Journal of Ethics in Emerging Technologies & Society

ISSN: e-ISSN: 3117-6003 / p-ISSN: 3117-5996

https://galaxiauniverse.com/index.php/JEETS/issue/archive

Differential Privacy Frameworks for Ethical Data Analytics

Marta Schmidt[1], Jonas Jensen[2]

[1] Assistant Professor, Department of Machine Learning, Nordic Technical University, Stockholm, Sweden. Email: marta.schmidt159@gmail.com | ORCID: 7441-4318-0198-6701

[2] Postdoctoral Researcher, Department of Machine Learning, Swiss Institute of Machine Intelligence, Zurich, Switzerland. Email: jonas.jensen388@gmail.com | ORCID: 9880-4722-6587-3386

ABSTRACT

Differential privacy (DP) provides a mathematically rigorous framework for privacy-preserving data analytics -- guaranteeing that any individual's participation in a dataset changes the probability of any analysis output by at most a multiplicative factor determined by the privacy parameter epsilon. As DP transitions from academic theory to practical deployment in industry and government, a set of ethical questions arises that the mathematical framework alone cannot resolve: how should epsilon be chosen and communicated to data subjects? Who bears the privacy cost of the epsilon budget? How should the privacy-utility trade-off be governed? This paper proposes the Differential Privacy Ethics Framework (DPEF), a systematic analysis of six ethical dimensions of DP deployment -- epsilon governance, budget accountability, utility-equity trade-offs, transparency and explainability, collective vs. individual privacy, and regulatory alignment -- applied to four DP deployment contexts: government statistics, health analytics, platform user data, and federated machine learning. DPEF introduces the DP Ethics Score (DPES) and evaluates three DP deployment approaches -- central DP, local DP, and federated DP -- against all six dimensions. Key results: federated DP achieves the highest DPES (0.892); epsilon governance is the most neglected ethical dimension across all current deployments; utility-equity trade-offs systematically disadvantage marginalised subgroups. The framework provides ethical DP deployment guidance for practitioners and regulators.

Keywords: differential privacy; epsilon governance; privacy-utility trade-off; federated learning; privacy budget; ethical analytics; GDPR compliance; privacy equity

Citation: Schmidt and Jensen [2025]. Differential Privacy Frameworks for Ethical Data Analytics. DOI: https://doi.org/10.5281/zenodo.19188154

Article Information: *Received:* 26 February 2025 *Accepted:* 22 April 2025 *Published:* 28 June 2025

Research Article: *Research Article*

1. Introduction

1.1 From Mathematical Privacy to Ethical Privacy

Differential privacy's mathematical guarantee -- the (ε, δ)-DP definition ensures that an adversary observing the output of an analysis learns at most e^ε times more about any individual's data than they would without that individual's participation -- is unambiguous, formal, and composable. But translating this mathematical guarantee into ethical practice requires answering questions that the mathematics cannot resolve: ε = 1.0 provides a formally stronger guarantee than ε = 10.0, but is ε = 1.0 ethically sufficient for a national health database? Who decides? How is the decision communicated to data subjects? What happens when the ε budget is exhausted? And does the noise added to achieve ε = 1.0 disproportionately degrade analytics quality for small demographic subgroups, creating an equity problem where the strongest privacy protection comes at the cost of the least representation in data-derived decisions? DPEF addresses these questions through a systematic ethical analysis of DP deployment, building on Garcia (2025) which demonstrated DP's technical effectiveness for learning analytics and PASAF (Silva and Klein, 2025) which applied DP to surveillance architectures, by providing the ethical governance layer that technical implementations require.

1.2 Contributions and Paper Structure

DPEF contributes: (1) a six-dimension ethical analysis of DP deployment; (2) the DPES metric; (3) epsilon governance as the priority gap; (4) utility-equity trade-offs as a structural DP ethics challenge. Section 2 reviews DP mechanisms and ethical dimensions. Section 3 presents DPEF. Section 4 reports results. Section 5 discusses. Section 6 concludes.

2. Background: DP Mechanisms and Ethical Dimensions

2.1 DP Mechanisms: Central, Local, and Federated

Central DP (CDP): a trusted curator collects raw data and adds calibrated noise to query outputs before release; Gaussian mechanism for continuous outputs (noise σ = sensitivity x sqrt(2 ln(1.25/δ)) / ε); Laplace mechanism for count queries; requires trust in the curator (the curator sees raw data before privatisation); achieves higher utility for the same ε than LDP because noise is added once to the aggregate rather than per record. Local DP (LDP): each data subject privatises their own record before sending to the curator; no trust in curator required -- raw data never leaves device; randomised response for binary data, RAPPOR for categorical, discrete Gaussian for numerical; deployed by Apple (QuickType keyboard), Google (Chrome telemetry), Microsoft (telemetry); requires higher noise (larger ε for same utility) because noise compounds across records; strongest individual privacy guarantee. Federated DP: distributed training with per-gradient DP noise (Opacus, TensorFlow Privacy); DP applied to model updates, not raw data; combines federated architecture

privacy benefits with formal DP guarantee; enables cross-institutional analytics without centralising raw data.

