

# The Promise and Limitations of Formal Privacy

Aaron R. Williams and Claire McKay Bowen

## 1 Differential privacy is everywhere

Differential privacy (DP) is in our smart phones, web browsers, social media, and the federal statistics used to allocate billions of dollars. Despite the mathematical concept being only 17 years old, differential privacy has amassed a rapidly growing list of real-world applications.

The U.S. Census Bureau launched the first major deployment of DP with its 2008 release of OnTheMap, an interactive tool for exploring United States income and commuting patterns (Machanavajjhala et al. 2008). Since then, there have been several applications within industry, academia, and government. Apple uses DP to learn about users' preferences including emojis, popular health data types, and playback preferences in Safari (Differential Privacy Team, Apple, n.d.). Opportunity Insights at Harvard University used DP at Meta to summarize 21 billion Facebook friendships for 72.2 billion Facebook users to understand the relationship between social capital and economic mobility (Chetty, Jackson, Kuchler, Stroebel, Hendren, Fluegge, Gong, Gonzalez, Grondin, Jacob, Johnston, Koenen, Laguna-Muggeburg, et al. 2022; Chetty, Jackson, Kuchler, Stroebel, Hendren, Fluegge, Gong, Gonzalez, Grondin, Jacob, Johnston, Koenen, Laguna-Muggeburg, et al. 2022). The Census Bureau applied a variation of DP in the 2020 Decennial Census (J. Abowd et al. 2022).

The use of DP has major implications for people in the United States. For instance, the U.S. Census Bureau estimates that census data was used to allocate \$675 billion through 132 federal programs in fiscal year 2015 (Hotchkiss and Phelan 2017). The amount of money allocated is even greater today.

Why is DP so pervasive? DP is currently the only mathematical framework that provides a finite and quantifiable bound on disclosure risk when releasing information from confidential data. Previous concepts of data privacy and confidentiality required various assumptions about how a bad actor might attack sensitive data. DP is often called formally private because statisticians can mathematically prove the worst-case scenario privacy loss that could result from releasing information based on the confidential data.

Although DP ushered in a new era of data privacy and confidentiality methodologies, many researchers and data practitioners criticize differentially private frameworks. In this paper, we

This is the author manuscript accepted for publication and has undergone full peer review but has not been through the copyediting, typesetting, pagination and proofreading process, which may lead to differences between this version and the Version of Record. Please cite this article as doi: [10.1002/wics.1615](https://doi.org/10.1002/wics.1615)

This article is protected by copyright. All rights reserved.

provide readers a critical overview of the current state-of-the-art research on formal privacy methodologies and various relevant perspectives, challenges, and opportunities.

*A note on terminology:* The data privacy community or ecosystem encompasses a wide range of stakeholders, which we define as follows:

- **Data users and practitioners:** individuals who consume the data, such as analysts, researchers, planners, and decision-makers.
- **Data privacy experts or researchers:** individuals who specialize in developing data privacy and confidentiality methods.
- **Data curators, maintainers, or stewards:** individuals who own the data and are responsible for its safekeeping.
- **Data intruders, attackers, or adversaries:** individuals who try to gather sensitive information from the confidential data.

## 2 Threats to confidentiality are real, growing, and controversial

Many entities, including federal statistical agencies, do not release valuable data because of real threats to confidentiality. These threats are growing due to increasing computing power and exploding sources of auxiliary information, such as social media data and corporate data breaches (Thompson and Warzel 2019). Additionally, privacy researchers showed for years that simply removing personally identifiable information is insufficient and that anonymized data are often not anonymized (Sweeney 2000).

One of the most famous examples is the Netflix Prize. In 2006, Netflix hosted a competition to see if external teams could improve their predictions of movie ratings by 10 percent with a \$1 million prize. For the competition, Netflix released a data set of 100,480,507 movie ratings from 480,189 users. Narayanan and Shmatikov (2008) quickly demonstrated that the supposedly anonymized records in the data set could be re-identified by leveraging publicly available information from the Internet Movie Database (IMDb). Furthermore, an attacker could learn about movies that IMDb users had watched but not rated on Netflix, including movies that could be used to infer an IMDb user's sexual orientation or political preferences. Facing a lawsuit and privacy concerns, Netflix cancelled their second prize in 2010 (Lohr 2010).

Another example is the 2020 Decennial Census. Every ten years, the U.S. Census Bureau aims "...to count everyone once, only once, and in the right place." In other words, a decennial census includes information about all residents in the United States. Because Title 13 of the United States Code mandates that the Census Bureau protects census data, the U.S. Census Bureau does not release microdata or individual-level decennial census data. The Census Bureau first applies several statistical disclosure control methods (or methods of data privacy and confidentiality) before releasing about 6.2 billion statistics as summary tables, such as the number of people in Philadelphia, Pennsylvania or Salmon, Idaho. The U.S. Census

Bureau refers to their data privacy and confidentiality protection as the Disclosure Avoidance System.

Given the significant shift in public data access and computational power since 2010, the Census Bureau conducted a simulated attack on the 2010 Decennial Census. Using linear computing and substantial computing power, the U.S. Census Bureau generated detailed microdata from the tables released for the 2010 Decennial Census (Hawes 2021). Specifically, the Census Bureau reported they could exactly match almost 47 percent of the real population data and matched between 52 million and 179 million of the almost 309 million respondents using commercial databases with financial and marketing data that the U.S. Census Bureau purchased. However, the names for the matched data were in the identified blocks only 38 percent of the time. This reconstruction attack demonstrates a concept at the roots of formal privacy called the database reconstruction theorem (Dinur and Nissim 2003).

The U.S. Census Bureau uses the simulated reconstruction attack to justify adopting formal privacy methodologies for the 2020 Decennial Census. But, this simulated reconstruction attack has several criticisms. For instance, Ruggles and Van Riper (2022) demonstrated through a Monte Carlo simulation that many of the matches the re-identification simulation identified could have been identified by random chance. They state, “We would therefore expect the Census Bureau to be ‘correct’ on age and sex most of the time even if they had never looked at the tabular data from 2010 and had instead just assigned ages and sexes to their hypothetical population at random.” Further, the Census Bureau has not released the full technical details of the reconstruction attack, leading the census data user community to demand a technical report. In response, the Census Scientific Advisory Committee recommended in the 2022 Fall Meeting that the U.S. Census Bureau release such a report.<sup>1</sup>

The Census Bureau responded publicly to these critiques through a public presentation about how the random guess does not account for the higher re-identification rate of the population uniques for non-modal race/ethnicity.<sup>2</sup> The Associate Director for Research and Methodology and Chief Scientist of the U.S. Census Bureau also discussed the reconstruction attack and criticisms in his third Declaration for the Fair Lines America Foundation, Inc., vs. United States Department of Commerce lawsuit.<sup>3</sup> As of the publication of this article, the Census Bureau has not responded to the Census Scientific Advisory Committee’s list of recommendations.

---

<sup>1</sup>“Census Scientific Advisory Committee Virtual Meeting: September 29-30, 2022”, <https://www.census.gov/about/cac/sac/meetings/2022-09-meeting.html>

<sup>2</sup>“Reconstruction and re-identification of the Demographic and Housing Characteristics File (DHC)”, <https://www2.census.gov/about/partners/cac/sac/meetings/2022-09/presentation-reconstruction-and-re-identification-of-dhc-file.pdf>

<sup>3</sup>“Third Declaration of John M. Abowd”, <https://www2.census.gov/about/policies/foia/records/disclosure-avoidance/17-1-abowd-decl-3.pdf>

### 3 The promise of formal privacy

These examples highlight why data privacy and confidentiality methods are needed to protect released microdata and statistics from confidential data against disclosures. The field of statistical disclosure control (SDC) or limitation has existed within the broader statistics domain for decades. The goal of SDC methods is to balance protecting the privacy of records with providing useful statistical results from the data. But, properly applying SDC techniques is difficult. When developing a SDC method, privacy researchers must predict how a data intruder might attack the data, considering what sensitive information they want and what resources they have now or in the *future*.

