Wired Article Claim and Response

By: Wade Miller and Andrew White

On October 8, 2025, *WIRED* published an article entitled "The Republican Plan to Reform the Census Could Put Everyone's Privacy at Risk." It is so flawed that it requires an extended response. While differential privacy and census policy are complex topics, the "experts" cited provided technical falsehoods or out-of-context propaganda, with the implication being an intent to mislead the public about differential privacy and its impacts. Because of the sheer volume of misinformation that resulted, we have structured what follows in a "claim and response" format. We hope the editors at *WIRED* will issue a series of corrections to the piece or pull the article entirely to prevent its misinformation from spreading further online.

Claim: The Republican Plan to Reform the Census Could Put Everyone's Privacy at Risk: A little-known algorithmic process called "differential privacy" helps keep census data anonymous. Conservatives want it gone.

Response: The title of this article implies that conservatives want no privacy protections in the census process. This claim is never substantiated in the piece, and indeed, the article itself admits that other options exist. Differential privacy was first used in the 2020 Census, which also happened to be the most inaccurate census in modern American history. Every census from 1960 through 2010 used different approaches—often "swapping" characteristics with other individuals—to protect personally identifiable information. Suggestions that these measures, which were used for half a century, were inadequate are mere speculation. The first laws regarding data privacy in the census date back to at least 1880, and the modern protections were codified in 1954. Some variation of swapping was used in 1990, 2000, and 2010. If the argument is that digital capabilities are advancing too fast for swapping to remain a satisfactory option, then data privacy plans must also comport with the constitutional principles the census is designed to advance, a metric by which current differential privacy methods fall short.

Claim: 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.

Response: If redistricting is what was meant by "distributed," then this statement is correct. The American republic belongs to its citizens and its citizens alone. The citizenship question prevents noncitizens, especially illegal immigrants, who have broken American immigration laws, from having the same impact as, or arguably an even greater impact on, political representation than the American people. And why should lawful permanent residents impact the creation of districts meant to represent voting citizens? Might there be some legitimate constitutional questions and concerns about that situation? If by "distributed" the process of apportionment is meant, then this statement is imprecise and speculative. Court precedent would dictate that lawful permanent residents would need to be counted for purposes of apportionment, but there are legitimate constitutional arguments that illegal aliens do not need to be counted for the purposes of apportionment.

Claim: In 2019, the Supreme Court struck down an attempt by the first Trump administration to add a citizenship question to the census.

Response: This is a significantly misleading claim. The first attempt to add a citizenship question to the census was not struck down on substantive grounds but rather because the Supreme Court determined that the administration's reasoning was "arbitrary and capricious" since it did not properly follow the Administrative Procedures Act. In the eyes of the court, the opinion said little more than "This was not done the correct way. Try again." It is troubling that this article failed to include that context. The average person who reads that claim will come away thinking that the Supreme Court has already determined that residency and citizenship status cannot be asked, which is categorically false.

Claim: 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.

Response: Indisputably, the 2020 Census was the most inaccurate and unreliable in modern American history. Fourteen states had statistically significant overcounts or undercounts, resulting in *at least* six seats in the House of Representatives being illegitimately awarded to Democrats. The census acknowledged these counting

errors in its Post-Enumeration Survey in 2022. Additionally, the census's use of differential privacy moved populations around below statewide totals in a manner that researchers at Harvard University in a 2021 [study](#) concluded was likely unconstitutional. The mentioned "experts" are hiding behind a technicality by only pointing to statewide data and ignoring subdivisions below that level. But again, even those statewide totals were the most inaccurate in recent history.

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

Response: This is hyperbolic nonsense. There are multiple methods for providing data privacy at statistically similar levels; differential privacy is just one such method. The census has clear constitutional importance, and the data is relied upon to carry out other constitutional duties. Setting aside the unqualified implication that moving away from differential privacy would risk privacy protections, statutory requirements cannot require the use of processes that would violate the Constitution. Processes that flow from statutory privacy requirements *must* comply with constitutional requirements. If a privacy method violates constitutional requirements, it is de facto impermissible. Differential privacy methods do not clear these threshold considerations and should never have been implemented in the first place, especially in place of other privacy methods that do not interfere with the Constitution.

Claim: 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.