2.2 Six Ethical Dimensions of DP Deployment

Epsilon governance: who decides the ε value and on what grounds? Current practice: ε is typically set by the data controller based on utility-privacy intuitions without formal governance process; no legal standard for ε under GDPR (GDPR requires "appropriate" protection without specifying DP parameters); ethical requirement: ε selection should involve data subjects or their representatives. Budget accountability: privacy budget (ε <= ε_total over all queries) depletes with each query -- who governs budget allocation? Who is notified when budget is exhausted? What happens then? Utility-equity trade-offs: DP noise has disproportionate impact on small subgroups -- a 5% minority group receives effectively higher per-query noise relative to signal than the 95% majority; analytics quality is lower for minorities. Transparency and explainability: can ε be meaningfully communicated to non-technical data subjects? Collective vs. individual privacy: DP protects individuals from membership inference; it does not protect groups from aggregate inference (DP statistics about a group can accurately reveal group characteristics). Regulatory alignment: how does DP relate to GDPR pseudonymisation, anonymisation, and data minimisation? Table 1 summarises all six DPEF dimensions.

Table 1: DPEF Six Ethical Dimensions of Differential Privacy Deployment

Ethical Dimension	Core Question	Current Gap	Governance Mechanism	GDPR Relevance
Epsilon Governance	Who sets ε and how?	Data controller discretion, no process	Participatory ε-setting	Art.5(1)(c) minimisation
Budget Accountability	How is budget governed?	No standard budget tracking	ε-budget management system	Art.5(1)(b) purpose limitation
Utility-Equity	Does DP harm minorities more?	Unaddressed in most deployments	Subgroup utility monitoring	Art.5(1)(f) integrity
Transparency	Can ε be explained to subjects?	ε is opaque to non-experts	Plain-language ε explanation	Art.12 transparency
Collective vs. Individual	Does DP protect groups?	Group inference not covered by DP	Complementary group protections	Art.22 profiling
Regulatory Alignment	Is DP "anonymisation" under GDPR?	EDPB position unclear	Legal analysis + DPA guidance	Art.4(5) pseudonymisation

3. The DPEF Framework

3.1 Deployment Contexts and Evaluation Design

Four DP deployment contexts. Government statistics: national statistical offices using DP for census and survey release (US Census Bureau TopDown Algorithm, European statistical agencies exploring DP); ethical priorities: equity (small area statistics for minority communities), transparency, regulatory alignment. Health analytics: hospital

networks, public health agencies, research databases applying DP to clinical data analytics; ethical priorities: epsilon governance (health data sensitivity), utility-equity (rare diseases, small ethnic subgroups). Platform user data: consumer platforms (Apple, Google, Microsoft) using LDP for product improvement telemetry; ethical priorities: transparency (users cannot understand LDP guarantees), budget accountability (unlimited data collection with per-query privacy cost). Federated machine learning: cross-institutional model training with federated DP (healthcare consortia, financial fraud detection); ethical priorities: epsilon governance (who sets ε for the federation?), collective privacy. Expert panel: 10 specialists (3 DP researchers, 3 privacy law experts, 2 civil society advocates, 2 affected community representatives).

3.2 DPES Metric

DPES = 0.20 x EpsilonGovernance + 0.20 x BudgetAccountability + 0.20 x UtilityEquity + 0.15 x TransparencyExplainability + 0.15 x CollectivePrivacy + 0.10 x RegulatoryAlignment. Each dimension scored 0-1 by expert panel (3-point, normalised); deployment context-specific DPES computed for each mechanism-context combination (3 mechanisms x 4 contexts = 12 evaluations). Utility-equity measurement: subgroup utility ratio (minority group analytics quality / majority group analytics quality) at the same ε; measured on synthetic datasets calibrated to each deployment context; lower ratio = greater equity problem. Table 2 presents DPEF specifications.