DP did away with those assumptions about attacks on confidential data and started from scratch. Earlier, we stated that DP is formally private, but the privacy community has not fully agreed on a common definition. The U.S. Census Bureau<sup>4</sup> officially defined formal privacy as a subset of SDC methods that give “formal and quantifiable guarantees on inference disclosure risk and known algorithmic mechanisms for releasing data that satisfy these guarantees.” For the remainder of the paper, we will refer to this broader mathematical framework or concept as formal privacy. We will also refer to the SDC methods not developed within a formal privacy framework as traditional SDC methods. Although methods developed within the formal privacy framework are considered SDC methods, data privacy researchers often separate formal privacy from other SDC methods.

*Another note on terminology:* In the formal privacy literature, researchers often use the terms *mechanism*, *algorithm*, and *method* interchangeably to describe the process of releasing a private statistical output. Sometimes these researchers refer to a simple process, such as adding noise directly to a computed statistic. Other times they refer to more complicated processes, such as post-processing (explained later in this section). We do not see a clear delineation in the literature when using the three terms. More crucially is that anything referred to as a formally private method, formally private mechanism, or formally private algorithm must provably satisfy the relevant definition of formal privacy.

In general, formally private methods have the following features (Bowen and Garfinkel 2021):

- Ability to quantify and adjust the privacy-utility trade-off, typically through parameters.
- Ability to rigorously and mathematically prove the maximum privacy loss that can result from the release of information.
- Formal privacy definitions also allow one to “compose” multiple statistics. In other words, a data curator can compute the total privacy loss from multiple individual information releases.

The main difference between traditional SDC methods and formally private methods is the ability to account for all information being “leaked” from the confidential data. We use the

---

<sup>4</sup>“Consistency of data products and formally private methods for the 2020 census,” US Census Bureau, p. 43, <https://irp.fas.org/agency/dod/jason/census-privacy.pdf>

example given in Bowen, Williams, and Pickens (2022) to explain. We can think of traditional SDC methods as someone charging a limitless credit card; formally private methods are when someone charges to a debit card with a set budget. In both scenarios, there is a running bill, but only one requires constantly checking the balance. We can easily imagine that not tracking that bill is the equivalent of releasing too many statistics with enough accuracy, which could compromise the confidential data (Bowen and Garfinkel 2021). Although data stewards must limit the type and number of questions asked of the data in both traditional and formal privacy settings, they are faced with “tracking the bill” under a formal privacy framework.

### 3.1 Formal privacy definitions

Formal privacy is a relatively new set of definitions for quantifying the worst-case amount of information disclosed from statistics calculated on a private database. We mathematically define several formally private definitions and key theorems. We use the following notation:  $\mathcal{D} \in \mathbb{R}^{n \times d}$  is the confidential data set representing  $n$  data points and  $d$  variables and  $q : \mathbb{R}^{n \times d} \rightarrow \mathbb{R}$  denotes the statistical query, i.e.,  $q$  is a function mapping  $\mathcal{D}$  to  $\mathbb{R}$  real numbers. We denote a randomized or noisy version of  $q$  using  $\mathcal{M} : \mathbb{R}^{n \times d} \rightarrow \mathbb{R}$ , which is a function that satisfies a formally private definition.

DP is the most widely known formal privacy definition. Privacy experts often refer to the original definition of DP as pure-DP or  $\epsilon$ -DP.

**Differential Privacy** (Dwork, McSherry, et al. 2006): A sanitization algorithm,  $\mathcal{M}$ , satisfies  $\epsilon$ -DP if for all subsets  $S \subseteq \mathcal{D}$  and for all  $\mathcal{D}, \mathcal{D}'$  such that  $q(\mathcal{D}, \mathcal{D}') = 1$ ,

$$\frac{\Pr(\mathcal{M}(\mathcal{D}) \in S)}{\Pr(\mathcal{M}(\mathcal{D}') \in S)} \leq \exp(\epsilon) \quad (1)$$

where  $\epsilon > 0$  is the privacy loss budget and  $q(\mathcal{D}, \mathcal{D}') = 1$  represents the possible ways that  $\mathcal{D}'$  differs from  $\mathcal{D}$  by one record.

There are two definitions for “ $\mathcal{D}'$  differs from  $\mathcal{D}$  by one record.” One definition assumes the presence or absence of a record, where the dimensions of  $\mathcal{D}$  and  $\mathcal{D}'$  differ by one row. The other definition assumes the change of the value in one record, where  $\mathcal{D}$  and  $\mathcal{D}'$  have the same dimensions. Li et al. (2016) refers to these as *unbounded DP* and *bounded DP*, respectively. They state that unbounded DP satisfies an important composition theorem, which we will discuss later in this section, whereas bounded DP does not. Most differentially private methods use unbounded DP, because they rely on the composition theorems.

Privacy researchers developed new formally private definitions that are considered relaxations of  $\epsilon$ -DP, because they inject less noise into the output, such as  $\delta$ -DP (Dwork, Kenthapadi, et al. 2006), probabilistic DP (Machanavajjhala et al. 2008), concentrated DP (Bun and Steinke 2016), Rényi differential privacy (Mironov 2017), and zero-concentrated DP (Bun and Steinke 2016). Although these definitions use the same provable privacy framework, they have other parameters offering different privacy guarantees that allow other types of noise.

We will cover approximate DP (i.e.  $(\epsilon, \delta)$ -DP) and zero-concentrated DP (zCDP or  $\epsilon$ -zCDP) in depth, because they're the most common formally private definitions used in real-world applications.

$(\epsilon, \delta)$ -Differential Privacy (Dwork, Kenthapadi, et al. 2006): A sanitization algorithm,  $\mathcal{M}$ , satisfies  $(\epsilon, \delta)$ -DP if for all  $\mathcal{X}, \mathcal{X}'$  that are  $\mathcal{X}(\mathcal{X}, \mathcal{X}') = 1$ ,

$$\Pr(\mathcal{M}(\mathcal{X}) \in \mathcal{S}) \leq \exp(\epsilon) \Pr(\mathcal{M}(\mathcal{X}') \in \mathcal{S}) + \delta \quad (2)$$

where  $\delta \in [0, 1]$ .

This definition adds the parameter  $\delta$  to allow the privacy loss associated with the  $\epsilon$  bound to fail at a rate no greater than  $\delta$ . The  $\epsilon$ -DP definition can also be defined as a special case of  $(\epsilon, \delta)$ -DP when  $\delta = 0$ .

Another common formally private definition is zero-concentrated DP (zCDP or  $\epsilon$ -zCDP), which the Census Bureau used to protect the 2020 Decennial Census.

**Zero-Concentrated Differential Privacy** (Bun and Steinke 2016): A sanitization algorithm,  $\mathcal{M}$ , satisfies  $(\epsilon, \delta)$ -zero-concentrated differential privacy if for all  $\mathcal{X}, \mathcal{X}'$  that are  $\mathcal{X}(\mathcal{X}, \mathcal{X}') = 1$  and  $\epsilon \in (1, \infty)$ ,

$$\mathbb{D}_{\epsilon}(\mathcal{M}(\mathcal{X}) || \mathcal{M}(\mathcal{X}')) \leq \epsilon + \delta \epsilon, \quad (3)$$

is the  $\epsilon$ -R'enyi divergence between the distribution of  $\mathcal{M}(\mathcal{X})$  and  $\mathcal{M}(\mathcal{X}')$ .

### 3.2 Global sensitivity

Most formally private methods rely on global sensitivity, which describes how resistant the statistic is to the presence of outliers. We can quantify the global sensitivity by how much an output can change with the addition or removal of the most extreme possible record that could exist in the population. In other words, regardless of whether that record is actually present, we must consider any arbitrary realization of the data. This means formally private methods that use global sensitivity try to account for any possible version of the data that could exist, protecting against future data releases and new technologies.

We borrow the example explained in Bowen, Williams, and Pickens (2022) to help explain this concept. Imagine the data we want to protect contains socioeconomic information and the question we want answered is, "What is the median wealth?" Under formal privacy, we must consider the change of the most extreme possible record that could exist in any given data that has demographic and financial information. In our example, that person is Bernard Arnault, who was the wealthiest person in the world in 2022. If Arnault is present or absent in the data, the median wealth should not change too much. This means we can provide a more accurate answer by applying fewer alterations to the median income statistic, because it is less sensitive to the extreme outlier, Arnault. Consider, however, the question, "What is

the average wealth?” Unlike the previous statistic, the answer would significantly change if Arnault were present or absent from the data. To protect the extreme case at a given level of privacy loss, a formally private algorithm would need to provide a significantly less accurate answer by altering the statistic more.

