Natural differential privacy—a perspective on protection guarantees

Micah Altman[1,*] and Aloni Cohen[2,*]

[1] CREOS, MIT Libraries, Massachusetts Institute of Technology, Cambridge, MA, United States
[2] Computer Science, University of Chicago, Chicago, IL, USA
[*] These authors contributed equally to this work.

Submitted 24 May 2023
Accepted 15 August 2023
Published 28 September 2023

Corresponding author
Micah Altman,
micah_altman@alumni.brown.edu

Academic editor
Sedat Akleylek

Additional Information and Declarations can be found on page 9

DOI 10.7717/peerj-cs.1576

ABSTRACT

We introduce “Natural” differential privacy (NDP)—which utilizes features of existing hardware architecture to implement differentially private computations. We show that NDP both guarantees strong bounds on privacy loss and constitutes a practical exception to no-free-lunch theorems on privacy. We describe how NDP can be efficiently implemented and how it aligns with recognized privacy principles and frameworks. We discuss the importance of formal protection guarantees and the relationship between formal and substantive protections.

Subjects Cryptography, Security and Privacy
Keywords Differential privacy, Physical mechanisms, No free lunch, Privacy by design, Privacy by default

INTRODUCTION

Differential privacy offers provable privacy guarantees (*Wood et al., 2018*) but has been criticized as difficult to integrate into existing data production systems and requiring substantial utility loss (*Blanco-Justicia et al., 2022*).

We introduce natural differential privacy (NDP)—a framework for guaranteeing differential privacy for arbitrary computations by leveraging features of existing hardware architectures and natural sources of entropy.

NDP provides all the advantages of “pure” differential privacy as originally formulated in *Dwork et al. (2006)*, not resorting to any of the myriad relaxed definitions that provide weaker guarantees (*Pejó & Desfontaines, 2022*). NDP provides a worst-case bound on privacy loss that is substantially better than some high-profile, large-scale commercial implementations of DP.

Moreover, in contrast to existing implementations, NDP provides privacy by default for all computations on a platform. Furthermore, NDP is simple and inexpensive to implement at a large scale and requires no practical reduction in utility or performance.

ORGANIZATION

The article proceeds as follows: Section 3 provides a definition of NDP, explains the concept, and provides theoretical foundations, including provable privacy guarantees. Section 4 discusses related work and explains how NDP differs from other approaches. Section 5 discusses the advantages of NDP in comparison to other approaches and how NDP aligns with existing privacy principles and frameworks. Section 6 discusses implementation approaches—including sufficient hardware and software features for implementation—and analyzes the privacy parameter obtained (and thus protection guaranteed) in exemplar implementations. Section 7 summarizes experimental results. Section 8 characterizes limitations and directions for future research—including the relation to other security properties. Section 9 provides a more general discussion—informed by NDP—of the substantive importance of formal privacy guarantees and guidance for the interpretation of protection claims.

CONCEPT: PRELIMINARIES, DEFINITION, ABSTRACT IMPLEMENTATION

We consider the setting of a dataset x consisting of n records, where each record is a bitstring of dimension d. We view each row as containing the data of a single individual. Databases x and x′ are neighboring if they differ in at most one record. A mechanism M is a randomized mapping from datasets to some set of possible outputs Y.

Definition 2.1 (ε-Differential Privacy (ε-DP) (*Dwork et al., 2006*)). M is ε-*differentially private* if for all neighboring datasets x and x′, and for all sets $S \subseteq Y$:

$$\Pr[M(x) \in S] \leq e^{\varepsilon} \cdot \Pr[M(x') \in S] \tag{1}$$

where the probabilities are taken over M's coins.

NDP is defined as any system that integrates DP protections directly in a Von Neumann architecture (*von Neumann, 1945*) *via* hardware implementation using persistent sources of entropy for noise infusion. By construction, every internal computation by an NDP system integrates noise infusion guaranteeing (ε, 0)-DP. And because DP preserves privacy under postprocessing—all outputs from the system are thus (ε, 0)-DP.

Implementation: NDP applies to the computation of arbitrary m-bit functions f of the data x, for any m. To evaluate the NDP-version of f, one simply evaluates f on a RAM machine. For best results, the RAM should be operated at or above sea level.