Response: The claim stumbles upon an important point: Census data is tied to federal funding formulas. For states, counties, cities, municipalities, etc., to receive funding levels that reflect their actual populations, the census must provide accurate population data. However, differential privacy is at direct odds with this aim because it specifically moves population data across the state, with permissible variation rates of nearly 20 percent of the population, according to some reports. If an important goal of the census is to provide accurate data for federal funding formulas, differential privacy, *by design*, makes that goal far more difficult. It remains an open question, though it is very doubtful, whether the correct data is available to all relevant federal, state, and local agencies. Indeed, the use of differential privacy may be grounds for thousands of government subdivisions to sue the Commerce

Department over improper funding levels. Regardless of one's opinion on the inclusion of the citizenship question in the census, the use of differential privacy creates massive problems for funding formulas.

Claim: The more people in a state, the more Congressional representation—and more votes in the Electoral College.

Response: This is correct, but there is a legitimate legal debate over who should be counted for apportionment and, therefore, how the Electoral College is impacted from state to state. If one holds the viewpoint that it is unconstitutional to count illegal aliens for the purposes of apportionment, let alone for the purposes of redistricting, then there is a constitutional obligation to ascertain the legal status of a respondent. Implying that differential privacy is the only method of providing data privacy (which is false) and that asking the citizenship question would impact response rates is not sufficient grounds for the argument that the citizenship question cannot be asked, because not asking it implicates clear constitutional requirements that, in the order of things, have a paramount level of importance. If, in the process of complying with the Constitution, other statutory hurdles are encountered, then the appropriate action is to find solutions that comport with the threshold constitutional obligations. Neither differential privacy nor the lack of a determination of citizenship status appears to meet the constitutional obligations mandated for the census process.

Claim: 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.

Response: Previous methods to protect individuals' personal identifiable information worked just fine before the implementation of differential privacy. If the argument is that computers are getting better at deciphering past methods of protection and therefore new methods are needed, so be it. However, the article implies there are no alternatives (until it finally admits that other options exist). This admission, of course, is buried towards the end of the piece after bombastically suggesting that all privacy protections are on the cusp of being eliminated by "the Republicans." In reality, there are many concerns with differential privacy. Among the most pressing issues is that the algorithm intentionally inserts false information, false characteristic data, and false numerical data into the publicly available dataset. Only a select few individuals

at the Census Bureau are privy to the true information, a concern that Harvard University researchers identified in their 2021 [evaluation](#) of differential privacy.

Claim: 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.

Response: This is a solution in search of a problem. First, it assumes that no new methods would be implemented when removing differential privacy, which is an absurd assertion given the statutory obligation to protect data privacy. Second, there is no publicly available empirical evidence to suggest that any outside nefarious entity has successfully reverse engineered previous disclosure protection methods in the decennial census to target specific individuals en masse, at scale, or based on specific attributes. Third, the decennial census does not collect data on transgenderism, so that fear-mongering tactic regarding exposure is technically inaccurate. Finally, this claim inadvertently reveals the potential *political* purpose behind the adoption of differential privacy. Specifically, it allows unelected bureaucrats to intentionally distort information such as legal status so that it is not readily identifiable and available. This is a useful tool if one is part of a political movement that is more interested in protecting special classes critical to one's hold on power than in carrying out the mundane constitutional mission of the Census Bureau.

Claim: 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."

Response: There is no published evidence of any Decennial Census participant being "unmasked" ever, largely because the swapping protection worked. Outside of World War II, we are not aware of any instances where law enforcement used census records in this manner. Additionally, there is no evidence that the response rates of

permanent residents or citizens would be in any way affected by the inclusion of a citizenship question. To the degree that illegal populations may or may not have opinions about whether they should fill out the census that asks such questions, there should be a discussion of how to encourage participation. Nevertheless, the constitutional obligation to know where citizens live within states and to draw political districts represented by citizens alone supersedes other considerations. Further, citizens have withheld personal information from census efforts for various reasons for a long time. For example, the anticommunist John Birch Society famously encouraged its members not to comply with census workers and census efforts due to suspicions that the federal government would weaponize the information against them and their families. This admission confirms what many already know: Differential privacy is an agency effort, spearheaded at the behest of the progressive economist John Abowd, to intentionally thwart present and future efforts to determine the location and number of illegal immigrants in the country and thus distort political representation and channel power in favor of the political left. Respondents' participation and truthfulness in the census are not new problems, but differential privacy doesn't solve them. Characteristic data is not the main purpose and intent of the census, but population counts are.