There are two different versions of global sensitivity  $\ell_1$ -global sensitivity and  $\ell_2$ -global sensitivity.

$\ell_1$ -Global Sensitivity (Dwork, McSherry, et al. 2006): For all  $\mathcal{D}, \mathcal{D}'$  such that  $d(\mathcal{D}, \mathcal{D}') = 1$ , the global sensitivity of a function  $f$  is

$$\Delta_1(f) = \sup_{d(\mathcal{D}, \mathcal{D}')=1} \|f(\mathcal{D}) - f(\mathcal{D}')\|_1 \quad (4)$$

The  $\ell_2$ -global sensitivity calculates the maximum amount a statistic can change in absolute value terms with the addition or removal of the most extreme possible observation. In contrast,  $\ell_1$ -global sensitivity calculates the maximum amount a statistic can change when the statistic is squared, summed, and rooted with the addition or removal of the most extreme possible observation. Global sensitivity is straightforward but calculating the global sensitivity for some statistics can be very difficult. For instance, we cannot calculate a finite global sensitivity of sample mean if we do not bound the variable.

### 3.3 Fundamental sanitizers

We present two fundamental formally private sanitizers. We call these sanitizers fundamental because they’re the original formally private sanitizers that privacy researchers still often use as building blocks for more sophisticated formally private methods.

Dwork, McSherry, et al. (2006) first proposed protecting statistics by adding noise from a Laplace distribution, called the Laplace mechanism, but we can think of it as a Laplace sanitizer. The Laplace distribution is centered at zero and the distribution variability is the ratio of the privacy loss budget,  $\epsilon$ , over the  $\ell_1$ -global sensitivity of the statistic. Since the distribution is centered at zero, there is a higher probability of adding very little or no noise to the statistic. For the noise variability, if  $\epsilon$  is large or the sensitivity of the statistic is low, then there is a higher probability of adding very little noise to the confidential data statistic. If  $\epsilon$  is small or the sensitivity of the statistic is high, then there is a higher probability of adding a lot of noise to the statistic.

**Laplace mechanism** (Dwork, McSherry, et al. 2006): Given any function  $f : \mathbb{R}^{\mathcal{D} \times \mathcal{D}} \rightarrow \mathbb{R}^{\mathcal{D}}$ , the Laplace mechanism is defined as:

$$\mathcal{M}(f) = f(\mathcal{D}) + (\mathcal{Z}_1, \dots, \mathcal{Z}_{|\mathcal{D}|}). \quad (5)$$

where  $(\mathcal{Z}_1, \dots, \mathcal{Z}_{|\mathcal{D}|})$  are i.i.d.  $\mathcal{N}(0, \frac{\epsilon}{\Delta_1(f)})$ .

Similar to the Laplace mechanism, the Gaussian mechanism adds random noise from a Gaussian distribution. The Gaussian distribution is also centered at zero and the distribution variability is the ratio of the privacy loss budget,  $\epsilon$ , over the  $\epsilon_2$ -global sensitivity of the statistic (mathematically, the Gaussian mechanism does not satisfy  $\epsilon_1$ -global sensitivity).

**Gaussian mechanism** (Dwork and Roth 2014): Given any function  $f : \mathbb{R}^{\epsilon \times \epsilon} \rightarrow \mathbb{R}^{\epsilon}$ , the Gaussian mechanism is defined as:

$$\mathcal{M}(f) = f(\epsilon) + (\epsilon_1, \dots, \epsilon_{\epsilon}). \quad (6)$$

where  $(\epsilon_1, \dots, \epsilon_{\epsilon})$  are i.i.d.  $\epsilon \sim (0, \epsilon^2 = (\frac{\Delta_2(\epsilon)\sqrt{2\log(1.25/\epsilon)}}{\epsilon})^2)$ .

Both fundamental sanitizers are easy to apply in practice, but only apply to numerical values without additional post-processing. Determining which fundamental sanitizer to use depends on the data and the use case. For a single statistic, the Laplace distribution has less variation than the Gaussian distribution. However, the sum of multiple draws from independent Gaussian distributions is Gaussian-distributed, which has appealing properties when aggregating noisy statistics. This was key in the U.S. Census Bureau's implementation of their SDC method for the 2020 Census. A drawback is the Gaussian mechanism has two privacy parameters ( $\epsilon$  and  $\epsilon_2$ ), whereas the Laplace mechanism only has  $\epsilon$ .

### 3.4 Important theorems

As mentioned earlier, DP requires methods to compose or account for the total privacy loss from each public data release or statistic. For example, composition or accounting allows the data curator to track the total privacy loss from multiple summary tables or multiple statistics requests from several data users. This is the main advantage of DP compared to traditional SDC methods, which cannot quantify the total privacy loss. There are two main composition theorems: sequential and parallel. We also cover another important theorem (post-processing) that is essential in developing formally private methods.

#### 3.4.1 Sequential composition theorem

The sequential composition theorem allows the data users to calculate the privacy loss budget from multiple noisy statistics on the same part of the confidential data (Bun and Steinke 2016; McSherry 2009). To help explain this concept, suppose we have establishment economic data set that reports the state of operation, the number of employees, and the average income for each establishment. We want to conduct three different analyses that cost  $\epsilon_1 = 1$ ,  $\epsilon_2 = 0.5$ , and  $\epsilon_3 = 0.5$ , respectively. Since we are applying the three analyses on the entire data, sequential composition requires us to add up the individual privacy loss budgets for the total. i.e.,  $\epsilon_{\text{total}} = \epsilon_1 + \epsilon_2 + \epsilon_3 = 2$ . Figure 1 shows the application of sequential composition to our fictitious economic data set.



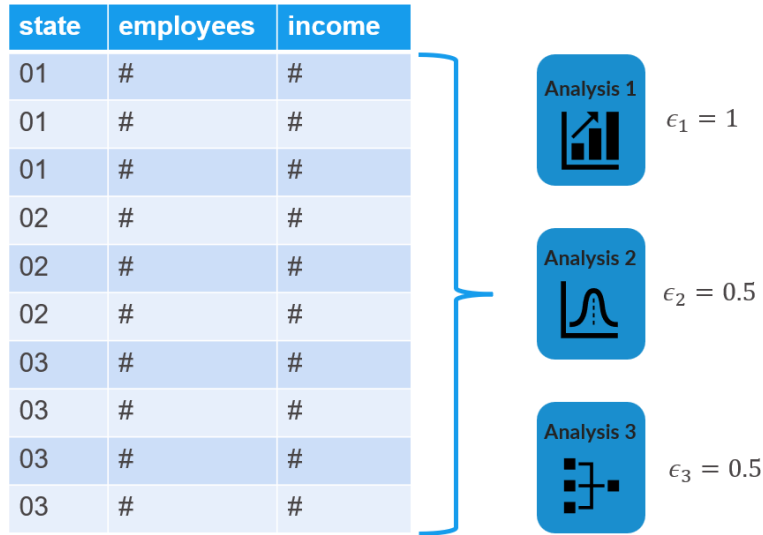


Figure 1: An Example of Sequential Composition.

### 3.4.2 Parallel composition theorem

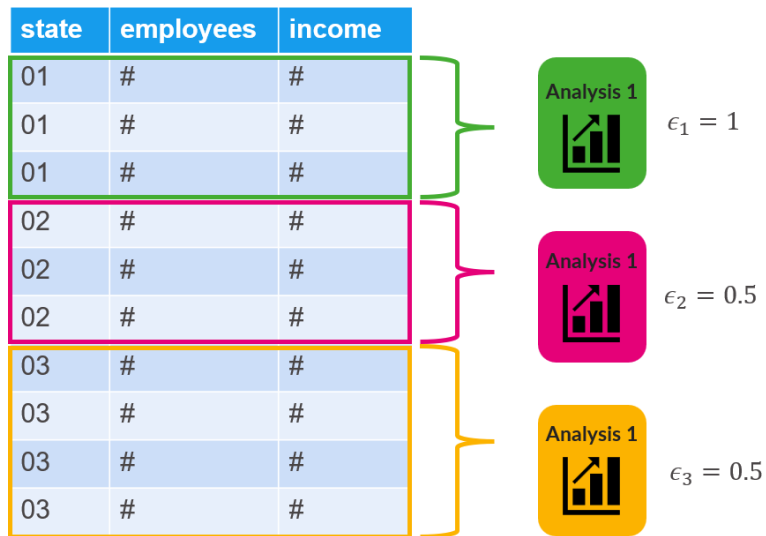


Figure 2: An Example of Parallel Composition.