We use as a building block the Randomized Response mechanism. The Randomized Response mechanism is parameterized by a probability $0 < p < 0.5$, and we denote the corresponding mechanism RR_p. RR_p takes as input a bit $b \in \{0,1\}$, and outputs 1-b with probability p, otherwise outputting b. Results established in *Willis (2014)* provide a formula for the exact equivalence between the probability of randomized response and the epsilon parameter. For any $p < 0.5$, Eq. (2) expresses this relationship:

$$1 - p = \exp(\varepsilon)/(1 + \exp(\varepsilon)) \tag{2}$$

Privacy parameters: Let $T_{in} > 0$ and $T_{out} > 0$ be the length of time that the input x and output f(x) are stored in RAM over the course of the computation, respectively.[1]

Each computation has a corresponding parameter q that depends on the environment within which the computation is performed. Thus q is the probability of any single bit flip caused by cosmic rays occurring on 1 GB of RAM over the course of 1 day (see Table 1). From q, it is easy to derive the probability p that any single bit is flipped in the period T_{in} or

[1] If the portions of the input (respectively, output) are in RAM for different lengths of time, then we take T_{in} (resp., T_{out} to be the minimum time over every bit of the input (resp., output).

T_{out}. Using p and applying Eq. (1), it is straightforward to solve for a value of ε (at the bit event level).[2]

RELATED WORK

Other variants of DP, such as epsilon-delta DP and concentrated DP, have been proposed (*Dwork & Rothblum, 2016*).[3] However, these variants relax the definition of DP yielding weaker privacy properties (We refer hereafter to such relaxations as 'artificial').

Current implementations of DP at scale have used artificial DP. Because of the substantial utility tradeoffs that artificial DP often requires—commercial implementations often use values of epsilon well above 1. Recent large-scale implementations of differential privacy by major corporations (including Google and Apple) have employed effective epsilon levels ranging from dozens to hundreds—with one major implementation exceeding seven hundred and fifty[4] (*Rogers et al., 2020*).

Natural sources of entropy for noise diffusion have been studied for over four decades (*Ziegler & Lanford, 1979*). Their importance in security and privacy has been recognized in related areas:

- Bit flipping induced by radiation or other environmental conditions has been previously used for practical attacks against system security (*Dinaburg, 2011*; *Govindavajhala & Appel, 2003*).
- The importance of high-quality random number generation for all differential privacy methods has recently been recognized (*Garfinkel & Leclerc, 2020*). Nearly all implementations rely on pseudo-random sequences seeded from a physical entropy source. The use of physical sources of randomness for direct noise infusion has not been well-examined.
- More recently, the inherent instability of quantum computation has been examined as a theoretical source of protective noise infusion—although practical implementation remains far off (*Zhou & Ying, 2017*).

ADVANTAGES OF NDP

Although natural noise infusion has been studied in related work, the use of natural sources directly for differential privacy is novel. The NDP approach offers a number of advantages:

- NDP protects all computations made on a system.
- NDP does not require any relaxation of the formal differential privacy guarantees—unlike artificial DP variants.
- NDP is simple to implement and inexpensive to deploy.
- NDP provides protections that are substantively equivalent (or better) than the formal guarantees provided by notable commercial implementations—while maintaining higher utility, substantially reducing implementation cost, and extending protection to a broader range of computations.

[2] Many consider the event-level as the most practical unit of protection for streaming systems (*Lécuyer et al., 2019*)—and has been used at scale for public release of large scale Facebook data for scientific research (*King & Persily, 2019*, *2020*) In addition, the value of ε for multi-bit events is arithmetically derivable—see Footnote 8. Note that as with any other random-response based approach, redundant, or compressed encoding of measurements prior to protection may result in under- or over-protection. Specifically, input data should be represented as bit-fields, integers or character strings in which each bit of the data corresponds to a bit of information being protected. For example, integers, characters, or bit-fields as implemented in C++ (*ISO, 2020*) would be suitable. The induced value of ε for inputs stored in floating point representations (*IEEE Computer Society, 2019*) remains a topic of research. However, computations on the input data are unrestricted—thus protected functions may use IEEE standard floating point computations as long the initial input data are represented as integers (*etc.*).