Furthermore, the latest allegations in the Arctic Frost investigation, past abuses at the IRS, Cybersecurity and Infrastructure Security Agency censorship regimes, and the targeting of concerned parents at school board meetings may also have a justifiable effect on the willingness of Americans to provide the U.S. government with detailed information about themselves and their families. Will *WIRED* publish a follow-up article on how the weaponization of government by Democratic administrations will affect census data?

Claim: 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 or census block has to remain the same. But other demographic characteristics, like race or gender, are randomly 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. In other words, you'll know how many women or Hispanic people are in a census block, just not exactly where.

Response: The claim that "the total number of people in a state or census block has to remain the same" is either a lie or a display of ignorance of how the algorithm operates. Regardless, it is false. The Census Bureau admits in its disclosure avoidance guide for the 2020 Census that population counts and characteristic data below the state level contain noise introduced into the data. Differential privacy scrambles both characteristic and numerical data, down to the lowest census unit: the block level. There is no guarantee that everything adds up at the block level, but rather an assurance that as the geographical units nest higher, everything will eventually add up at the top-line state level. This means that individual blocks will contain people who don't exist and erase people who actually do, include inaccurate numerical counts that may be higher or lower than the number of people who actually reside in that area, and potentially may be moved into higher census units (like census tracts), including across voting district boundaries.

While the total numbers at the state level are accurate (or supposed to be), there is no way to confirm that the algorithm guarantees the accuracy of characteristic data or numerical count data at the lowest block level. Unlike the census's geographical units, which nest in a way that should make mathematical sense, the political units (like voting districts) do not correspond to the geographical units. If everything published by the census and every academic study of how differential privacy actually operates is incorrect, then Abowd and others should grant access to the algorithm and original datasets to prove it.

But the algorithmic data is kept secret, and no documentation from any source has been found in Center for Renewing America's research to substantiate claims of maintaining accuracy. These facts raise three important questions:

1. What is the source of this claim?
2. Who provided that information?
3. Were any laws violated in the process of that exchange by a Census Bureau staffer?

Claim: 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 mathematics professor at Tufts University who worked with census data to inform electoral maps in Alabama.

Response: This claim is dubious at best. Because differential privacy injects noise (i.e., falsified information) down into the lowest possible census units and moves

populations around throughout the various units and because the political geography (i.e., a voting district) does not correlate with these geographical units, an accurate count on even the racial composition of a voting district is not remotely guaranteed. In fact, differential privacy assumes that both the characteristic data and the numerical counts used for funding and voting rights are inaccurate. Only a select few at the Census Bureau have access to the actual totals and datasets. It is strange that a mathematics professor would provide a response that is so easily refutable. Either the professor does not actually understand how differential privacy works within the census framework or she is not telling the truth.

Claim: 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.

Response: This is not the argument Center for Renewing America was making about differential privacy. Curiously, or perhaps not curiously at all, the article seems to avoid discussing the impacts of differential privacy as it pertains directly to *redistricting* because the "experts" know full well that differential privacy does in fact affect redistricting. The question is by how much and to what extent there is district-by-district population and demographic variance.

Further, Texas and Florida were denied at least three congressional seats due to counting errors in the 2020 Census. Minnesota and Rhode Island—deep blue states—each held on to a congressional seat that they should have lost, and Colorado illegitimately picked up a seat it should not have gained. The result was a net gain of at least six seats for one political party (Democrats) over the other (Republicans). Given the scale to which leftists in the federal bureaucracy have turned their powers on political opposition, it is hard to dismiss the possibility that the current census process is being weaponized. It is certainly possible that a statistically unlikely series of events occurred, but most Americans no longer accept such outcomes at face

value without appropriate oversight and verification. Otherwise, yes, the writers of Center for Renewing America's post are fully aware that, in theory, differential privacy should not affect apportionment at all, only redistricting.

Claim: "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."

Response: If the 2020 Census had not resulted in significant counting errors in fourteen states that led to six seats being illegitimately awarded to congressional Democrats, and if the algorithm used to process the census had not intentionally falsified characteristic and numerical datasets, leading to numerous unconstitutional outcomes, the calls to "redo," reform, or republish the census would not exist. Claiming that differential privacy is just a punching bag as a means of delegitimizing the serious concerns about the shortcomings of differential privacy is academic dishonesty at best and partisan propaganda at worst.

Claim: "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, driver's licenses, etc.)."