The parallel composition theorem allows data users to calculate the privacy loss budget from multiple noisy statistics on different or disjoint parts of the confidential data (Bun and Steinke 2016; McSherry 2009). Using the same example as before in figure 1, suppose we apply three analyses to partitions of the data (i.e., the three different states) that cost  $\epsilon_1 = 1$ ,  $\epsilon_2 = 0.5$ , and

$\epsilon_3 = \epsilon$ , respectively. Since we are applying the three analyses on disjoint subsets of the data, parallel composition states that the total privacy loss budget is the maximum privacy loss budget of the three analyses. i.e.,  $\epsilon_{\text{total}} = \max(\epsilon_1, \epsilon_2, \epsilon_3) = \epsilon$ . Figure 2 shows the application of sequential composition to our fictitious economic data set.

### 3.4.3 Post-processing theorem

Another important theorem is the post-processing theorem that allows the continued use of formally private information without losing the privacy guarantee (Bun and Steinke 2016; Dwork, McSherry, et al. 2006; Nissim, Raskhodnikova, and Smith 2007). In other words, if someone modifies a formally private data set or statistic without using additional information from the confidential data, then that data set or statistic is still formally private. For example, if the number of employees from a formally private method said there are 3.7 employees, then we could round that value to 4 without leaking more information. Simply put, the post-processing theorem makes the data usable after formally private noise is added.

Post-processing also provides the opportunity to improve utility. Data stewards can use available public or expert knowledge to reduce the amount of noise without accruing additional privacy loss (McKenna, Sheldon, and Miklau 2019). The public information can come from data released without formal privacy or from individuals who are comfortable sharing their information without noise. Yet, few formally private methods leverage this feature. Bowen and Garfinkel (2021) have stated that, “Approaches for making use of public data are thus a largely unrealized opportunity for researchers to develop new mechanisms that would improve accuracy and corresponding impact on privacy.” Of course, the opportunities and benefits of leveraging public knowledge would diminish if most or all releases of data use formal privacy.

Formal privacy is transparent and allows users to account for the noise introduced into statistics. Post-processing can give up some of this transparency and make it more difficult to account for the noise added to statistics.

## 3.5 Privacy loss budget

The privacy loss budget bounds the privacy risk associated with releasing data or statistics. Thus, privacy experts could use the privacy loss budget to adjust and tune the privacy-utility trade-off. The formally private definitions we have introduced use a concept of a privacy loss budget represented mathematically as  $\epsilon$ ,  $\delta$ , and  $\rho$ . For simplicity, we focus on  $\epsilon$ .

Privacy researchers can increase or decrease  $\epsilon$ , adjusting the resulting privacy-utility trade-off. If a privacy researcher increases  $\epsilon$ , then they increase the maximum disclosure risk (i.e., the upper bound of the disclosure risk) associated with a given release of information. Simply put, a larger  $\epsilon$  means we potentially add less noise to a statistic, resulting in higher accuracy and less privacy. A smaller  $\epsilon$  means we potentially add more noise to a statistic, resulting in lower accuracy and more privacy.

We can imagine the privacy-utility trade-off in two extreme cases. In one case, a data steward could achieve perfect privacy by not releasing any information about the confidential data. In the other case, a data steward could achieve perfect utility by releasing all information about the confidential data. These extreme cases show that it is impossible to obtain perfect privacy and utility.

The definition of  $\epsilon$ DP covers these extremes. When  $\epsilon \rightarrow 0$ , we release no information about the confidential data. When  $\epsilon \rightarrow \infty$ , we release unaltered information about the confidential data.

As we learned from the composition theorems, an important characteristic for data stewards is that the privacy loss budget composes. This means data curators and privacy researchers can treat  $\epsilon$  as a global privacy loss budget, similar to setting a budget on a debit card. In other words, a data steward could allocate  $\epsilon$  to individual queries that sum up to  $\epsilon$ .

How to determine an appropriate privacy loss budget remains an open question. We elaborate on this challenge later in this paper.

### 3.6 Models of formal privacy

Privacy experts have developed two models for implementing a formal privacy framework: the *trusted curator model* and the *local model*.

The trusted curator model (or central model) involves a centralized data curator that receives confidential data, creates the data products, applies the formally private method, and releases the results. In practice, the trusted curator must apply the formally private method to any released statistic, even if the statistic is similar. If the data curator decides to cap the privacy loss budget, then the data curator must stop releasing statistics based on the confidential data. If the data curator doesn't, then this leads to the  $\epsilon \rightarrow \infty$  scenario, where a data intruder could make precise statistical inferences about the confidential data.

In the local model, data participants or data collection points receive their own privacy loss budget instead of using a global budget that is applied to the entire confidential data. In other words, the participants add formally private noise locally to their own data before sending their information to the data curator. This means that the data curator is not trusted. The concept of the local model is very similar to the randomized response survey method (Warner 1965), where Wang et al. (2020) showed that they are mathematically equivalent under many conditions. However, compared to the trusted curator model, the local model adds substantially more noise and tends to break the global relationships (Bowen and Garfinkel 2021).

## 4 Desired statistical privacy properties

Regardless of which framework a privacy expert uses (traditional SDC vs. formal privacy, trusted curator vs. local), we can imagine at least four desired properties when developing any SDC framework:

1. Quantifiable bound that composes across multiple data and statistics releases
2. Measure of absolute disclosure risk
3. Easy to apply and understand for data stewards and users
4. Result in useful data and statistics while providing appropriate protection

### 4.1 Quantifiable bound that composes across releases

Data stewards must balance the incremental privacy loss caused by each data use and determine if that privacy loss is justified in terms of its economic benefits and risks. This idea is not new. For years, privacy professionals have known that privacy loss is cumulative. For instance, it is possible to combine many seemingly innocuous facts about an individual to gain a detailed picture of that person. Similarly, it is possible to release many seemingly innocuous statistics that together generate untenable disclosure risks for individuals in a population. This is called the *mosaic effect*.

Privacy loss accounting, or the ability to maintain a universal privacy loss budget using privacy parameters, is a major strength of formal privacy. To our knowledge, formal privacy is the only approach to releasing statistics with this property. Traditional SDC has always relied on ad hoc approaches or judgement to account for the impact of multiple releases. Again, traditional SDC methods use a credit card instead of a debit card to track and account for the privacy loss with every public statistic or data release.

### 4.2 Measure of absolute disclosure risk (not relative disclosure risk)

Formal privacy definitions place a bound on the ratio of probabilities that a statistic comes from one of the two configurations of the underlying data and potential data. Ultimately, the privacy parameters like  $\epsilon$  quantify a relative disclosure risk. A disclosure avoidance framework would ideally identify and abate absolute disclosure risks. For example, person  $x$  has a 1-in-10 chance of being re-identified without disclosure control and a 1-in-100,000 chance of being re-identified with disclosure control.

Unfortunately, this is often intractable and measures instead focus on relative risk. For example, person  $x$  is twice as likely to be re-identified without disclosure control than with disclosure control. The usefulness of relative disclosure risks is limited without understanding the absolute disclosure risk. For example, knowing that the disclosure risk has doubled is almost useless without knowing if the baseline risk is 1-in-10 or 1-in-1 billion.

Using a Bayesian framework, Reiter (2005) and McClure and Reiter (2012) worked to develop measures of absolute disclosure risks using prior distributions to represent a situation in which no information is released at all. Unfortunately, as summarized by (Hotz et al. 2022), “the Bayes theorem expression also makes plain that measuring absolute disclosure risk is difficult, as it depends on the intruder’s information. Learning this information, or making assumptions about it, can be challenging.” To our knowledge, there are no SDC methods that sufficiently quantify absolute disclosure risk.

