# Differential Privacy and the 2020 Census

The mission of the U.S. Census Bureau is to provide quality data about the people and economy of the United States. Protecting privacy and ensuring accuracy are, and have always been, core to this mission. The Census Bureau is required by law (Title 13 of the U.S. Code) to ensure that information about any specific individual, household, or business is never revealed, even indirectly, through our published statistics. The quality and accuracy of Census Bureau statistics depend on the public's trust and participation.

The Census Bureau is modernizing its approach to privacy protection for the 2020 Census. We're using a statistical method called differential privacy to mask information about individuals while letting us share important statistics about communities.

## What is differential privacy?

Differential privacy is a mathematical approach inspired by modern cryptography principles that disguises an individual's identity in published data. Similar to protection methods used in recent censuses, differential privacy adds statistical noise (slight alterations) to data to create uncertainty about the identities of the people behind the numbers. However, unlike past methods, this modernized approach allows the Census Bureau to precisely control the amount of statistical noise that's added to strike a balance between data utility and personal privacy.

## Why are we using differential privacy?

Differential privacy is a modern safeguard against today's privacy threats. Supercomputers can now find and match data from multiple databases to identify personal information. That's particularly true if you live in a small area and are a different race or ethnicity from your neighbors. It can be easier to pick you out of a crowd. Serious threats to privacy exist today that didn't exist 10 years ago during the last census. We must use new techniques to continue to protect people's privacy. Given the scale of today's privacy threats, reusing the past methods would require significantly larger distortions in the published data, rendering much of the data unfit for use.

## Stakeholder feedback and engagement is key to ensuring that 2020 Census results protect privacy while delivering the detailed, useful statistics communities need.

We are making hard but data-driven decisions to balance the level of detail we can provide in our published statistics, especially for smaller geographic areas and population groups, while protecting the privacy of individuals. We've relied on the extensive feedback of independent experts and data users to help us fine-tune the new, differentially private system, called the "Disclosure Avoidance System," at every stage in development.

## Differential privacy is not applied to the apportionment count.

State population counts used to apportion seats in the U.S. House of Representatives are total counts of residents and overseas residents for each state. Neither differential privacy nor any other form of statistical noise is applied to those counts.

More information about 2020 Census data products and disclosure avoidance modernization is available at <www.census.gov/programs-surveys/decennial-census/decade/2020/planning-management/process/disclosure-avoidance.html>.

United States® Census 2020

D-FS-GP-EN-047
July 2021