

The Republican Plan to Reform the Census Could Put Everyone's Privacy at Risk

Vittoria Elliott — Read time: 9 minutes

President Donald Trump and the Republican Party have spent the better part of the president's second term [radically reshaping](#) the federal government. But in recent weeks, the GOP has set its sights on taking another run at an old target: the US census.

Since the first Trump administration, the right has sought to [add a question](#) to the census that captures a respondent's immigration status and to [exclude noncitizens](#) from the tallies that determine how seats in Congress are distributed. In 2019, the Supreme Court [struck down](#) an attempt by the first Trump administration to add a citizenship question to the census.

But now, a little-known algorithmic process called "[differential privacy](#)," created to keep census data from being used to identify individual respondents, has become the right's latest focus. WIRED spoke to six experts about the GOP's ongoing effort to falsely allege that a system created to protect people's privacy has made the data from the 2020 census inaccurate.

If successful, the campaign to get rid of differential privacy could not only radically change the kind of data made available, but could put the data of every person living in the US at risk. The campaign could also discourage immigrants from participating in the census entirely.

The Census Bureau regularly publishes anonymized data so that policymakers and researchers can use it. That data is also sensitive: Conducted every 10 years, the census counts every person living in the United States, citizen and noncitizen alike. The data includes detailed information like the race, sex, and age, as well the languages they speak, their home address, economic status, and the number of people living in a house. This [data is used](#) for allocating the federal funds that support public services like schools and hospitals, as well as for how a state's population is divided up and represented in Congress. The more people in a state, the more Congressional representation—and more votes in the Electoral College.

As computers got increasingly sophisticated and data more abundant and accessible, census employees and researchers realized the data published by the Census Bureau could be reverse engineered to identify individual people. According to [Title XIII of the US Code](#), it is illegal for census workers to publish any data that would identify individual people, their homes, or businesses. A government employee revealing this kind of information [could be punished](#) with thousands of dollars in fines or even a possible prison sentence.

For individuals, this could mean, for instance, someone could use census data without differential privacy to identify transgender youth, according to [research from the University of Washington](#).

For immigrants, the prospect of being reidentified through census data could “create panic among noncitizens as well as their families and friends,” says Danah Boyd, a census expert and the founder of Data & Society, a nonprofit research group focused on the downstream effects of technology. LGBTQ+ people might not “feel safe sharing that they are in a same-sex marriage. There are plenty of people in certain geographies who do not want data like this to be public,” she says. This could also mean that information that might be available only through something like a search warrant would suddenly be

obtainable. “Unmasking published records is not illegal. Then you can match it to large law enforcement databases without actually breaching the law.”

Differential privacy keeps that data private. It's a mathematical framework whereby a statistical output can't be used to determine any individual's data in a dataset, and the bureau's algorithm for differential privacy is called TopDown. It injects “noise” into the data starting at the highest level (national), moving progressively downward. There are certain constraints placed around the kind of noise that can be introduced—for instance, the total number of people in a state. But other demographic characteristics, like race or gender, are reassigned to individual records within a set tranche of data. This way, the overall number of people with a certain characteristic remains constant, while the characteristics associated with any one record don't describe an individual person.

Most Popular

-
-
-
-
-

“Differential privacy solves a particular problem, which is if you release a lot of information, a lot of statistics, based on the same set of confidential data, eventually somebody can piece together what that confidential data had to be,” says Simson Garfinkel, former senior computer scientist for confidentiality and data access at the Census Bureau.

Differential privacy was first used on data from the 2020 census. Even though one couldn't identify a specific individual from the data, “you can still get an

accurate count on things that are important for funding and voting rights,” says Moon Duchin, a professor of computer science and data science at the University of Chicago who worked with census data to inform electoral maps in Alabama. The first use of differential privacy for the census happened under the Trump presidency, though the reports themselves were published after he left office. Civil servants, not political appointees, are the ones responsible for determining how census data is collected and analyzed. Emails [obtained by the Brennan Center](#) later claimed that the officials at the Census Bureau, overseen by then-Commerce Secretary Wilbur Ross, expressed an “unusually high degree” of interest in the “technical matters” of the process, which deputy director and COO of the bureau Ron Jarmin called “unprecedented.”

It's this data from the 2020 census that Republicans have taken issue with. On August 21, the Center for Renewing America, a right-wing think tank founded by Russ Vought, currently the director of the US Office of Management and Budget, [published a blog post](#) alleging that differential privacy “may have played a significant role in tilting the political scales favorably toward Democrats for apportionment and redistricting purposes.” The post goes on to acknowledge that, even if a citizenship question was added to the census—which Trump [attempted](#) during his first administration—differential privacy “algorithm will be able to mask characteristic data, including citizenship status.”

Duchin and other experts who spoke to WIRED say that differential privacy does not change apportionment, or how seats in Congress are distributed—[several red states](#), including Texas and Florida, gained representation after the 2020 census, while blue states like California lost representatives.