### 4.3 Easy to apply and understand for stewards and users

Quantitative researchers already need subject matter and methodological expertise to publish quality research. Expecting researchers to additionally become privacy experts to access any data from sensitive populations is unreasonable. Similarly, the government and private industry have finite and limited resources to implement disclosure control frameworks. Given the societal benefits of data for research, significantly reducing the amount of data available for research in the name of disclosure control is a bad outcome.

Any framework for limiting disclosure risks needs to be easy to apply and understand for data stewards and data users. Ideally, the privacy-preserving framework should be transparent for participants on how their information is being protected, easy for data stewards to implement to protect the data, and practical for data users to account for the impacts of the disclosure control methods.

Consider formal privacy and a traditional SDC framework like cell suppression. Both are highly technical for data stewards to apply to data. Cell suppression requires identifying and applying primary and secondary suppressions based on certain pre-specified conditions, such as suppressing cells with less than five contributors. Formal privacy requires an entirely new set of tools including calculating sensitivities and applying the proper composition theorems. However, formal privacy requires injecting noise into statistics during analysis, which creates additional challenges. The formal privacy framework is a stark contrast to most traditional SDC methods, which can be applied at the end of an analysis. In some cases, this difference can shift the responsibility from data stewards to data users when accounting for the analysis impact on downstream uses.

On the other hand, data users have a difficult time accounting for the uncertainty added by traditional SDC. This is especially true when data stewards go to great lengths to hide the technical details about SDC for privacy reasons, like not reporting the swap rate in the 1990 to 2010 Decennial Census. Unlike traditional SDC methods, formal privacy can be transparent and should allow users to account for the added noise. However, theoretical work on accounting for the formally private noise is limited and post-processing can undermine this benefit (Gong 2022; J. Abowd et al. 2021; Slavković and Seeman 2023).

Finally, data users may be limited in the types of statistics they can use and may need to learn different methods for each type of statistic. Cell suppression is often determined by the

number of observations behind a statistic regardless of the type of statistic, whereas each type of statistic in formal privacy can have a different sensitivity and different method for adding noise. Formal privacy can work well with robust statistics, such as counts and medians, but can perform poorly for statistics that inform decision-making based on totals and regression coefficients. Robust statistics are useful but insufficient for all data users' needs.

#### **4.4 Result in useful data and statistics while providing appropriate protection**

Data accessibility for researchers generates great benefits to society. If informed decision-making improves lives and accurate analyses are necessary for informed decision-making, then generating incorrect results in the name of confidentiality creates harm. It is important that any SDC procedure generates sufficiently accurate statistics or at least informs respondents that the results are insufficiently accurate.

Formal privacy makes an extreme assumption that an intruder has information about all observations in a data set except one. This framework allows for some mathematical conveniences and the ability to maintain a universal privacy loss budget. However, the framework creates the challenge of explainability. Formal privacy is difficult to understand, difficult to implement, and often generates very noisy results that are not useful for levels of privacy budgets typically recommended in the literature.

Formal privacy clearly does not achieve all four of these desired properties. However, to our knowledge, no framework has achieved all four.

### **5 Known Challenges and Opportunities**

Formal privacy is full of promise. The introduction of a quantifiable and finite bound on disclosure risk is groundbreaking and relies on a minimal number of, albeit extreme, assumptions. In many applications, formal privacy will result in better and more robust protections against unintentional disclosures. In some applications, especially applications based on counts, formal privacy could result in more useful data than techniques like swapping.

Formal privacy could also be used to expand access to data. In some applications, noisy statistics from small cells may be preferable to outright suppression. Overall, the robust bound on disclosure risk offered by formal privacy could be used to release data sets that would never be released in the absence of formal privacy. Governments and businesses are sitting on vast troves of information that could be used to learn about the world and promote human flourishing.

Businesses and governments give access to some researchers for research projects. The results of these projects often go through tedious manual reviews for disclosure risks. Formal privacy could allow for automated reviews in a general-purpose validation server (Taylor et al. 2021). It is possible for businesses or governments to use ad hoc reviews to suppress undesirable or

unflattering results. A well-executed formally private method for accessing sensitive data could solve this issue and promote equitable access to data for research.

Formal privacy solves a major limitation of traditional SDC techniques, providing the ability to directly measure the trade-off between data accuracy and privacy protection. But the young technology has other unresolved challenges, such as moving from theoretical work to practice, where the theory is not currently appropriate for many important practical applications. Through formally private use cases, we highlight the various challenges and research opportunities.

## 5.1 Theoretical scenarios and practical applications

As discussed above, the scale of noise added to statistics is often determined by global sensitivity. Privacy experts can easily calculate global sensitivity for certain statistics, such as counts, because the most a count can change with the addition or subtraction of one observation is one. This means many of the real-world applications still apply to only counts of data. For example, two of Google's major applications of formal privacy added noise to counts of bits (Erlingsson, Pihur, and Korolova 2014) or counts of people.<sup>5</sup> The National Institute of Standards and Technology Public Safety Communications Research (NIST PSCR) Division hosted the first "Differential Privacy Synthetic Data Challenge." NIST PSCR tasked competitors to create formally private synthetic data methods. Despite the data being non-tabular (emergency response data and microdata with continuous and categorical data), the competitors considered the data as tabular to apply their methods and then later post-processed the synthetic data to resemble the confidential data structure.

What about other simple statistics? For many common and simple statistics like means and totals, the global sensitivity could be theoretically infinite. Unless the range of the data is known without observing the data, special techniques are required to calculate the global sensitivity for these statistics. The special techniques often result in biased statistics or poor results, especially with skewed distributions.

The challenge of identifying a finite global sensitivity also means that formal privacy only works for certain types of analyses. As mentioned before, Opportunity Insights developed a measure of economic connectedness to estimate what proportion of Facebook friends have above-median socio-economic status. The measure includes a machine learning model to label socioeconomic status, identifying if observations are above or below the median, and evaluating friendships in a network (Chetty, Jackson, Kuchler, Stroebel, Hendren, Fluegge, Gong, Gonzalez, Grondin, Jacob, Johnston, Koenen, Laguna-Muggeburg, et al. 2022). The global sensitivity is intractable. The authors used formally private methods to protect tabular statistics and implemented a non-formally private method based on local sensitivity for economic connectedness even though they used DP for the rest of their metrics.

---

<sup>5</sup>Google COVID-19 community mobility reports: anonymization process description (version 1.1) <https://arxiv.org/abs/2004.04145>

When it is possible to come up with a global sensitivity, the results are often poor even with very large privacy parameters. Additionally, many formal privacy papers often demonstrate methods on data sets that are simulated or too ideal. Methods that appear feasible are often unfeasible in real-world applications.

Another challenge is that formally private methods don't perform well on other types of data, such as text and photos, except in specific applications. Venkatesaramani, Malin, and Vorobeychik (2021) explored the privacy threat of linking public photos to people within genomic data and present their own process of distorting the photo data to protect people's privacy. They showed that a small amount of noise is needed to protect people from being identified in genomic data.

What about a photo of a person in a suburban neighborhood? Bowen and Garfinkel (2021) walks through this example. The entire image could be protected by adding random noise to every pixel, but the result picture would be useless. The person in the image could be altered, such as changing their facial features or hair color, but what if an attacker could identify the house in the background with Google Street View and find where that person lives. Protecting text data has similar issues, such as knowing how to protect certain words or phrases without losing the meaning in the sentence.

We see that there is a huge disconnect between theory and practice. These examples highlight that there are few viable formally private methods to protect certain data types. This is likely why many entities in the private and public sector have not adopted formally private methods. Garfinkel and Bowen (2022) also advised businesses to use formal privacy for small, well-defined pilot projects. Given the void in literature, statisticians have an opportunity to contribute their expertise and be a connector between the theory and practice.

## 5.2 An appropriate and interpretable privacy loss budget

Major challenges persist for formal privacy, even in applications where the global sensitivity is known, and the methods generate reasonable amounts of error. The formal privacy literature largely avoids suggesting the appropriate privacy parameters. Instead, most papers say this decision should be made by policymakers instead of privacy experts. Two major issues intersect with the challenge of picking parameters.

