

Differential Privacy – research report

Privacy Technologies for Financial Intelligence



Trimester 3, 2023

Deakin University

By Heera Mohanadas, Brett Youngman & Scott West

Contents

[What is differential privacy? Overview 2](#_Toc153196811)

[The Strengths, Weaknesses, and Challenges of Differential Privacy 3](#_Toc153196812)

[Trade-off: Accuracy vs Privacy 3](#_Toc153196813)

[Trade-off: Sharing data vs Sharing bad data 3](#_Toc153196814)

[Differential Privacy in Machine Learning 3](#_Toc153196815)

[Differential Privacy Offers Deniability 4](#_Toc153196816)

[Methods of Noise Injection 4](#_Toc153196817)

[Method of ‘Privacy Budget’ 4](#_Toc153196818)

[Advantages of Differential Privacy: A Summary 5](#_Toc153196819)

[Disadvantages of Differential Privacy: A Summary 5](#_Toc153196820)

[Comparison of Differential Privacy and Other Privacy Enhancing Technology (PET) 6](#_Toc153196821)

[Differential Privacy and Federated Learning 6](#_Toc153196822)

[Differential Privacy and Homomorphic Encryption 6](#_Toc153196823)

[BIBLIOGRAPHY 8](#_Toc153196824)

[Applying Differential Privacy 12](#_Toc153196825)

[Benefits of Differential Privacy for Implementation 12](#_Toc153196826)

[References for Scott West 12](#_Toc153196827)

Understanding Differential Privacy by Heera Mohanadas & Brett Youngman

# What is differential privacy? Overview

According to Dwork (2008) differential privacy uses algorithms to introduce small random changes, or noise, into datasets containing personal information from individual people; this acts to preserve the privacy of these individuals, while maintaining the statistical characteristics of the datasets. Dwork (2008) accepts that differential privacy does not eliminate risk, but rather ‘ensures … a limited amount of additional risk’ (Dwork p.3) which is assumed to be outweighed by other benefits provided by the database’s existence and use. The larger the database, the lower the risk that differential privacy techniques will result in privacy loss.

Nissim et al. (2018) define differential privacy as ‘a strong, mathematical definition of privacy in the context of statistical and machine learning analysis’ which enables collection, analysis and sharing of data derived from individual people, while maintaining these individuals’ privacy. Rather than describing a specific tool or algorithm, differential privacy is a ‘mathematically provable guarantee’ (Nissim et al, 2018 p.2) that a technique protects against ‘privacy attacks’' designed to identify individuals in a given dataset. Further, Nissim et al. (2018, p.2) consider differential privacy to provide specific metrics of privacy loss by being able to quantify privacy loss as a mathematical function (ε) which allows comparison of differential privacy techniques and can assist data holders to demonstrate compliance with privacy laws and standards.

Near and Darais (2020) concur with Nissim et al. (2018) and their view that differential privacy is a mathematical standard or property which an algorithm can satisfy, rather than a process in and of itself. They expound on this by examining the trade-off between higher privacy and lower result accuracy: adding additional noise to results lowers the privacy loss value (ε), but also reduces the accuracy of results from queries on the database. A balance needs to be struck between protecting individual privacy and achieving useful database query results, this has been described in the literature as a ‘privacy budget’ (Wright 2019). Near and Darais’ (2021) are careful to draw a distinction between the mathematical guarantee of privacy and its associated privacy loss value (ε), and real-world applications of differential privacy. They discuss the ways in which software bugs can create exploitable flaws in the mathematical guarantee and undermine the application of the technology. They identify two common causes of bugs: 1) adding the wrong amount of noise, and 2) incorrectly calculating a function’s sensitivity. These observations highlight the importance of thoroughly testing the implementation of a differential privacy technology which may in theory provide satisfactory privacy but fail in implementation and unintentionally or negligently expose private information.