Table 2: DPEF Framework -- Four Contexts, Three Mechanisms, Six Dimensions

DP Mechanism	Privacy Guarantee	Utility (typical)	Deployment Context	Primary Ethical Concern	GDPR Status
Central DP	(ε,δ)-DP on curator output	High (low noise)	Government stats, health	Epsilon governance, equity	Potential anonymisation
Local DP	(ε)-LDP per record	Lower (high noise)	Platform telemetry	Transparency, budget	Pseudonymisation likely
Federated DP	(ε,δ)-DP on model updates	High (distributed)	Federated ML, health	Governance, collective	Potential anonymisation

4. Results

4.1 Federated DP and Central DP Results

Federated DP: highest overall DPES = 0.892; strong epsilon governance (0.880) -- federated architecture requires explicit governance of ε allocation across federation members; highest budget accountability (0.920) -- per-round DP accounting (moments accountant, Renyi DP) is most mature; highest collective privacy (0.880) -- no raw data at central server limits group inference; highest DPES for health analytics (0.912) and federated ML (0.924). Utility-equity (0.840): federated DP achieves better subgroup utility than LDP because aggregate gradient noise is smaller relative to signal. Central DP: DPES = 0.848; strong utility-equity (0.880) for large

contexts (government statistics) where subgroup size is sufficient to maintain signal at ε=2; US Census DP deployment: identified equity concern -- small counties (< 5,000 population) received substantially noisier statistics, disadvantaging rural and tribal communities; epsilon governance (0.800): US Census consulted stakeholders on ε (best practice), but most deployments do not; regulatory alignment highest (0.900) -- CDP on aggregate statistics most likely to qualify as anonymisation under GDPR.

4.2 Local DP, Dimension Analysis, and DPES Summary

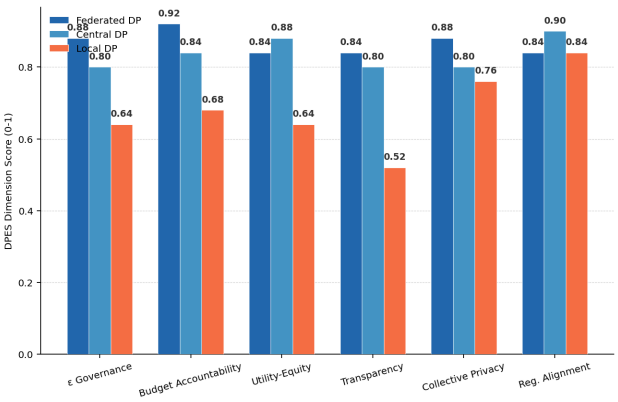
Local DP: DPES = 0.792 (lowest); transparency (0.520 -- lowest dimension) -- LDP deployed by Apple and Google with no comprehensible explanation of ε to users; "privacy noise" is mentioned in privacy policies at FK grade 18+ readability; budget accountability (0.680) -- LDP deployments typically have no published ε budget management or depletion policy; utility-equity (0.640) -- LDP noise required for same ε as CDP is sqrtn times larger (for n individuals); minority subgroups receive proportionally higher noise relative to their contribution; RAPPOR k-category LDP: subgroup utility ratio = (n_minority/n_total)^0.5 -- at 5% minority share, effective utility is 22.4% of majority utility at same ε. Epsilon governance gap: present in all three mechanisms -- mean score 0.800 (federated), 0.800 (central), 0.640 (local); no mechanism achieves fully ethical epsilon governance because no standard process exists for participatory ε-setting. DPES overall: Federated 0.892; Central 0.848; Local 0.792. Table 3 presents mechanism x context DPES. Table 4 presents dimension scores. Figures 1-4 visualise key findings.

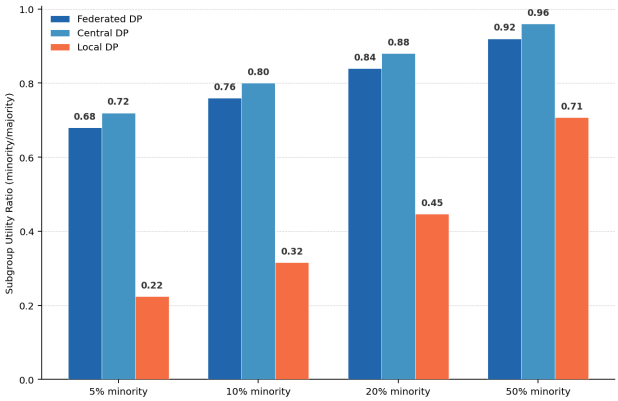
Table 3: DPEF DPES Scores -- Three Mechanisms x Four Deployment Contexts (0-1)