First, applications of formal privacy have adopted large values of  $\epsilon$  because many formally private results are highly inaccurate. These privacy budgets are a big departure from earlier theoretical work. Dwork (2008) called the choice of  $\epsilon$  a social question and said "we tend to think of  $\epsilon$  as, say, 0.01, 0.1, or in some cases,  $\ln 2$  or  $\ln 3$ ." They continued to say that in some cases  $\epsilon$  could be 2 or 3. The applications outlined above use privacy budgets many times greater than 1, 2, or 3.

For instance, when Rogers et al. (2021) introduced their Audience Engagement API to protect LinkedIn members' content engagement data, they compared their daily ( $\epsilon = 0.15$  and  $\epsilon =$



$10^{-10}$ ) and monthly ( $\epsilon = 34.9$  and  $\epsilon = 10^{-9}$ ) privacy loss budget against other big tech implementations of formal privacy. For instance, Google created reports of movement trends over time within certain geographic regions, such as county level in the United States, for six different area types (e.g., residential) to help health policies officials during the COVID-19 pandemic. This formally private application has a daily privacy loss budget  $\epsilon = 2.64$  or a monthly budget of  $\epsilon = 79.2$ .<sup>6</sup>

Second, it is difficult to interpret parameters for formally private methods. This may explain why it is difficult to know what values of  $\epsilon$  are appropriate and why  $\epsilon$  values are higher than originally theorized. For pure DP,  $\epsilon$  places a bound on a log ratio of two probabilities. This ratio represents a difficult to conceive relative risk and is on a log scale.

Table 1: The ratio increases exponentially with  $\epsilon$

$\epsilon$	Ratio
0.25	1.28
0.5	1.65
0.75	2.12
1	2.72
2	7.39
4	54.60
6	403.43
8	2980.96
10	22026.47

Table 1 demonstrates how quickly the ratio in the definition of pure DP explodes as  $\epsilon$  increases by modest amounts. The community does not have a clear way to reason about the difference between a ratio of 2,000 and a ratio of 22,000. On its own,  $\epsilon$  and other privacy parameters in formal privacy, are like a speedometer without any labels. The parameters can show you faster or slower, but they can't tell you how quickly you are going. And without knowing exactly how fast you are going, it's tough to drive near the speed limit. This is why we need people to add context and interpretability to the speedometer.

Privacy experts avoiding budget recommendations and firms adopting relatively large privacy parameters may reflect a more fundamental issue. The firms from the private and public sector may adopt formal privacy as a binary strategy to avoid litigation and regulation. That is, a firm may say the data are absolutely safe because the firm used formal privacy instead of engaging in the much trickier conversation about the trade-off between data utility and disclosure risks with different methods and privacy parameters. If this is the case, then adopting formal privacy may be more smoke and mirrors than privacy revolution.

<sup>6</sup>Google COVID-19 community mobility reports: anonymization process description (version 1.1) <https://arxiv.org/abs/2004.04145>

### 5.3 Biases and uncertainty in statistics

Sometimes formally private estimates can suffer from bias, which can occur for a few different reasons. First, privacy research can bias estimates because values have been truncated to come up with a finite global sensitivity. This is seen in Bowen and Liu (2020) through bounding the values to estimate the global sensitivity for mean.

Second, many post-processing approaches introduce bias from steps as simple as rounding values to integers or rounding negative values to zero. An example of this is the 2020 Census post-processing method called the TopDown Algorithm. At a high level, the U.S. Census Bureau added discrete Gaussian noise to their target statistics, which is roughly over 2,000 target statistics for each census geographic region (states, counties, tracts, block groups, and blocks). The Census Bureau then applied the TopDown Algorithm that enforced invariant statistics (i.e., no change to the statistics) and constraints (J. Abowd et al. 2022). An example of an invariant statistic is total number of housing units within each census block staying the same and an example of a constraint is the population counts in all counties in the state should equal the state population. These post-processing decisions for the TopDown Algorithm biased the 2020 Census data products, which resulted in several top researchers (e.g., two authors of the original DP paper) sending formal letters to the U.S. Census Bureau to release pre-post-processed data, i.e., the “noisy measurements data set” (Dwork, Greenwood, and King 2021).

Finally, adding noise with the same scale to statistics based on differing numbers of observations is another way to introduce bias. This was particularly apparent during the 2020 Decennial Census because of the wide range of sizes of geographies in the US and the distribution of different racial and ethnic groups (Kenny et al. 2021; Kurz et al. 2022).

The 2020 Decennial Census shows how modern SDC methods are trapped in an unfortunate position of balancing between privacy and utility. A data steward can start with principles (e.g., a safe bound on privacy loss and reasonable utility) and end up with inadequate methods, or they can start with methods and end up with inadequate principles (e.g., a murky bound and/or poor data quality).

### 5.4 Communication and education

Besides the technical difficulties of implementing a formally private framework, communicating these major changes to data users became a major challenge for the 2020 Decennial Census. Traditional SDC methods are more intuitive and easier to explain (e.g., aggregating smaller populations to higher levels, such as educational attainment), whereas formally private methods are more complicated and have a non-intuitive interpretation. The communication difficulty led the Census Bureau to hire a senior advisor to focus on communication efforts, but the initial lack of communication and community engagement resulted in several lawsuits

against the Census Bureau's formally private framework.<sup>7</sup> Although the U.S. Census Bureau has since increased their communication and community engagement efforts, such as calling for example use cases<sup>8</sup> and publishing more documentations,<sup>9</sup> many data users still urge the Census Bureau to not implement formal privacy for future census data products.<sup>1011</sup>

As mentioned earlier, top researchers urged the U.S. Census Bureau to release the noisy measurements file so that data users could better account for the bias. However, this would create a new communication issue. How do you explain to data users and other decision-makers that there are two data sets? One data set is similar in structure to past decennial census data products but with biased results. The other data set violates certain physical constraints, such as having negative counts, but allows for data users to conduct bias corrections. In other words, releasing such a file means that data users and practitioners would be expected to understand this difference, know how to properly analyze both sets of data, and know how to explain these different sets of results to decision-makers.

Despite the obvious demand, most higher education institutions do not provide data privacy courses. If they are taught, professors usually teach them at the graduate level in computer science departments. At the undergraduate level, some professors who research data privacy and confidentiality occasionally introduce the topics through seminar courses, but not in separate dedicated courses. This means the important skills and experiences of statisticians, data scientists, data stewards, and data users, who have technical backgrounds outside of computer science, are severely underrepresented.

Academic departments outside of computer science should either create data privacy and confidentiality courses or incorporate these ideas into existing courses. A full course should also move beyond the basic introduction. For instance, a course could demonstrate how to apply appropriate methods to real data and evaluate the effectiveness of these methods. When integrating data privacy and confidentiality concepts, professors could prompt students to think about the legal, social, and ethical ramifications of data privacy and confidentiality as well as the concepts behind data guardianship and custodianship, and data permissions. These ideas can start as early as elementary school to middle school. Instructors can ask students

<sup>7</sup>"Alabama drops lawsuit challenging Census privacy method", <https://apnews.com/article/alabama-lawsuits-census-2020-redistricting-us-census-bureau-3c6f5eacc6c5638756700ba8308c45d2>

<sup>8</sup>"2020 Census Data Products: A Workshop", a committee of the National Academies of Sciences, Engineering, and Medicine Workshop, <https://www.nationalacademies.org/our-work/2020-census-data-products-a-workshop>

<sup>9</sup>"2020 Decennial Census: Processing the Count: Disclosure Avoidance Modernization", <https://www.census.gov/programs-surveys/decennial-census/decade/2020/planning-management/process/disclosure-avoidance.html>

<sup>10</sup>"Researchers ask Census to stop controversial privacy method", <https://apnews.com/article/census-2020-us-bureau-government-and-politics-20e683c71eeb62ee4b7792d7d8530419>

<sup>11</sup>"Census Bureau tables controversial privacy tool for survey", [https://www.washingtonpost.com/politics/census-bureau-tables-controversial-privacy-tool-for-survey/2022/12/14/6240eb42-7bec-11ed-bb97-f47d47466b9a\\_story.html](https://www.washingtonpost.com/politics/census-bureau-tables-controversial-privacy-tool-for-survey/2022/12/14/6240eb42-7bec-11ed-bb97-f47d47466b9a_story.html)

how they would feel if their information is in the data<sup>12</sup> or learn how to find someone from an anonymized data set with a few pieces of public information, such as social media posts.<sup>13</sup>

## 5.5 Resources

The U.S. Census Bureau, large tech companies, and open-source projects supported by technology companies and affluent universities are leading the theoretical and practical development of formal privacy. It's no accident that large, well-resourced institutions are some of the only places where formal privacy has been used.