A common use case cited for differential privacy is in making census data public. Near et al (2020) citing the work of Sweeney (2000), among others, refer to the traditional use of de-identification as a privacy preserving technique which is not quantifiable and which is vulnerable to re-identification attacks where datasets are combined and then used to infer individual identities and reconstruct data which has been removed. Near et al. (2020) consider differential privacy is a more reliable method to preserve privacy in such datasets as privacy loss can be quantified (ε) and calibrated based on risk appetite, whereas de-identification cannot make the same mathematical guarantee. The quantification and comparison of privacy risk is one of the key advantages of correctly implemented differential privacy techniques.

# The Strengths, Weaknesses, and Challenges of Differential Privacy

As noted by Wayner (2021) differential privacy’s proposed algorithms rely on the addition of enough “noise” to make it impossible or at least unlikely for an adversary to be able to pluck the data of a single individual from a noisy set of data, which is the approach’s main guarantee as highlighted by Wright (2019). Moreover, it is crucial to remember that the application and theorisation of differential privacy is motivated by organisations’ need to use data to conduct research; as data that is safely locked away does not allow for aggregation for statistical analysis and cannot be analysed to train machine learning algorithms (Wayner 2021).

Previously mentioned are the two main concerns that accompany the usage of differential privacy: a) the query sensitivity and b) the implementation of a “privacy budget” to be expanded on later (Wright 2019). It is essential to keep in mind that foundation of differential privacy is the concept of concealing the participation a single person (Wright 2019) to ensure privacy protection independent of attack models (Kan 2023).

## Trade-off: Accuracy vs Privacy

Moreover, when it comes to the adoption of the differential privacy framework, there will always be a trade-off between privacy and accuracy (Wayner 2021). All algorithms made with respect to differential privacy often include the Greek letter epsilon, used to signify the ‘privacy parameter’ for the idea of a ‘privacy budget’; applied in an inverse manner where large values of epsilon result in almost no change in the dataset accuracy, while small values of epsilon result in the injection of large amounts of noise (Wayner 2021). This notion is echoed by Wright (2019) who acknowledges that maintaining the privacy of individuals and their data comes at the expense of having precise answers to queries.

Essentially, the advantage of this approach is that where the epsilon value is large there is almost no change in the resulting dataset’s accuracy when responding to queries. However, there is still no definitive way to choose a good epsilon value (Wayner 2021) and the best practices to determine an epsilon value have not been identified. The issue concerning the determination of an epsilon value arises because setting such a value is complex, especially in cases where datasets are less predictable (Wayner 2021). Accordingly, it will mostly be a practice of trial and error to identify the best epsilon value that will create an ‘ideal’ noise level to blur the distinction between individual data.

## Trade-off: Sharing data vs Sharing bad data

This means that while the goal of being able to share data is achieved (Wayner 2021), the data is shared at the expense of it having “bad” or “noisy” data included. While lower-level queries, such as the computation of the mean, would allow for the errors to be cancelled out and still result in accurate measures of the data, more complex queries will result in inaccurate measures (Wayner 2021). This is contrary to the ultimate goal of differential privacy, which arose from the need of organisations from distinct and separate sections needing to share information without sacrificing the privacy of the individuals’ datum it collects (Wayner 2021).

## Differential Privacy in Machine Learning

While the differential privacy framework enables the sharing of large amounts of data necessary to train machine learning algorithms the noise injected into the datasets may have unknown effects on query results (Wayner 2021). For instance, there are reports that differential privacy results can sometimes have the effect of compounding the errors within a study (Fredrikson 2014).

## Differential Privacy Offers Deniability

As described by Wayner (2021), differential privacy has the added advantage of offering deniability to individuals as the information they have given in a dataset might just be a random lie outputted by the noise injecting algorithm. Hence, there is a reduction in liability as a result of the deniability offered by this approach. However, this raises an additional concern, where people still lie about their answers because they do not want truthful information about themselves leaking out (Wayner 2021); this means that differential privacy, while adding additional errors (noise), may already be subject to errors because of research participants or the falsification of data already present in the dataset.