[3] Differential privacy is the most developed and popular of a larger set of possible formal privacy measures—for a survey of current measures see *Wagner & Eckhoff (2018)*. Further the core protection provided by formal privacy measures is to limit (in a statistically well-defined way) what an adversary can infer from protected outputs. In practice, formal approaches may be complemented by a range of other privacy-enhancing technologies (*e.g.*, that provide limits on computation rather than inference)—as well as complementary security control mechanisms. The scope of complementary technologies is vast and expanding—so a discussion is beyond the scope of this article. For reviews of potential complementary privacy technologies see OECD (2023), Altman et al. (2018).

[4] Estimates are for the effective protection of user information over a month of activity. Because of composition effects, the effective epsilon for protection of a user information in these systems grows geometrically over time. Thus a cumulative epsilons of ten thousands or more is possible for frequent, long-term users of these systems.

Table 1 Privacy budget configuration through altitudinal adjustment. Derivative-free numerical minimization (*Brent, 1973*) is used to obtain epsilon corresponding to p, given Eq. (2). Bit-level frequency data is provided by *Soft Error (2022)*, *Enyinna (2016)*. Epsilon levels are calculated for protection at the (bit) event-level, To calculate epsilon for other units of protection, it is straightforward to calculate the effective epsilon by using the standard dp composition formula across the maximum number of shared events in the computation (*Kairouz, Oh & Viswanath, 2015*). Even under composition, the effective epsilon remains trivially small relative to the baseline: Where B is the number of independent bits measured per unique event, the protection produced by this method is, in the worst case, εB.

m > sea-level	Exemplar location	µSv/h	Error/GBxDay	Max ε
−3,840	Mponeng gold mine	0	0	∞
10	Cambridge, MA	0.06	0.2	33.70711
1,742	Mount Wilson observatory	0.237	2	31.39832
10,000	Jet airplane's lower cruising altitude	6	60	27.99537
781,000	Iridium satellite constellation	60	600	25.69307

Further, DP has additional attractive features:

1) First, NDP encourages privacy by design (*Cavoukian, 2009*)—NDP can be integrated into hardware architecture, systems design, and facility deployment, as well as at the application level.
2) Second, NDP provides privacy by default (*Willis, 2014*) since a floor for protection is provided for all users without requiring any opt-ins (*NISO, 2015*).
3) Third, NDP aligns well with the widely adopted 'five safes framework' (*Desai, Ritchie & Welpton, 2016*). Specifically, it uses architectural privacy by design to guarantee 'safe outputs'.
4) Fourth, NDP can be implemented either at the time of manufacture or during deployment. This facilitates certification and auditing of secure hardware and facilities.
5) Fifth, NDP provides guaranteed, measurable privacy with zero marginal utility loss—theoretical no-free-lunch theorems notwithstanding (*Kifer & Machanavajjhala, 2011*).[5]

SETTING PRIVACY PARAMETERS WITHIN NDP SYSTEMS—HARDWARE AND SOFTWARE IMPLEMENTATION

NDP, when fully integrated into the architecture, operates by default, continuously, and at the hardware level. In modern architectures, which implement random access memory using MOSFET technology, bit-flipping is an ideal mechanism for noise infusion.

At manufacturing time, the infusion of readily available alpha sources into memory chip packaging material requires no increase in manufacturing cost. This approach can be used to ensure a maximum bound for epsilon that is both auditable through inspection and can be verified through hardware certification processes.[6]

More generally, ionizing radiation provides a natural and ubiquitous source for inducing randomized responses at the bit level—acting through the injection of memory faults. Utilizing this physical mechanism for entropy provides true randomness, which

[5] In theory, theory and practice are the same—in practice, they differ. See *Brewster (1882)*, *Quote Investigator (2018)* for the original formulation by Brewster, and contributions attributed to Berra and Einstein.

[6] Even without changes in manufacturing processes, manufacturers can readily certify that their RAM is not unsafe by design—in that it does not provide ECC or this feature has been disabled (*e.g.*, at the firmware level).

provides stronger formal guarantees than pseudorandom number generation (*Vadhan, 2012*; *Garfinkel & Leclerc, 2020*).

Results established in *Wang, Wu & Hu (2016)* provide a formula for the exact equivalence between the probability of randomized response and the epsilon parameter.

$$p = 1/(1 + \exp(\varepsilon)) \tag{3}$$

Many sources of radiation are readily available, as shown in Fig. 1.[7]

Post-manufacture, maximum bounds on epsilon can be further reduced at deployment time through the positioning of the hardware. Entire computing facilities may be certified as safe using this method.

