Donna. 2022. "Disclosure Avoidance Protections for the American Community Survey."

https://www.census.gov/newsroom/blogs/random-samplings/2022/12/disclosure-avoidance-protections-acs.html.

Dwork, Cynthia, Frank McSherry, Kobbi Nissim, and Adam Smith. 2006. "Calibrating Noise to Sensitivity in Private Data Analysis." In, edited by Shai Halevi and Tal Rabin, 3876:265–84. Berlin, Heidelberg: Springer Berlin Heidelberg. http://link.springer.com/10.1007/11681878_14.

Hotchkiss, Marisa, and Jessica Phelan. 2017. "Uses of Census Bureau Data in Federal Funds Distribution: A New Design for the 21st Century," September.

https://www2.census.gov/programs-surveys/decennial/2020/program-management/working-papers/Uses-of-Census-Bureau-Data-in-Federal-Funds-Distribution.pdf.

Hotz, V. Joseph, and Joseph Salvo. 2022. "A Chronicle of the Application of Differential Privacy to the 2020 Census." *Harvard Data Science Review*, June. https://doi.org/10.1162/99608f92.ff891fe5.

Mather, Mark, and Paola Scommegna. 2019. "Why Is the u.s. Census so Important?" March.

https://www.prb.org/resources/importance-of-u-s-census/.

Near, Joseph P, and Chiké Abuah. 2022. *Programming Differential Privacy*.

United States Census Bureau. 2017. "American Community Survey Information Guide," October.

Wang, Teng, Xuefeng Zhang, Jingyu Feng, and Xinyu Yang. 2020. "A Comprehensive Survey on Local Differential Privacy Toward Data Statistics and Analysis." *Sensors* 20 (24): 7030. https://doi.org/10.3390/s20247030.

Warner, Stanley L. 1965. "Randomized Response: A Survey Technique for Eliminating Evasive Answer Bias." *Journal of the American Statistical Association* 60 (309): 63–69. https://doi.org/10.1080/01621459.1965.10480775.

Williams, Aaron R., and Claire McKay Bowen. 2023. "The Promise and Limitations of Formal Privacy." *WIREs Computational Statistics*, May, e1615. https://doi.org/10.1002/wics.1615.

URBAN INSTITUTE · ELEVATE · THE · DEBATE

500 L'Enfant Plaza SW
Washington, DC 20024

www.urban.org