## Methods of Noise Injection

There are countless algorithms created for the usage of achieving differential privacy (Wayner 2021) but there are two main and distinct methods of implementing the approach as noted by Wright (2019): output noise injection and input noise injection. Both methods pose their own issues and concerns.

To start, output noise injection, as described by Wright (2019), ‘involves the addition of noise at the query level’; where the algorithm is applied correctly and with the right epsilon value it is sufficient to guarantee the system as differentially private. While this method offers protection from basic dataset reconstruction attacks Wright (2019) also notes that more intelligent approaches to the reconstruction of the dataset can result in sets of microdata that are often most consistent with the original dataset, thought they will still device from the original.

Input noise injection, as described by Wright (2019), is where noise is added to the dataset before the data is tabulated. There are various downsides to this, including that the same level of inaccuracy is received by each query as access to the same noisy datasets is given to all users (Wright 2019). Additionally, Wright (2019) notes, the input noise injection approach is still susceptible to database reconstruction attacks, though the reliability of such reconstructed data is limited.

There is the additional method of adding noise by ‘swapping’, as described by Wright (2019), where row values within each column of the dataset are randomly swapped. While theoretically this method has some great features, in actual use a substantial quantity of rows would need to be switched to preserve each participant’s anonymity and hence privacy. There is also the additional disadvantage of the operation having no impact on outcomes of high-level queries; for instance, the swapping of two rows lists A as having brown eyes instead of green, and B as having green eyes instead of brown, meaning that the overall counts of individuals with green eyes or brown eyes remains the same (Wright 2019).

## Method of ‘Privacy Budget’

The ‘privacy budget’ method is a means of controlling the level of noise injected into a dataset as a result of a query being made (Wright 2019). Essentially, the idea of a ‘privacy budget’ can be implemented in two ways, as explained by Wright (2019). The first way is where there is a quota on how may queries can be made in reference to a specific dataset, and when the quota is reached no more queries can be made because of the amount of noise being injected into the dataset rendered it too inaccurate for a meaningful statistical analysis to be made (Wright 2019). The second way is to set a privacy budget, where the noise injected into the dataset is halved each time, and the quantity of queries to be made is never limited; instead, the dataset just becomes less and less accurate (Wright 2019). The second approach would mean that the user making queries would have to save their most important queries to be the first ones they make, to ensure that their queries are exposed to the least amount of noise (Wright 2019).

However, while this method contains a means to control the level of noise that a dataset is exposed to, Kan (2023) notes a glaring deficiency in the algorithm’s application; namely, there is no current consensus on the level of privacy budget that is sufficient for protecting privacy in practice.

# Advantages of Differential Privacy: A Summary

Kan (2023) highlights some broad advantages of differential privacy, noting the trade-offs and disadvantages of each approach discussed above; namely, differential privacy ensures protection of the privacy of individuals independent of attack models applied by adversaries. This is because of the precautionary nature of the approach, Kan (2023) describes, which is desirable in the future because it means that the data of a single individual cannot be reconstructed or identified confidently despite the many organisations that might gain access to the data. Kan (2023) also emphasises that differential privacy implementation is advantageous in situations where databases accept and respond to a wide variety of queries; so, it might not be the optimal choice for databases which accept limited types of queries.

Wayner (2021) emphasises that differential privacy is something of a philosophical approach, in that many different algorithms can achieve the outcomes that are desired from the approach, while not producing the same outcome each and every time. Specifically, there are countless researchers who evolve and create new differential privacy algorithms that offer slightly different guarantees; lots of different options to be explored to protect data (Wayner 2021). Moreover, these algorithms are supposedly built to be chained together (Wayner 2021); the theoretical foundations of the framework explain how various algorithms can be layered atop one another to protect different points (Wright 2019). For instance, the OpenDP project aims to deliver a broad collection of algorithms that can work together to protect data; one algorithm might protect Point A, while another algorithm protects Point B, and when layered on top one another they protect both points (Wayner 2021).