Conveniently, cosmic rays cause i.i.d. bit flips at a rate directly related to the level of cosmic radiation (typically measured in micro-sieverts) exposure, which is itself a function of atmospheric density (above sea level) and crustal density (below sea level) at a given altitude. The levels of radiation experienced at specified altitude relative to sea level has been established empirically and fits a geometric distribution within near-earth orbiting distances. Using these empirical results and Eq. (3), we can derive the effective value of epsilon at exemplar locations, as shown in Table 1.

Note that relative to baseline, very low values of epsilon can be achieved through altitudinal adjustment. Further, note that the level of epsilon provided naturally at sea level is more protective than the level provided by the most notable and largest scale production implementations of differential privacy to date (*Greenberg, 2017*). Finally, in practice, the effective epsilon will be statistically indistinguishable from implementations using a theoretically lower value.[8]

At runtime, noise injection can readily and effectively be achieved by altering the thermal operating environment (*Govindavajhala & Appel, 2003*). Further, in high-density computing deployments, simply reducing the level of external cooling will not only increase protective noise infusion but also reduce electricity usage—benefitting the global environment. Moreover, various external noise injection tools are available and can provide additional protection without affecting the location or manufacturing process (*Hsueh, Tsai & Iyer, 1997*). Finally, given the wide availability of (level-2) hypervisor-based system-level virtual machine technologies, simulation-based noise infusion (aka. synthetic natural differential privacy) can be used to produce any desired level of epsilon with a relatively small decrease in runtime performance (*Li et al., 2017*).

EXPERIMENTAL RESULTS

The primary contribution of the article is a formal analysis of NDP properties. And the derivation of protection levels for a specific implementation rely on the value of physical parameters (such as levels of background radiation and the corresponding bit-level error rates) that are already well-established in the literature (as detailed in the previous section).

For replication, we conducted a set of implementation experiments deployed in the exemplar locations in Table 1, Cambridge, MA. The experiment involved running 25 output audits of the form described above in footnote 9. The experiment was conducted on a 12th Gen Intel Core i5-1235U CPU, using LPDDR4 RAM, and running the Linux

[7] This chart illustrates approximate point estimates of source intensity, for use in general comparison of types and magnitude of sources. For specific details on each source see *Mettler et al. (2008)*, *Munro (2023)*.

[8] Assuming a continuous audit period of 1 h, and conventional levels of statistical significance ($p = 0.05$) is used, the observed value at sea level will not be statistically distinguishable from a theoretical epsilon of 31.91007 (Zero bits flipped will be observed during that period at either level of epsilon, during at least 95% of audits).