Ideally, entities in the public and private sector would hire professionals who are experts in data privacy and confidentiality techniques that can design and implement tailored approaches to their applications, evaluate the effectiveness of the approaches, and potentially provide training on the methods to colleagues. However, most entities do not have the resources to hire or contract these experts and likely never will.

Data derived from individuals and the insights they can support are too valuable to outlaw. Heavy regulation will likely reward scale and burden smaller firms who cannot afford privacy expertise, such as when General Data Protection Regulation initially took effect in Europe.<sup>14</sup><sup>15</sup> Educational institutions expanding data privacy education and companies specializing in data privacy and tools they develop could reduce some of this burden. Ultimately, there will always be a tension between disclosure risks and the cost of mitigating disclosure risks, which will be unreachable for a non-trivial number of firms and researchers. Formal privacy does not solve this major problem.

## 6 The Future

Some advocates of formal privacy say the time is now and that all releases should adhere to this standard (J. M. Abowd 2018). Some skeptics of formal privacy argue the opposite. Ruggles and Van Riper (2022) stated "it is apparent that DP for census data is an unfortunate mistake." Others argue that we need to conduct more studies on the impact of formal privacy before it is put into widespread use (Hotz et al. 2022).

<sup>12</sup>Data4Kids: Virtually Teaching Kids about Data Science, <https://www.urban.org/data4kids-virtually-teaching-kids-about-data-science>

<sup>13</sup>"Where's Wenda: An Activity on Teaching Middle-School Students Data Privacy", <https://www.statisticteacher.org/2017/02/22/wheres-wenda/>

<sup>14</sup>"Amid confusion, EU data privacy law goes into effect", <https://apnews.com/article/3b6945f9f5794d87bb5c78bb093f724a>

<sup>15</sup>"Wetherspoons just deleted its entire customer email database – on purpose", <https://www.wired.co.uk/article/wetherspoons-email-database-gdpr>

<sup>16</sup>"More than 1,000 U.S. news sites are still unavailable in Europe, two months after GDPR took effect", <https://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/>

The ideal path forward is likely some middle ground path between the two extreme views. The formal privacy toolkit is incomplete for the SDC needs of modern society. Stewards can't stop releasing data while privacy experts figure out the serious limitations of formal privacy, so there is a role for traditional approaches applied responsibly.

Data stewards could pursue effective and well understood applications of formal privacy, like counts, while pausing and further investigating applications with insufficient results, like regressions. At the same time, the field could open up to a larger and broader set of stakeholders and experts through additional recruitment efforts and robust training. This new and different generation of experts could reinvestigate some of the core ideas and motivations of formal privacy through a new lens. They could also seek to bridge the gap between the theory and the practice of formal privacy.

The promise of formal privacy is diminished by its limitations, but these limitations are far from fatal. Formal privacy is now an important tool in the SDC toolbox, and its uses will grow with time.

## **7 Acknowledgments**

### **7.1 Funding**

This research was funded by the NSF National Center for Science and Engineering Statistics [49100422C0008].

### **7.2 Collaborators**

We would like to thank Jennifer Andre for reviewing our paper.

### **7.3 Contributions**

ARW: Conceptualization, Visualization, Writing – original draft (lead), and Writing – review & editing

CMB: Conceptualization, Writing – original draft, and Writing – review & editing

## References

- Abowd, John M. 2018. "Staring-down the Database Reconstruction Theorem," July. <https://www.census.gov/content/dam/Census/newsroom/press-kits/2018/jsm/jsm-presentation-database-reconstruction.pdf>.
- 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>.
- Abowd, John, Robert Ashmead, Ryan Cumings-Menon, Simson Garfinkel, Daniel Kifer, Philip Leclerc, William Sexton, Ashley Simpson, Christine Task, and Pavel Zhuravlev. 2021. "An Uncertainty Principle Is a Price of Privacy-Preserving Microdata." *Advances in Neural Information Processing Systems* 34: 11883–95.
- Bowen, Claire McKay, and Simson Garfinkel. 2021. "Philosophy of Differential Privacy." *Notices of the American Mathematical Society* 68: 1727–39.
- Bowen, Claire McKay, and Fang Liu. 2020. "Comparative Study of Differentially Private Data Synthesis Methods." *Statistical Science* 35 (2): 280–307.
- Bowen, Claire McKay, Aaron R Williams, and Madeline Pickens. 2022. "Decennial Disclosure."
- Bun, Mark, and Thomas Steinke. 2016. "Concentrated Differential Privacy: Simplifications, Extensions, and Lower Bounds." In, edited by Martin Hirt and Adam Smith, 9985:635–58. Berlin, Heidelberg: Springer Berlin Heidelberg. [http://link.springer.com/10.1007/978-3-662-53641-4\\_24](http://link.springer.com/10.1007/978-3-662-53641-4_24).
- Chetty, Raj, Matthew O. Jackson, Theresa Kuchler, Johannes Stroebe, Nathaniel Hendren, Robert B. Fluegge, Sara Gong, Federico Gonzalez, Armelle Grondin, Matthew Jacob, Drew Johnston, Martin Koenen, Eduardo Laguna-Muggeburg, et al. 2022. "Social Capital I: Measurement and Associations with Economic Mobility." *Nature* 608 (7921): 108–21. <https://doi.org/10.1038/s41586-022-04996-4>.
- Chetty, Raj, Matthew O. Jackson, Theresa Kuchler, Johannes Stroebe, Nathaniel Hendren, Robert Fluegge, Sara Gong, Federico Gonzalez, Armelle Grondin, Matthew Jacob, Drew Johnston, Martin Koenen, Eduardo Laguna-Muggeburg, et al. 2022. "Codebook for Publicly Available Data on Social Capital." [https://s3.us-east-1.amazonaws.com/hdx-production-filestore/resources/fbe5b0b9-e81c-41c7-a9f2-3ebf8212cf64/data\\_release\\_readme\\_31\\_07\\_2022\\_nomatrix.pdf?AWSAccessKeyId=AKIAXYC32WNARK756OUG&Signature=Pxlwx%2BkP4zfzIRJiRDYh%2BQx1Kus%3D&Expires=1663162869](https://s3.us-east-1.amazonaws.com/hdx-production-filestore/resources/fbe5b0b9-e81c-41c7-a9f2-3ebf8212cf64/data_release_readme_31_07_2022_nomatrix.pdf?AWSAccessKeyId=AKIAXYC32WNARK756OUG&Signature=Pxlwx%2BkP4zfzIRJiRDYh%2BQx1Kus%3D&Expires=1663162869).
- Differential Privacy Team, Apple. n.d. "Learning with Privacy at Scale." <https://docs-assets.developer.apple.com/ml-research/papers/learning-with-privacy-at-scale.pdf>.
- Dinur, Irit, and Kobbi Nissim. 2003. "The Twenty-Second ACM SIGMOD-SIGACT-SIGART Symposium." In, 202–10. San Diego, California: ACM Press. <https://doi.org/10.1145/773153.773173>.
- Dwork, Cynthia. 2008. "Differential Privacy: A Survey of Results." In, edited by Manindra Agrawal, Dingzhu Du, Zhenhua Duan, and Angsheng Li, 4978:1–19. Berlin, Heidelberg: Springer Berlin Heidelberg. [http://link.springer.com/10.1007/978-3-540-79228-4\\_1](http://link.springer.com/10.1007/978-3-540-79228-4_1).