With the use of the epsilon value, present in the majority of differential privacy algorithms, there is a mathematical bound to identify how much information, if any, is leaking with each query made (Wayner 2021).

# Disadvantages of Differential Privacy: A Summary

As there are multiple algorithms enabling the implementation of this privacy-protection framework, each offering their own guarantee of protection, there are no firm guarantees because not all algorithms will fit the wide-open model of the internet (Wayner 2021). For example, there may be slow leaks in the data, where some queries leak a small, manageable amount of information that is true. The issue arises where the attacker is able to repeat similar queries, with leaks compounding, and rendering the total loss significant. This means that architects for the implementation of the framework must ensure that their privacy models do not allow for leaks in data to compound (Wayner 2021).

A disadvantage of the differential privacy, applicable regardless of the method of its implementation, is that when datasets are small, adding noise can result in bigger distortions of the data (Wayner 2021).

# Comparison of Differential Privacy and Other Privacy Enhancing Technology (PET)

It is important to note that in the comparison of differential privacy and other privacy enhancing technology (PET), that what differential privacy is most suited for might not be what another technology is suited for. In noting that, differential privacy is most suited for usage in the sharing of information and training of machine learning or AI models.

Hence, differential privacy will only be considered for comparisons with PET useful for sharing data; to compare it to privacy measures geared towards it cannot do is redundant and will not be recounted here.

## Differential Privacy and Federated Learning

To start, federated learning (FL), also known as federated analytics or analysis, is a technique where the insights of a dataset are shared, rather than a raw dataset itself, and the individual models trained on its dataset are moved to a centralised model (OPC Blogger, 2021). This means that, unlike in differential privacy, in adopting the FL approach the data never leaves its source (McMahan, 2023). Moreover, it means that the insights are already there and there is no risk of the privacy of individuals being at risk. However, federated learning does not allow for individual organisations to gather their own insights from the datasets, rather, organisations are only able to utilise results from queries already made into the dataset; if they want a specific query to be made, they would have to request it from the host of the original data.

FL and differential privacy are similar in that they share the potential to be used for machine learning (OPC Blogger, 2021), however, FL has a more focused intent whereas differential privacy enables different queries to be made in relation to a dataset; insights made from FL are arguably more reliable because they are not subject to the “noise” that differential privatised datasets are.

Both FL and differential privacy are similar in that they carry great computational cost (Wright 2019 and McMahan 2023); FL’s cost is generated from the frequency and cost of moving the smaller, individual models to the centralised models and differential’s privacy’s cost arises from its implementation and the computational cost. Moving and sharing of data is no issue under differential privacy, rather the aim is for its datasets to be shared with the open web (Wayner 2021); FL’s aims is for the insights of datasets to be shared amongst trusted parties. Moreover, differential privacy computation is not well-suited to data of many data sources and data types (OPC Blogger, 2021) whereas federated learning is.

## Differential Privacy and Homomorphic Encryption

For the sharing of financial data while preserving the personally identifiable information of individuals DP is more well-suited to the task than homomorphic encryption (HE), considering the conclusions and uses evaluated by Vaikuntanathan (2011:5-16). Namely, HE allows for computations and insights to be gathered on encrypted data, with the insights themselves remaining encrypted so that the evaluator assessing the data for an individual cannot see any data that is personally identifiable (Weinkauf 2023). This means that, unlike differential privacy, HE is not made to be used to supply information to machine learning models. So, why bother with the comparison to DP?

HE is made with the intention for individuals or organisations to be able to entrust encrypted data to a third party to have extra analysis performed, which their own systems may not allow for, and to gain the extra analyses without having to just trust in the way a third party handles their data since the data shared remains encrypted throughout the entire process (Vaikuntanathan 2011:5-16). Similarly, DP was created with the intention to share data and result in extra insights, without compromising an individual’s privacy. However, DP and HE differ in that the insights gained according to that information remain hidden for homomorphically encrypted datasets, unlikely to be shared and instead held private by the person or organisation that request it (Vaikuntanathan 2011:5-16).