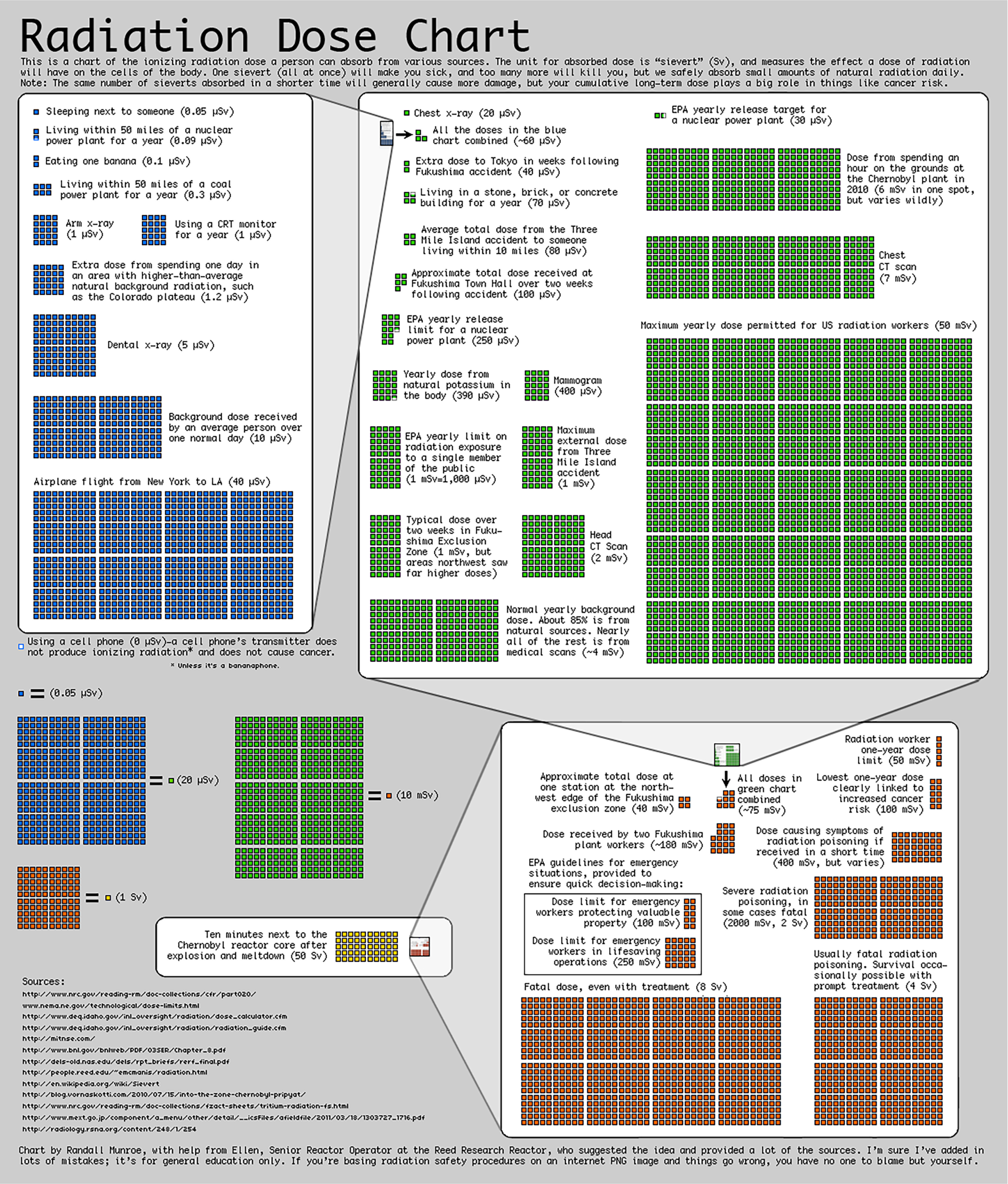

Figure 1 Comparison of readily available entropy sources for setting ε. (Source *Munro (2011)*, in the public domain).

Full-size DOI: 10.7717/peerj-cs.1576/fig-1 operating system (See Appendix for replication code). The expected protection level was observed in all 25 experiments, replicating previously established values at conventional levels of significance ($p = 0.05$).

LIMITATIONS AND FUTURE WORK

On occasion, serious points are best conveyed through humor.[9] This article is intended as a work of (serious) humor. While each of the individual technical assertions in the article is true, catastrophic drawbacks are omitted or glossed over. Thus the substantial benefits claimed for the method, particularly in "Advantages of NDP," are parodically misleading.

For example, some of the limitations of the above proposal include the following:

- Formal privacy-protecting methods aim to limit adversarial inferences based on outputs. Other potentially desirable security properties, such as integrity, non-repudiation, *etc*., are orthogonal to this goal. Thus it is often appropriate to use privacy-protecting methods in conjunction with other privacy-enhancing technology and security controls. See *OECD (2023)*, *Altman et al. (2015)* for selected reviews of complementary approaches.
- As is true generally for formal approaches to privacy, guarantees are provided under the assumption that the adversary does not observe timing characteristics of the computation, which would potentially allow for timing channel attacks (*Biswas, Ghosal & Nagaraja, 2017*).
- As is generally true for privacy-preserving methods, guarantees rely on the assumption that the computing platform itself is secure. For example, if adversaries can intercept input data prior to applying the protection method, observe all computations on the system, or alter the implementation of arbitrary code, including protecting algorithms, this may subvert privacy and other security properties. For these reasons, privacy-protecting methods are often deployed in a secure environment to produce outputs that may then be shared publicly—and complementary security controls are deployed with privacy-protecting methods. For a review of complementary security controls recommended in conjunction with privacy protective methods generally and with DP-related methods specifically, see *Altman et al. (2015)*, *Wood et al. (2020)*.
- Use of ε above 1, although frequent in practice, requires caution for any DP-based method.
- It is rarely the proper objective of law or public policy to protect the privacy of an 'event'. It is usually a more appropriate policy goal to protect the privacy of a persistent actor—such as a person, organization, or designated group of people.
- Information about an event or other unit of protection is rarely limited to a single bit. Where measurements of the unit of protection comprise multiple bits, composition will multiplicatively increase the effective ε. Further multi-bit events should be encoded efficiently—so that each bit of input data represents a unique measured bit of information (This limitation applies only to inputs. Other representations, such as floating-point, may be used for computations on those inputs. See footnote 2).