On August 28, Republican representative August Pfluger introduced the [COUNT Act](#). If passed, it would add a citizenship question to the census and force the Census Bureau to “cease utilization of the differential privacy

process.” Pfluger’s office did not immediately respond to a request for comment.

“Differential privacy is a punching bag that's meant here as an excuse to redo the census,” says Duchin. “That is what's going on, if you ask me.”

Got a Tip?

Are you a current or former government employee who wants to talk about what's happening? We'd like to hear from you. Using a nonwork phone or computer, contact the reporter securely on Signal at Vittoria89.82.

On October 6, Senator Jim Banks, a Republican from Indiana, [sent a letter](#) to Secretary of Commerce Howard Lutnick, urging him to “investigate and correct errors from the 2020 Census that handed disproportionate political power to Democrats and illegal aliens.” The letter goes on to allege that the use of differential privacy “alters the total population of individual voting districts.” Similar to the COUNT Act and the Renewing America post, the letter also states that the 2030 Census “must request citizenship status.”

Most Popular

-
-
-
-
-

Peter Bernegger, a Wisconsin-based “election integrity” activist who is facing a criminal [charge](#) of simulating the legal process for allegedly falsifying a subpoena, [amplified Banks’ letter on X](#), alleging that the use of differential

privacy was part of “election rigging by the Obama/Biden administrations.” Bernegger’s post was viewed more than 236,000 times.

Banks’ office and Bernegger did not immediately respond to a request for comment.

“No differential privacy was ever applied to the data used to apportion the House of Representatives, so the claim that seats in the House were affected is simply false,” says John Abowd, former associate director for research and methodology and chief scientist at the United States Census Bureau. Abowd oversaw the implementation of differential privacy while at the Census Bureau. He says that the data from the 2020 census has been successfully used by red and blue states, as well as redistricting commissions, and that the only difference from previous census data was that no one would be able to “reconstruct accurate, identifiable individual data to enhance the other databases that they use (voter rolls, drivers licenses, etc.).”

With a possible addition of the citizenship question, proposed by both Banks and the COUNT Act, Boyd says that census data would be even more sensitive, because that kind of information is not readily available in commercial data. “Plenty of data brokers would love to get their hands on that data.”

Shortly after Senator Banks published his letter, Abowd found himself in the spotlight. On October 9, the X account @amuse posted a [blog-length post](#) alleging that Abowd was the bureaucrat who “stole the House.” The post also alleged, without evidence, that the census results meant that “Republican states are projected to lose almost \$90 billion in federal funds across the decade as a result of the miscounts. Democratic states are projected to gain \$57 billion.” The account has more than 666,000 followers, including billionaire [Elon Musk](#), venture capitalist [Marc Andreessen](#), and US pardon attorney Ed

Martin. (Abowd told WIRED he was “keeping an eye” on the post, which was viewed more than 360,000 times). That same week, America First Legal, the conservative nonprofit founded by now deputy chief of staff for policy Stephen Miller, [posted](#) about a [complaint the group had recently filed in Florida](#), challenging the 2020 census results, alleging they were based upon flawed statistical methods, one of which was differential privacy.

The results of all this, experts tell WIRED, are that fewer people will feel safe participating in the census and that the government will likely need to spend even more resources to try to get an accurate count. Undercounting could lead to skewed numbers that could impact everything from congressional representation to the amount of funding a municipality might receive from the government.

Neither the proposed COUNT Act nor Senator Banks' letter outlines an alternative to differential privacy. This means that the Census Bureau would likely be left with two options: Publish data that could put people at risk (which could lead to legal consequences for its staff), or publish less data. “At present, I do not know of any alternative to differential privacy that can safeguard the personal data that the US Census Bureau uses in their work on the decennial census,” says Abraham Flaxman, an associate professor of health metrics sciences at the University of Washington, whose team conducted the study on transgender youth.

Most Popular

-
-
-
-
-

Getting rid of differential privacy is not a “light thing,” says a Census employee familiar with the bureau’s privacy methods and who requested anonymity because they were not authorized to speak to the press. “It may be for the layperson. But the entire apparatus of disclosure avoidance at the bureau has been geared for the last almost 10 years on differential privacy.” According to the employee, there is no immediately clear method to replace differential privacy.

Boyd says that the safest bet would simply be “what is known as suppression, otherwise known as ‘do not publish.’” (This, according to Garfinkel, was the backup plan if differential privacy had not been implemented for the 2020 census.)

Another would be for the Census Bureau to only publish population counts, meaning that demographic information like the race or age of respondents would be left out. “This is a problem, because we use census data to combat discrimination,” says Boyd. “The consequences of losing this data is not being able to pursue equity.”

Update: 10/30/2025, 3:05 PM EDT: WIRED has clarified its description of differential privacy.