There is also the challenge of implementing a fully functional HE, which allows for a range of functions and computations to be made, rather than restricting the computations to a series of families of functions (Vaikuntanathan 2011:5-16). This was a challenged demonstrated by Sahai and other researchers, who noted that while HE schemes work for several types of functions, the creation of an encryption scheme that is fully functional is still wide open (Sahai 2005:457-747). DP, on the other hand, does not have this issue; there is no restriction on the queries made to the differentially private datasets (Wayner 2021).

# BIBLIOGRAPHY

Agrawal S, Freeman D, and Vaikuntanathan V (2011) ‘Functional Encryption for Inner Product Predicates from Learning with Errors’*, ASIACRYPT 2011*, accessed 27 November 2023. https://doi.org/10.1007/978-3-642-25385-0\_2

Boneh D, Segev G, and Waters B (2012) ‘Targeted malleability: Homomorphic Encryption for restricted computations, Cryptology ePrint Archive’, *IACR*, accessed 27 November 2023. http://eprint.iacr.org/2011/311

Dwork C (2008) ‘Differential Privacy: A Survey of Results’, *Microsoft Research.* Available at: https://web.cs.ucdavis.edu/~franklin/ecs289/2010/dwork\_2008.pdf (Accessed: 28 November 2023).

Fredrikson M, Lantz E, Jha S, Lin S, Page D, and Ristenpart T (2014) ‘Privacy in Pharmacogenetics: An End-to-End Case Study of Personalized Warfarin Dosing’, *USENIX The Advanced Computing Systems Association*, accessed 20 November 2023. https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-fredrikson-privacy.pdf

Kan K (2023) ‘Seeking the Ideal Privacy Protection: Strengths and Limitations of Differential Privacy’, *IMES*, accessed 19 November 2023. Available at: https://www.imes.boj.or.jp/research/papers/english/23-E-02.pdf

Katz J, Sahai A, and Waters B (2008:146-162) ‘Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products’, *EUROCRYPT 2008*, accessed on 27 November 2023. https://doi.org/10.1007/978-3-540-78967-3\_9

Lewko A (2010:62-91). ‘Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption’, *EUROCRYPT 2010*, accessed on 27 November 2023. https://doi.org/10.1007/978-3-642-13190-5\_4

Majumdar I, Soni H, Chubb C, and Uykhur D (2019) ‘Data sharing in financial services: Five techniques to enhance privacy and confidentiality’, *Deloitte*, accessed 23 November 2023. https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/Deloitte\_WEF\_FS\_Executive\_summary\_Data\_sharing\_2019.pdf

McMahan B, Moore E, Ramage D, Hampson S and y Arcas B (2023:1273-1282), ‘Communication-Efficient Learning of Deep Networks from Decentralized Data’, *Artificial intelligence and* statistics, accessed 24 November 2023. <https://arxiv.org/pdf/1602.05629.pdf>

Near J, Darais D, Boeckl K (2020) ‘Differential Privacy for Privacy-Preserving Data Analysis: An Introduction to our Blog Series’, *National Institute of Standards and Technology*, accessed 28 November 2023. https://www.nist.gov/blogs/cybersecurity-insights/differential-privacy-privacy-preserving-data-analysis-introduction-our

Near J and Darais D (2021), ‘Differential Privacy Bugs and Why They’re Hard to Find’, *National Institute of Standards and Technology,* accessed 28 November 2023. https://www.nist.gov/blogs/cybersecurity-insights/differential-privacy-bugs-and-why-theyre-hard-find

Nissim K (2018), ' Differential Privacy: A Primer for a Non-technical Audience∗’, *Privacy Tools for Sharing Research Data at Harvard University,* accessed on 28 November 2023. https://privacytools.seas.harvard.edu/files/privacytools/files/pedagogical-document-dp\_new.pdf