[9] See *Janko (1987)* for foundations of this principle, and *Van Stempvoot, Portinga & Johnson (2022)* for both a modern defense and exemplar of the principle.

- Randomized response does not generally result in an efficient tradeoff between privacy and utility—especially as the effective information measured grows large.
- Inducing a high level of bit flipping at random in main memory may cause unwanted side effects—such as entirely incorrect results, nonsense output, program failures, and system crashes.
- Thus, there is no market for highly unreliable RAM, despite the low cost of manufacture.
- Further, introducing ionizing radiation to the deployment site to achieve a meaningful level of protection may risk exposure to lethal amounts of radiation and create a durable hazard. This potentially violates local regulations, national laws, and international treaties.

DISCUSSION

One of the triumphs of modern computer science is the ability to establish formal provable protection guarantees. However, when using any real system, it is vital to understand the extent, strength, and conditions under which provable protections.

The limitations above notwithstanding, there is a sense in which cosmic rays formally induce ε-DP. Further, the epsilon values used by some large-scale commercial implementations of DP provide provable worst-case privacy-loss guarantees that are arguably no stronger than those provided by cosmic rays in Cambridge.

Increasingly, production systems claim the benefit of provable privacy protections—almost all of them based on some form of differential privacy. When, as often happens, very high values of epsilon are employed, the amount of protection that is provable, while technically measurable, is substantively negligible.

This article, while parodic, illustrates that provable formal privacy and truthful compliance with privacy principles neither guarantee substantive protection nor require substantial implementation effort. Provable guarantees, such as those provided by differential privacy, have force only when the specific level of protection provided by implementation privacy parameters in practice is meaningful, the guarantees apply to a well-defined and substantively meaningful set of interactions between protected units and protective systems, and when the formal unit of protection corresponds to real-world entities with meaningful privacy interests. Moreover, when a system embeds a weak implementation of a protection mechanism at its core, compliance with other privacy principles, such as privacy-by-design, may offer little value.

Protections may still be of substantial value even if they are not formally proven—these implementations may provide useful protection in particular contexts even if such protections are not formally provable.[10] However, such protections should be established on their own merits—using appropriate non-formal (and especially, empirical) evidence. Notwithstanding, when the strong guarantees provided by a system are substantively negligible, it is grossly misleading to claim the system provides provable protection.

[10] And it is always possible that as new methods of formal analysis are developed, we may come to understand that some systems are more protective than could initially be proved.

ACKNOWLEDGEMENTS

We thank Stephen Chong and Kobbi Nissim for their helpful comments on prior drafts. We describe the authors' contributions following a standard taxonomy (*Allen et al., 2014*).

ADDITIONAL INFORMATION AND DECLARATIONS

Funding

The authors received no funding for this work.

Competing Interests

The authors declare that they have no competing interests.

Author Contributions

- Micah Altman conceived and designed the experiments, contributed to the conception of the report (including core ideas and statement of research questions), to the methodology, and to the writing through critical review and commentary, performed the experiments, analyzed the data, performed the computation work, prepared figures and/or tables, authored or reviewed drafts of the article, and approved the final draft.
- Aloni Cohen conceived and designed the experiments, contributed to the conception of the report (including core ideas and statement of research questions), to the methodology, and to the writing through critical review and commentary, authored or reviewed drafts of the article, and approved the final draft.

Data Availability

The following information was supplied regarding data availability:

The replication code is available in the Supplemental File.

Supplemental Information

Supplemental information for this article can be found online at http://dx.doi.org/10.7717/peerj-cs.1576#supplemental-information.