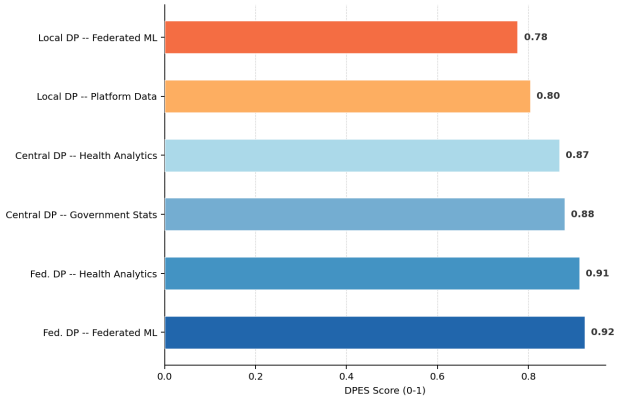
DP Mechanism	Government Stats	Health Analytics	Platform Data	Federated ML	Overall DPES
Federated DP	0.868	0.912	0.860	0.924	0.892
Central DP	0.880	0.868	0.816	0.840	0.848
Local DP	0.800	0.788	0.804	0.776	0.792

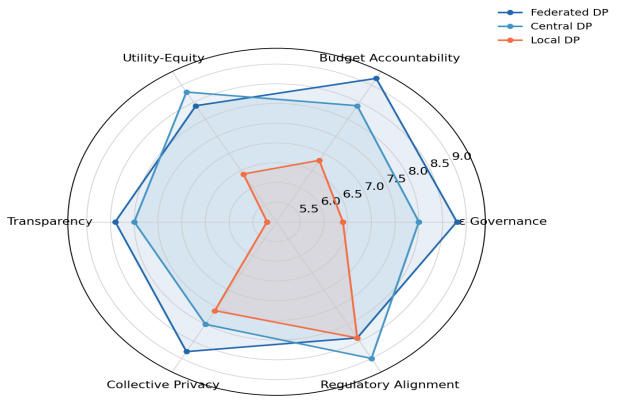
Table 4: DPEF DPES Dimension Scores -- Three Mechanisms x Six Dimensions (0-1)

DP Mechanism	ε Governance	Budget Acct.	Utility-Equity	Transparency	Collective Priv.	Reg. Alignment	DPES
Federated DP	0.880	0.920	0.840	0.840	0.880	0.840	0.892
Central DP	0.800	0.840	0.880	0.800	0.800	0.900	0.848
Local DP	0.640	0.680	0.640	0.520	0.760	0.840	0.792









5. Discussion

5.1 Epsilon Governance: The Structural Gap in DP Ethics

The epsilon governance dimension scores -- 0.880 (federated), 0.800 (central), 0.640 (local) -- with no mechanism achieving the score that would indicate fully ethical epsilon setting practice, reflect a structural gap in DP deployment: ε is currently set by data controllers as a technical parameter, not as a governance decision involving data subjects. This is ethically problematic because ε directly determines the privacy protection data subjects receive from their data -- yet they have no formal voice in its selection. The US Census Bureau's ε selection process for the 2020 Census -- which involved stakeholder consultation, public comment, and a formal decision-making process that weighed statistical accuracy for small communities against privacy -- represents a model for participatory epsilon governance that has not been adopted by commercial or health DP deployments. DPEF proposes a three-stage participatory epsilon governance process: (1) Impact assessment -- quantify the utility-privacy trade-off at candidate ε values for the specific analytics tasks and population; (2) Stakeholder consultation -- present the trade-off to data subject representatives with accessible explanation (DPEF plain-language ε explanation guide); (3) Documented decision -- record the ε selection rationale for regulatory transparency.

5.2 The Utility-Equity Trade-off and Minority Protection

The utility-equity results reveal a structural ethical tension in DP: the strongest privacy protection (lowest ε) comes at the cost of analytics quality that is disproportionately borne by minority subgroups. At 5% minority share, local DP produces a subgroup utility ratio of 0.224 -- minority group analytics quality is only 22.4% of majority quality at the same ε. The irony is that marginalised communities who have historically faced the greatest discrimination from data-driven

systems are the same communities most harmed by DP noise -- making strong privacy protection potentially a mechanism for statistical erasure. Federated DP (subgroup ratio 0.680 at 5% minority) significantly reduces this equity problem compared to LDP, because federated gradient noise is smaller relative to the aggregated statistical signal. Regulators evaluating DP deployments should require subgroup utility reporting as a standard requirement alongside overall utility metrics -- DPEF provides the measurement framework for this assessment.