OPC Blogger, Office of the Privacy Commissioner of Canada (12 April 2021) *Privacy Tech-Know blog: Privacy Enhancing Technologies for Businesses*, Government of Canada, accessed 24 November 2023. https://www.priv.gc.ca/en/blog/20210412/

Sahai A and Waters B (2005:457-47) *Fuzzy Identity-Based Encryption. In: Cramer, R. (eds) Advances in Cryptology – EUROCRYPT 2005*. EUROCRYPT 2005. Lecture Notes in Computer Science, vol 3494. Springer, Berlin, Heidelberg, accessed 27 November 2023. https://doi.org/10.1007/11426639\_27

Sweeney, L. (2000) ‘Simple Demographics Often Identify People Uniquely’, *Data Privacy Working Paper,* Volume 3, pp. 2-34. Available at: https://dataprivacylab.org/projects/identifiability/paper1.pdf (Accessed: 28 November 2023).

Vaikuntanathan V (2011:5-16) "Computing Blindfolded: New Developments in Fully Homomorphic Encryption," 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science, Palm Springs, CA, USA, doi: 10.1109/FOCS.2011.98, accessed 27 November 2023. https://www.cs.toronto.edu/~vinodv/FHE-focs-survey.pdf

Wayner P (2021) ‘Differential Privacy: Pros and cons of enterprise use cases’, *csoonline.com*, 4 January, accessed 19 November 2023. https://www.csoonline.com/article/570203/differential-privacy-pros-and-cons-of-enterprise-use-cases.html

Weinkauf D (24 October 2023) *Privacy Tech-Know blog: Computing while blindfolded – Lifting the veil on homomorphic encryption*, Government of Canada, accessed on 24 November 2023. https://www.priv.gc.ca/en/blog/20231024/

Wright C and Rumsey K (2019) *The Strengths, Weaknesses and Promise of Differential Privacy as a Privacy-Protection Framework*, *Math Univeristy of New Mexico,* accessed 19 November 2023. https://math.unm.edu/~knrumsey/pdfs/projects/DifferentialPrivacy.pdf

Applications of Differential Privacy by Scott West

*Financial Services Sector*

Differential Privacy holds promise in the financial services sector. It can assist with protecting sensitive financial information, allowing data to be shared securely for business purposes. It in particular holds promise for retail banks, insurers, payment service providers and accounting firms (Deloitte 2019).

Some specific applications of Differential Privacy (DP) within financial services include individual credit assessment, fraud detection and anti-fraud measures (Ma, Lu et Zhang 2023). Further areas where Differential Privacy application is actively being explored includes spending amounts and payment information. This is sensitive in nature, and it can be necessary to share for business.

In terms of individual credit assessment, there is potential to protect sensitive credit risk information through Differential Privacy. Credit risk measures the risk of loss to the lender if the borrower does not meet required repayments. Such risk is quantified via three major components: Probability of Default (PD), Exposure at Default (EAD) and Loss Given Default (LGD) (Maniar & Akkinepally & Sharma 2021). These models can be complex and require the incorporation of Know Your Customer (KYC) information, ranging from user age, location, demographic and sociographic features to calculate the risk level. Using this information in the algorithms possess a risk of privacy breaches either internally or externally for the institution.

These privacy breaches are a significant risk for financial services institutions and their customers. For example, if an organisation is exposed to a breach, then consumers can be subject to identity theft and financial loss. An organisation holding data which is subject to such breaches can therefore face repercussions (Federal Trade Commission 2022). As a result, there is certainly interest in applying Differential Privacy to protecting consumer financial data being an active area of research.

Maniar, Sharma and Akkinepally (2021) applied Differential Privacy to build credit risk models. In the process of building the models, random noise was added to the data sets for protecting sensitive information. Differentially Private (DP) models were then compared to Non-Differentially Private Models (NDPM). Results from the research was promising for using Differential Privacy (DP) as a privacy preserving technology in credit analysis. For example, there was a less than 5% change in the aggregated expected loss prediction. A much lower information loss than expected at the start of the analysis. However, it is noted that variance greatly increased with runs. Another drawback noted in their experiment was the processing time for DP algorithms was much higher than NDPM.