Response: Abowd's claim is intentionally misleading, and it raises serious red flags about his commitment to honesty and transparency in census policy. Differential privacy should not, in theory, impact apportionment (though the jury is still out, given the secrecy of the algorithmic processes). It is certainly understood that in a differential privacy system statewide population data is supposed to be invariant, but given Abowd's eagerness to elevate statutory provisions over constitutional requirements and principles, there is no universe in which anyone should simply trust these claims. Indeed, apportionment should not be affected by differential privacy, but the Census Bureau must demonstrate the accuracy of its data by subjecting it to appropriate oversight and external analysis.

Abowd's answer also cleverly ignores the elephant in the room by not mentioning that differential privacy's data is used to *redistrict*. Because the political geography of a state (voting districts) does not align with the boundaries of the census's geographic units (blocks, block groups, tracts, etc.), differential privacy does indeed move populations across voting district boundaries. This adjustment muddies the accuracy of the demographic composition for each voting district, with an allegedly acceptable variance rate as high as 20 percent. Abowd's pivot to apportionment (which ultimately relies on the invariant top-line state totals) is a slick attempt to avoid discussing the larger point.

Lastly, if differential privacy is not discarded and a citizenship question is added with the express purpose of *excluding* illegal aliens for purposes of apportionment or all noncitizens for redistricting (options that should be considered by the Trump administration), then differential privacy will be a significant issue for apportionment purposes because of its ability to falsify characteristic data. On this point, there are still unanswered questions. For example, how has differential privacy been used to move characteristic data that could also impact redistricting? Has the algorithm been abused to manipulate minority characteristics and create more minority-majority districts? The evidence remains murky at best. The default posture is that when people with power believe they can get away with something corrupt and no one will ever figure it out, they are more inclined to take such risks, especially when they can morally justify their actions to the public and benefit their side.

Claim: 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.

Response: There is no reason to engage in a hypothetical conjecture that this "could lead to skewed numbers." It already happened, and the Census Bureau admitted as much in its 2022 Post-Enumeration Survey. Undercounting occurred in six states in the 2020 Census. Of those six states (Arkansas, Florida, Illinois, Mississippi, Tennessee, and Texas), five were red states, which raises reasonable concerns about fairness. The Census Bureau admits that the errors in Texas alone totaled nearly 548,000 people. It is also known that both Texas and Florida lost at least three congressional seats due to these counting errors. Furthermore, compliance with constitutional principles in the process cannot just be jettisoned out of concerns for participation rates. The solution is to comply with constitutional requirements and then develop policies to encourage participation.

Claim: 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.

Response: The alternatives already exist and have been used since the mid-1950s. They include swapping protocols, in which characteristics are simply transferred from one individual to another; topcoding techniques; and even table suppression efforts to mask small-area data. The Integrated Public Use Microdata Series has written extensively over the years on better ways to protect privacy in the census. While the advent of new technologies may require developing new techniques, there are alternatives rooted in previously existing methods that do not intentionally falsify datasets and jeopardize the "one person, one vote" principle that the bureau ostensibly follows.

It is absurd for this activist professor to suggest that there are no alternatives to safeguard personal data and then add the qualification "that the Census Bureau uses." Alternatives do exist, census bureaucrats are well aware of those options, and they can choose to switch to better methods. Flaxman's quote is clever: It is dishonest while remaining technically accurate. Those alternatives were used in previous census efforts without outside nefarious actors reverse engineering data to identify individuals or groups of individuals. As it pertains to census functions, differential privacy is a political device masquerading as a privacy protection tool.

Claim: 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.

Response: It sounds like there is work to do before the 2030 Census. The reality is that differential privacy distorts the accuracy, transparency, and reliability of both

characteristic data and numerical data at every geographical level below the top-line state metrics. It muddies redistricting efforts due to population transference and falsification. It raises questions about federal funding formulas due to the secrecy of the original data. And it creates tools to hide legal status to protect illegal populations who are distorting the political representation and power *owed to American citizens and American citizens alone*. Differential privacy must be discarded with prejudice.

Claim: 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.)

Response: What is this? An *alternative*? Above, the article cites "experts" who repeatedly claim that none exist.

Claim: 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."

Response: To be clear, if the intent of the academic activists quoted in this piece is to "pursue equity," then the political motivations for this haphazard defense of differential privacy have been fully unmasked. Undermining the far more important purposes of the census, distorting federal funding streams, and creating fake political districts to advance DEI initiatives through census data seems to be their real agenda. Combating discrimination can be noble, depending on how one defines it and the intentions behind it, but we no longer accept that "equity" agendas are actually about stopping discrimination, and excluding so many clear constitutional principles in the process for this justification alone is not a serious position.