REFERENCES

Allen L, Scott J, Brand A, Hlava M, Altman M. 2014. Publishing: credit where credit is due. *Nature* **508(7496)**:312–313 DOI 10.1038/508312a.

Altman M, Wood A, O'Brien DR, Gasser U. 2018. Practical approaches to big data privacy over time. *International Data Privacy Law* **8(1)**:29–51 DOI 10.1093/idpl/ipx027.

Altman M, Wood A, O'Brien DR, Vadhan S, Gasser U. 2015. Towards a modern approach to privacy-aware government data releases. *Berkeley Technology Law Journal* **30(3)**:1967–2072 DOI 10.15779/Z38FG17.

Biswas AK, Ghosal D, Nagaraja S. 2017. A survey of timing channels and countermeasures. *ACM Computing Surveys (CSUR)* **50(1)**:1–39 DOI 10.1145/3023872.

Blanco-Justicia A, Sanchez D, Domingo-Ferrer J, Muralidhar K. 2022. A critical review on the use (and misuse) of differential privacy in machine learning. *ArXiv preprint*. DOI 10.48550/arXiv.2206.04621.

Brent R. 1973. *Algorithms for minimization without derivatives*. Englewood Cliffs, NJ: Prentice-Hall.

Brewster B. 1882. Theory and practice. *The Yale Literary Magazine, Conducted by the Students of Yale College* **47(5)**.

Cavoukian A. 2009. Privacy by design. *Available at https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf*.

Desai T, Ritchie F, Welpton R. 2016. "Five safes: designing data access for research" (PDF). In: *Bristol Business School Working Papers in Economics: Footnote 1*.

Dinaburg A. 2011. Bitsquatting: DNS hijacking without exploitation. In: *Proceedings of BlackHat Security*.

Dwork C, McSherry F, Nissim K, Smith A. 2006. Calibrating noise to sensitivity in private data analysis. In: *TCC*. Berlin, Heidelberg: Springer, 265–284.

Dwork C, Rothblum G. 2016. Concentrated differential privacy. *CoRR* DOI 10.48550/arXiv.1603.01887.

Enyinna PI. 2016. Radiological risk assessment of cosmic radiation at aviation altitudes (a trip from Houston Intercontinental Airport to Lagos International Airport). *Journal of Medical Physics/Association of Medical Physicists of India* **41(3)**:205 DOI 10.4103/0971-6203.189491.

Garfinkel SL, Leclerc P. 2020. Randomness concerns when deploying differential privacy. In: *Proceedings of the 19th Workshop on Privacy in the Electronic Society*. 73–86.

Govindavajhala S, Appel AW. 2003. Using memory errors to attack a virtual machine. In: *2003 Symposium on Security and Privacy*. Piscataway: IEEE, 154–165.

Greenberg A. 2017. How one of Apple's key privacy safeguards falls short. Wired. *Available at https://www.wired.com/story/apple-differential-privacy-shortcomings/*.

Hsueh M-C, Tsai TK, Iyer RK. 1997. Fault injection techniques and tools. *Computer* **30(4)**:75–82 DOI 10.1109/2.585157.

IEEE Computer Society. 2019. IEEE standard for floating-point arithmetic. IEEE STD 754-2019. IEEE. *Available at https://standards.ieee.org/ieee/754/6210/*.

ISO. 2020. *Programming languages—C++, standard ISO/IEC 14882:2020*. Geneva, Switzerland: International Organization for Standardization (ISO).

Janko R. 1987. *Poetics with tractatus coislinianus, reconstruction of poetics II and the fragments of the on poets. By Aristotle*. Cambridge: Hackett.

Kairouz P, Oh S, Viswanath P. 2015. The composition theorem for differential privacy. In: *International Conference on Machine Learning*. Cambridge: PMLR, 1376–1385.

Kifer D, Machanavajjhala A. 2011. No free lunch in data privacy. In: *Proceedings of the 2011 ACM SIGMOD International Conference on Management of data*. 193–204.

King G, Persily N. 2019. A new model for industry—academic partnerships. *PS: Political Science & Politics* **53(4)**:703–709 DOI 10.1017/S1049096519001021.

King G, Persily N. 2020. Unprecedented Facebook URLs dataset now available for academic research through social science one; IQSS, Harvard. *Available at https://socialscience.one/blog/unprecedented-facebook-urls-dataset-now-available-research-through-social-science-one*.