Another application of Differential Privacy is to credit card data. Data analysis of credit card data is prominent in various ways such as user behaviour, financial transactions and market analysis. With the proliferation of credit card data, the risk of data breaches has further increased exponentially.

*Machine Learning*

In a research paper, Luo, Wang, Chen and Luo (2023) explored the application of Differential Privacy to credit card transactions. They found that “*In a broader perspective, all three LDP mechanisms display a commendable ability to ensure that the utility of the data remains consistent with that of the original dataset.*” Most of the Machine Learning algorithms were robust and able to incorporate Differential Privacy effectively. However, the importance of selecting the right Differential Privacy (DP) Machine Learning algorithm based on the data set and mathematical characteristics was noted as paramount.

*Deep Learning*

Another research paper from Kumar et. al. (2023) uses Deep Neural Networks exploring the application of statistical differential privacy algorithms within such a context. It outlines how Privacy Preserving Deep Learning (PPDL) is a very exciting field combining privacy preserving techniques with the emerging Deep Learning domain. Financial Services, Marketing and medical datasets are used in testing. The paper outline that many privacy preserving algorithms are more suited to numerical data, compared to categorical data. With this in mind, the paper finds that the Deep Neural Networks have more merit with numerical data. This outlines categorical data as a further active research field for ameliorating Differential Privacy Applications. Examples could include categorical data such as names, locations and gender. These data types are often some of the most sensitive information that an institution can hold on an individual. So, exploring the future potential of deep learning to assist with research in this area is warranted.

*Government Agencies*

Drechsler (2023) pro-actively discusses the difficulties in the adoption of differential privacy by government agencies. The article initially outlines the benefits of differential privacy and why the concept is attractive in a public service sense. Offering strong mathematically provable privacy guarantees, being able to offer similar results whether a data record is included or omitted, and a guarantee of privacy irrespective of any other assumptions are some of the reasons. However, adoption by the U.S. Census Bureau is the only current prominent government example due to a variety of difficulties.

For one, the massive amounts of data collected by the government is performed in a very different manner compared to the private industry. Data in many private industry examples is collected every single day and easier to analyse and manipulate given it is owned by one entity. As a result, uncertainty is therefore easier to design and implement on private industry datasets. The privacy budget is also more quantifiable: “*Assuming that the data collected today is independent from the data analysed yesterday one can start with a new privacy budget regularly as the old data would not leak any information about the current data (*Drechsler 2023)*.*”

In contrast, most of the information contained from government agencies is still based on surveys. This makes the release of accurate and privacy protected results more challenging. Government agencies also often act as intermediaries of information unlike private companies. This means that they are not able to as effectively control the information they are storing on file.

Further Drechsler (2023) summarises that selecting an appropriate privacy loss guarantee ( e ) value is more difficult for a number of reasons. He notes that it touches on liberal and moral arguments around the roll of government within society which are not as prevalent within the private sector hindering implementation. Drechsler (2023) discusses:

*In practice, however, measuring the costs and benefits of sharing private information both on the personal level and for society is much more nuanced (see the excellent discussions in Acquisti, Taylor, and Wagman (2016) from the economic perspective and Cohen (2013), which addresses the importance of privacy in the era of Big Data). Challenges such as limited awareness of the consequences of data sharing, information asymmetries, and limited market access “raise questions regarding individuals’ abilities, as rational consumers, to optimally navigate privacy trade-offs,” which ultimately raises concerns about whether there are “privacy ‘equilibria’ that benefit both data holders and data subjects” (Acquisti, Taylor, and Wagman 2016). Moving beyond the personal level, Cohen (2013) argues that “freedom from surveillance, whether public or private is foundational to the practice of informed and reflective citizen-ship” and thus privacy “is an indispensable structural feature of liberal democratic political systems.”*

# Applying Differential Privacy

Fartale (2023) compares and discusses several different Differential Privacy Software libraries. In particular Fartale points out Tensor Flow DP, Google’s Differential Privacy Libraries, IBM Differential Privacy and Open DP as prominent software libraries that are open source, widely applicable and easily accessible.