- Dwork, Cynthia, Ruth Greenwood, and Gary King. 2021. "Letter to US Census Bureau: "Request for Release of "Noisy Measurements File" by September 30 Along with Redistricting Data Products"."
- Dwork, Cynthia, Krishnaram Kenthapadi, Fang McSherry, Ilya Mironov, and Moni Naor. 2006. "Our Data, Ourselves: Privacy via Distributed Noise Generation." In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 486–503. Springer.
- 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](http://link.springer.com/10.1007/11681878_14).
- Dwork, Cynthia, and Aaron Roth. 2014. "The Algorithmic Foundations of Differential Privacy." *Foundations and Trends® in Theoretical Computer Science* 9 (3–4): 211–407.
- Erlingsson, Úlfar, Vasyl Pihur, and Aleksandra Korolova. 2014. "Rappor: Randomized Aggregatable Privacy-Preserving Ordinal Response." In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 1054–67.
- Garfinkel, Simson L, and Claire McKay Bowen. 2022. "Preserving Privacy While Sharing Data." *MIT Sloan Management Review* 63 (3): 1–4.
- Gong, Ruobin. 2022. "Transparent Privacy Is Principled Privacy." *Harvard Data Science Review*, no. Special Issue 2 (June). <https://doi.org/10.1162/99608f92.b5d3faaa>.
- Hawes, Michael. 2021. "Understanding the 2020 Census Disclosure Avoidance System: Simulated Reconstruction-Abetted Re-Identification Attack on the 2010 Census," May. <https://www2.census.gov/about/training-workshops/2021/2021-05-07-das-presentation.pdf>.
- Hotchkiss, Marisa, and Jessica Phelan. 2017. "Uses of Census Bureau Data in Federal Funds Distribution." <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, Christopher R. Bollinger, Tatiana Komarova, Charles F. Manski, Robert A. Moffitt, Denis Nekipelov, Aaron Sojourner, and Bruce D. Spencer. 2022. "Balancing Data Privacy and Usability in the Federal Statistical System." *Proceedings of the National Academy of Sciences* 119 (31): e2104906119. <https://doi.org/10.1073/pnas.2104906119>.
- Kenny, Christopher T., Shiro Kuriwaki, Cory McCartan, Evan T. R. Rosenman, Tyler Simko, and Kosuke Imai. 2021. "The Use of Differential Privacy for Census Data and Its Impact on Redistricting: The Case of the 2020 U.S. Census." *Science Advances* 7 (41): eabk3283. <https://doi.org/10.1126/sciadv.abk3283>.
- Kurz, Christoph F., Adriana N. König, Karl M. F. Emmert-Fees, and Lindsay D. Allen. 2022. "The Effect of Differential Privacy on Medicaid Participation Among Racial and Ethnic Minority Groups." *Health Services Research*, May, 1475–6773.14000. <https://doi.org/10.1111/1475-6773.14000>.
- Li, Ninghui, Min Lyu, Dong Su, and Weining Yang. 2016. "Differential Privacy: From Theory to Practice." *Synthesis Lectures on Information Security, Privacy, & Trust* 8 (4): 1–138.
- Lohr, Steve. 2010. "Netflix Cancels Contest After Concerns Are Raised about Privacy." *The New York Times*, March. <https://www.nytimes.com/2010/03/13/technology/13netflix>.

- [html](#).
- Machanavajjhala, Ashwin, Daniel Kifer, John Abowd, Johannes Gehrke, and Lars Vilhuber. 2008. "Privacy: Theory Meets Practice on the Map." *24th Institute of Electrical and Electronics Engineers International Conference on Intelligent Transportation Systems*, 277–86.
- McClure, David, and Jerome P Reiter. 2012. "Differential Privacy and Statistical Disclosure Risk Measures: An Investigation with Binary Synthetic Data." *Trans. Data Priv.* 5 (3): 535–52.
- McKenna, Ryan, Daniel Sheldon, and Gerome Miklau. 2019. "Graphical-Model Based Estimation and Inference for Differential Privacy." *Proceedings of the 36th International Conference on Machine Learning* 97: 4435–44. <http://proceedings.mlr.press/v97/mckenna19a/mckenna19a.pdf>.
- McSherry, Frank D. 2009. "SIGMOD/PODS '09: International Conference on Management of Data." In, 19–30. Providence Rhode Island USA: ACM. <https://doi.org/10.1145/1559845.1559850>.
- Mironov, Ilya. 2017. "Rényi Differential Privacy." In *Institute of Electrical and Electronics Engineers 30th Computer Security Foundations Symposium*, 263–75. Institute of Electrical; Electronics Engineers.
- Narayanan, Arvind, and Vitaly Shmatikov. 2008. "2008 IEEE Symposium on Security and Privacy (Sp 2008)." In, 111–25. Oakland, CA, USA: IEEE. <https://doi.org/10.1109/SP.2008.33>.
- Nissim, Kobbi, Sofya Raskhodnikova, and Adam Smith. 2007. "Smooth Sensitivity and Sampling in Private Data Analysis." In *Proceedings of the 39th Annual Association for Computing Machinery Symposium on Theory of Computing*, 75–84. Association for Computing Machinery.
- Reiter, Jerome P. 2005. "Estimating Risks of Identification Disclosure in Microdata." *Journal of the American Statistical Association* 100 (472): 1103–12.
- Rogers, Ryan, Subbu Subramaniam, Sean Peng, David Durfee, Seunghyun Lee, Santosh Kumar Kancha, Shraddha Sahay, and Parvez Ahammad. 2021. "LinkedIn's Audience Engagements API: A Privacy Preserving Data Analytics System at Scale." *Journal of Privacy and Confidentiality* 11 (3). <https://doi.org/10.29012/jpc.782>.
- Ruggles, Steven, and David Van Riper. 2022. "The Role of Chance in the Census Bureau Database Reconstruction Experiment." *Population Research and Policy Review* 41 (3): 781–88. <https://doi.org/10.1007/s11113-021-09674-3>.
- Slavković, Aleksandra, and Jeremy Seeman. 2023. "Statistical Data Privacy: A Song of Privacy and Utility." *Annual Review of Statistics and Its Application* 10 (1). <https://doi.org/10.1146/annurev-statistics-033121-112921>.
- Sweeney, Latanya. 2000. "Simple Demographics Often Identify People Uniquely." *Health (San Francisco)* 671 (2000): 1–34.
- Taylor, Silke, Graham MacDonald, Kyle Ueyama, and Claire McKay Bowen. 2021. "A Privacy-Preserving Validation Server Prototype." <https://www.urban.org/research/publication/privacy-preserving-validation-server-prototype>.
- Thompson, Stuart A, and Charlie Warzel. 2019. "Twelve Million Phones, One Dataset, Zero



- Privacy." In *Ethics of Data and Analytics*, 161–69. Auerbach Publications.
- Venkatesaramani, Rajagopal, Bradley A Malin, and Yevgeniy Vorobeychik. 2021. "Re-Identification of Individuals in Genomic Datasets Using Public Face Images." *Science Advances* 7 (47): eabg3296.
- 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.
- Warner, Stanley L. 1965. "Randomized Response: A Survey Technique for Eliminating Evasive Answer Bias." *Journal of the American Statistical Association* 60 (309): 63–69.

Aaron R. Williams

[awilliams@urban.org](mailto:awilliams@urban.org)

Urban Institute, Washington, District of Columbia, United States

Claire McKay Bowen

[CBowen@urban.org](mailto:CBowen@urban.org)


Urban Institute, Washington, District of Columbia, United States




WICS\_1615\_graphical-visual-abstract-small.jpg

state	employees	income	
01	#	#	}
01	#	#	
01	#	#	
02	#	#	}
02	#	#	
02	#	#	
03	#	#	}
03	#	#	
03	#	#	
03	#	#	


Analysis 1


 $\epsilon_1 = 1$

Analysis 1


 $\epsilon_2 = 0.5$

Analysis 1


 $\epsilon_3 = 0.5$

WICS\_1615\_parallel.TIF

state	employees	income
01	#	#
01	#	#
01	#	#
02	#	#
02	#	#
02	#	#
03	#	#
03	#	#
03	#	#
03	#	#



$$\epsilon_1 = 1$$



$$\epsilon_2 = 0.5$$



$$\epsilon_3 = 0.5$$

WICS\_1615\_sequential.TIF