Lécuyer M, Spahn R, Vodrahalli K, Geambasu R, Hsu D. 2019. Privacy accounting and quality control in the sage differentially private ML platform. In: *Proceedings of the 27th ACM Symposium on Operating Systems Principles*. 181–195.

Li Z, Kihl M, Lu Q, Andersson JA. 2017. Performance overhead comparison between hypervisor and container based virtualization. In: *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*. Piscataway: IEEE, 955–962.

Mettler FA Jr, Huda W, Yoshizumi TT, Mahesh M. 2008. Effective doses in radiology and diagnostic nuclear medicine: a catalog. *Radiology* **248(1)**:254–263 DOI 10.1148/radiol.2481071451.

Munro R. 2011. Ration dose chart, XKCD. *Available at https://xkcd.com/radiation/*.

Munro R. 2023. Ration dose char explainationt, explain XKCD. *Available at https://www.explainxkcd.com/wiki/index.php/Radiation*.

NISO. 2015. Consensus principles on users' digital privacy in library, publisher, and software-provider systems. *Available at https://www.niso.org/publications/privacy-principles*.

OECD. 2023. Emerging privacy-enhancing technologies: current regulatory and policy approaches. OECD Digital Economy Papers, No. 351, OECD Publishing, Paris. *Available at https://doi.org/10.1787/bf121be4-en*.

Pejó B, Desfontaines D. 2022. *Guide to differential privacy modifications: a taxonomy of variants and extensions*. Berlin: Springer Nature.

Quote Investigator. 2018. In theory, theory and practice are the same. *Available at https://quoteinvestigator.com/2018/04/14/theory/*.

Rogers R, Subramaniam S, Peng S, Durfee D, Lee S, Kancha SK, Sahay S, Ahammad P. 2020. Linkedin's audience engagements API: a privacy-preserving data analytics system at scale. *ArXiv preprint* DOI 10.48550/arXiv.2002.05839.

Soft Error. 2022. Wikipedia. *Available at https://en.wikipedia.org/wiki/Soft_error*.

Vadhan SP. 2012. Pseudorandomness. *Foundations and Trends® in Theoretical Computer Science* **7(1–3)**:1–336 DOI 10.1561/0400000010.

Van Stempvoot S, Portinga DA, Johnson M. 2022. *Brief of the onion as amicus curiae in support of petitioner*. Ohio: Novak v. City of Parma.

von Neumann J. 1945. First draft of a report on the EDVAC. University of Pennsylvania. *Available at https://archive.computerhistory.org/resources/text/Knuth_Don_X4100/PDF_index/k-8-pdf/k-8-u2593-Draft-EDVAC.pdf*.

Wagner I, Eckhoff D. 2018. Technical privacy metrics: a systematic survey. *ACM Computing Surveys (CSUR)* **51(3)**:1–38 DOI 10.1145/3168389.

Wang Y, Wu X, Hu D. 2016. Using randomized response for differential privacy preserving data collection. In: *Proceedings of the EDBT/ICDT, 2016 Joint Conference*. Bordeaux, France.

Willis LE. 2014. Why not privacy by default? *Berkeley Technology Law Journal* **29**:61–133.

Wood A, Altman M, Bembenek A, Bun M, Gaboardi M, Honaker J, Nissim K, O'Brien DR, Steinke T, Vadhan S. 2018. Differential privacy: a primer for a non-technical audience. *Vanderbilt Journal of Entertainment & Technology Law* **21(17)**:209 DOI 10.2139/ssrn.3338027.

Wood A, Altman M, Nissim K, Vadhan S. 2020. Designing access with differential privacy. In: Cole, Dhaliwal, Sautmann, Vilhuber, eds. *Handbook on Using Administrative Data for Research and Evidence-based Policy*. Cambridge, MA: Abdul Latif Jameel Poverty Action Lab DOI 10.31485/admindatahandbook.1.0.

Zhou Li, Ying M. 2017. Differential privacy in quantum computation. In: *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*. Piscataway: IEEE, 249–262.

Ziegler JF, Lanford WA. 1979. Effect of cosmic rays on computer memories. *Science* **206(4420)**:776–788 DOI 10.1126/science.206.4420.776.