Some prominent Differential Privacy Libraries are below:

* IBM Differential Privacy Library. A general purpose, fit for all library to apply Differential Privacy on customer datasets. [IBM/differential-privacy-library: Diffprivlib: The IBM Differential Privacy Library (github.com)](https://github.com/IBM/differential-privacy-library)
* Google Differential Privacy Library - <https://github.com/google/differential-privacy>
* Apply Differential Privacy Library - <https://github.com/Samuel-Maddock/Apple-Differential-Privacy>

# Benefits of Differential Privacy for Implementation

There are a number of discernable benefits to Differential Privacy, making it attractive for implementation. Drechsler (2023) notes that some of the main benefits for Differential Privacy include:

* Offering strong mathematical privacy guarantees for risk. There is strong and relatively easier to understand mathematical guarantees for the technology. These guarantees can also easily quantify the risk for stakeholders. Knowledge of the tradeoffs between accuracy and privacy are therefore available. underlined.
* The underlying concept is intuitive and easy to understand for stakeholders. You can explain it simply though stating that you are injecting noise into the customer data set. This can be less technical to explain to stakeholders interested in implementation compared to other technologies which can be more technical to implement and understand.
* It is finally relatively transparent compared to other methods. There is a clear epsilon value which regulates the amount of information loss and the trade off between information loss and accuracy. It is also

# References for Scott West

*‘Data sharing in financial services: Five techniques to enhance privacy and confidentiality’*, accessed 19th of November 2023, Deloitte Touche Tohmatsu Limited, Deloitte 2019,

Yanjun Ma, Rui Lu, Yu Zhang, Year: 2023, *‘Research on the Application of Deep Learning-based Differential Privacy Protection Models in Financial Big Data’*, FFIT, DOI: 10.4108/eai.7-7-2023.2338057

Maniar, Tabish & Akkinepally, Alekhya & Sharma, Anantha. (2021). Differential Privacy for Credit Risk Model., Research Gate 2023, retrieved 22nd of November 2023, <https://www.researchgate.net/publication/353060744_Differential_Privacy_for_Credit_Risk_Model/citation/download>

Xiaopeng Luo, Siyuan Wang, Haolong Chen, Zongwei Luo. (2023). The Utility Impact of Differential Privacy on Credit Card Data in Machine Learning Algorithms. Procedia Computer Science, Volume 221, 2023, Pages 664-672, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2023.08.036>. Retrieved 22nd of November 2023, (<https://www.sciencedirect.com/science/article/pii/S1877050923007949>)

G. Sathish Kumar, K. Premalatha, G. Uma Maheshwari, P. Rajesh Kanna, G. Vijaya, M. Nivaashini, *Differential privacy scheme using Laplace mechanism and statistical method computation in deep neural network for privacy preservation*, Engineering Applications of Artificial Intelligence, Volume 128, 2024, 107399, ISSN 0952-1976, retrieved 23rd of November 2023, (https://www.sciencedirect.com/science/article/pii/S095219762301583X)

Jörg Drechsler (2023) ‘*Differential Privacy for Government Agencies—Are We There Yet?’*, Journal of the American Statistical Association, 118:541, 761-773, DOI: 10.1080/01621459.2022.2161385

*Equifax Data Breach Settlement (December 2022)*. FTC Refund Programs. Federal Trade Commission 2023. Accessed 5th of December 2023. [Equifax Data Breach Settlement | Federal Trade Commission (ftc.gov)](https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement)

Fartale H. (Posted on January 17th, 2023 under Differential Privacy). A Survey Of Differential Privacy Frameworks. OpenMined Blog 2023. Accessed 5th of December 2023. <https://blog.openmined.org/a-survey-of-differential-privacy-frameworks/>