Differential Privacy: A Modern Approach to Protecting Your Confidentiality

Differential privacy is the scientific term for a disclosure avoidance framework used to protect the confidentiality of respondents' data in our published data products. It is part of a broader family of disclosure avoidance approaches, known as formal privacy, that precisely quantify the disclosure risk associated with each and every statistic published.

More Precise Protection Against Digital-Age Threats

Differentially private disclosure avoidance mechanisms work by treating the data we publish with a controlled amount of statistical noise—small random additions or subtractions—so that no one can reliably associate the published data with a specific person or household. The use of statistical noise to protect confidentiality is not new; the U.S. Census Bureau has used similar techniques for decades.

Differential privacy is the best science available to protect 2020 Census respondent confidentiality, while minimizing the impact on statistical validity. It is particularly well-suited for large data products like those from a detailed decennial census. And with ever-advancing technology, the threats to disclosure will only grow with time.

Differential Privacy Allows Customized Solutions for Different Data Needs.

Differential privacy offers a significant advantage over the disclosure avoidance methods used in past censuses in that it allows us to tune the balance between confidentiality and accuracy more delicately than ever before. Where necessary, the mechanism can be adjusted to add less noise to specific statistics, thus making those particular results more accurate.

Decisions about how much noise to add and where to add it creates a delicate balance between the usefulness of the data and the need to protect confidentiality. If we add less noise to certain results (e.g., number of people aged 37 in a census tract) to improve accuracy, then we must compensate by adding more noise to certain other results to ensure confidentiality.

We Follow the Science to Choose the Most Appropriate Protections for Each Data Release.

Given modern-day confidentiality threats, differential privacy is the best science-based approach for 2020 Census results. However, it is just one tool in our disclosure avoidance toolbox. We continue to tailor our methods to each of the data products we release. Where appropriate, we are also strengthening our legacy methods such as swapping, aggregation, and suppression. In every case, we will follow the science to ensure that we are protecting the confidentiality of all responses, while still releasing usable quality statistics from Census Bureau data products.

United States® Census Bureau

U.S. Department of Commerce
U.S. CENSUS BUREAU
census.gov

v. 2023.05.01