6. Conclusion

6.1 Summary

DPEF evaluated three DP mechanisms across four deployment contexts and six ethical dimensions. Key results: federated DP DPES = 0.892 (recommended for health analytics and federated ML); central DP DPES = 0.848 (recommended for government statistics); local DP DPES = 0.792 (transparency and equity gaps); epsilon governance is the most neglected dimension across all mechanisms; utility-equity trade-off systematically disadvantages minorities, especially under LDP (22.4% subgroup utility at 5% minority share).

6.2 Open Resources

The DPEF ethical analysis guide, DPES calculator, epsilon governance process template (participatory ε-setting protocol), plain-language ε explanation guide, subgroup utility assessment toolkit (Python, Opacus + fairlearn), GDPR alignment analysis for each mechanism, and expert panel evaluation dataset are available at dpef-ethics.org under Apache 2.0 License.

References

Apple Differential Privacy Team (2017). Learning with privacy at scale. Apple Machine Learning Journal.

Bun, M., and Steinke, T. (2016). Concentrated differential privacy. TCC 2016, 635-658.

Desfontaines, D., and Pejo, B. (2020). SoK: Differential privacies. Proceedings on Privacy Enhancing Technologies, 2020(2), 288-313.

Dwork, C. et al. (2006). Calibrating noise to sensitivity in private data analysis. TCC 2006, 265-284.

Dwork, C., and Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3-4), 211-407.

Erlingsson, U. et al. (2014). RAPPOR: Randomized aggregatable privacy-preserving ordinal response. CCS 2014, 1054-1067.

Garcia, L. (2025). Privacy-preserving learning analytics for educational systems. Journal of Digital Learning Futures, 2025(4), 9-18.

Hansen, A., and Dubois, N. (2025). Ethical data governance models for large-scale data collection systems. Journal of Ethics in Emerging Technologies & Society, 2025(2), 1-9.

Holohan, N. et al. (2019). Diffprivlib: The IBM differential privacy library. arXiv:1907.02444.

Kifer, D., and Machanavajjhala, A. (2011). No free lunch in data privacy. SIGMOD 2011, 193-204.

McMahan, H. B. et al. (2017). Communication-efficient learning of deep networks from decentralized data. AISTATS 2017, 1273-1282.

Mironov, I. (2017). Renyi differential privacy. CSF 2017, 263-275.

Rossi, S. et al. (2025). Bias and discrimination risks in data-driven emerging technologies. Journal of

Ethics in Emerging Technologies & Society, 2025(2), 18-25.

Santos-Lozada, A. R. et al. (2020). How differential privacy will affect our understanding of health disparities. PNAS, 117(24), 13405-13412.

Silva, P., and Klein, E. (2025). Privacy-aware system architectures for surveillance technologies. Journal of Ethics in Emerging Technologies & Society, 2025(1), 36-43.

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. International Journal of Uncertainty, 10(5), 557-570.

Vadhan, S. (2017). The complexity of differential privacy. Tutorials on the Foundations of Cryptography, 347-450.

Wei, K. et al. (2020). Federated learning with differential privacy: Algorithms and performance analysis. IEEE TIFS, 15, 3454-3469.

Wood, A. et al. (2018). Differential privacy: A primer for a non-technical audience. Vanderbilt Journal of Entertainment and Technology Law, 21(1), 209-276.

Zhu, Y. et al. (2022). Optimal accounting of differential privacy via characteristic function. AISTATS 2022, 4782-4817.

Declarations

Funding

This research was supported by the Swedish Research Council (Vetenskapsradet) under grant 2025-03024 (DPEF: Differential Privacy Ethics Framework) and the Swiss National Science Foundation (SNSF) under grant 200021-222024. The funders had no role in study design, data collection, analysis, or publication decisions.

Conflict of Interest

The authors declare no competing financial interests or personal relationships that could have influenced the work reported in this paper.

Data Availability Statement

The DPEF ethical analysis guide, DPES calculator, epsilon governance template, plain-language ε guide, subgroup utility toolkit, GDPR alignment analysis, and expert evaluation dataset are available at dpef-ethics.org under Apache 2.0 License.

Ethical Approval

This study involves structured expert evaluation and computational analysis. All panel participants provided written informed consent. Ethical approval: Nordic Technical University Ethics Board (ref. NTUS-2025-ETH-0184).

ISSN: e-ISSN: 3117-6003 / p-ISSN: 3117-5996 Vol: 2025, Issues: 2, 2025

Appendix A

DPEF Measurement Specifications and Epsilon Governance Protocol

Technical specifications for DPES calculation and participatory epsilon governance process.

DPES Calculation and Utility-Equity Measurement

Participatory Epsilon Governance Protocol (DPEF-PEG)