

Pragmatism: The Missing Piece in Privacy Enhancing Technologies

REBECCA BALEBAKO, Zurich University of Applied Sciences (ZHAW), Switzerland

Current policy and academic focus on sophisticated "Privacy Enhancing Technologies" (PETs) creates a significant resource mismatch for most small and medium businesses. While complex PETs are heralded by regulators, they often require niche expertise and scale that many companies simply do not possess. This paper argues for a broader definition of privacy tech that includes "Pragmatic PETs"—accessible, well-understood engineering practices like automated data deletion and access controls. By prioritizing these scalable foundations, businesses can achieve more effective, company-wide privacy by design.

CCS Concepts: • **Security and privacy**;

Additional Key Words and Phrases: Privacy, Opinion, Privacy Enhancing Technology

ACM Reference Format:

Rebecca Balebako. 2026. Pragmatism: The Missing Piece in Privacy Enhancing Technologies . 1, 1 (July 2026), 4 pages. <https://doi.org/XXXXXXX.XXXXXXX>

Imagine the privacy hero of a midsize company. Previously a legal generalist, she now is responsible for data protection and compliance. No one has owned this role previously, and she inherits confusion about what data is being collected, how it is used, and where it is stored. She needs pragmatic tools that can bring order to the chaos and reduce the risks of storing and using personal data. Seeking guidance, she is delighted to learn about "Privacy Enhancing Technologies" or PETs. The term "Privacy Enhancing Technologies" (PETs) has become a high-status buzzword in the privacy world, but are they actually the most effective tool for our hero, or others like her?

Why has our hero become interested in PETs as the primary answer to her chaos? What exactly are PETs, and do they truly offer the 'magic bullet' for data protection? Finally, if PETs aren't the panacea for the midsize enterprise data protection, what practical, effective alternatives should she be building her foundation on instead?

Our hero can be found in many midsize companies, where the privacy work is often seated in the legal or compliance departments [5]. Therefore, the decisions about how to invest in privacy technologies will often be made by teams attuned to compliance, risk, or legal issues. The privacy recommendations made by regulators and policy-makers can influence what gets implemented in industry.

Policy-makers are talking about "Privacy Enhancing Technologies." Several governmental organizations, including the Information Commissioners Office in the UK [3] the Federal Reserve Bank of San Francisco in the USA [1] and Singapore's InfoComm Media Development Authority (IMDA), [4] and inter-governmental organizations, including the Organisation for Economic Co-operation and Development (OECD) have offered descriptions of PETs [8]. These reports are targeted at Data

Author's Contact Information: [Rebecca Balebako](mailto:rebecca.balebako@zhaw.ch), rebecca.balebako@zhaw.ch, Zurich University of Applied Sciences (ZHAW), Zürich, Switzerland.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2026 Copyright held by the owner/authors. Publication rights licensed to ACM.

ACM XXXX-XXXX/2026/7-ART

<https://doi.org/XXXXXXX.XXXXXXX>

Protection Officers and privacy leadership in industry. Several reports emphasize that PETs can protect user privacy and encourage their adoption.

However, these reports define PETs narrowly. Across the entire spectrum of technologies that help with privacy, only a few possibilities are included in these lists and definitions of PETs.

The lists of PET technologies are similar but not identical across these reports from governments and IGOs. Typically they include the three categories:

- Obfuscation and Anonymization: Differential Privacy is frequently named.
- Privacy Preserving Computation: Homomorphic Encryption, Multi-Party Computation and Trusted Execution Environments.
- Federated Learning for Machine Learning: sometimes also called distributed learning.

There are sound technical reasons to emphasize these specific technologies. Differential privacy offers a principled approach to reasoning about the privacy of individuals in a dataset. Privacy preserving computation allows mathematical computations to be performed on data without the data being seen. Federated learning allows more personal data to remain local, and less data is shared less often with a server computing a larger machine learning model.

These PETs are all implemented on specific datasets for specific use cases; they are not general purpose for all the data in a company. For example, for the implementation of differential privacy, there are many knobs to be tuned to find a good trade-off between what form of data is useful, and how much protection should be added. These decisions are made on a case by case basis. While PETs are justifiably heralded as the gold standard for data protection, for the average business, they represent a fundamental mismatch between ambition and operational reality; far from being a gateway to privacy by design, they often introduce a level of complexity that creates a huge leap instead of a first-step. First, these PETs require skilled teams and have limited available libraries or tools. Second, businesses stepping into privacy engineering will get more benefits by implementing privacy engineering systems across the business, not just improving one product or use case at a time. But PETs are practical for large, specific datasets, or for training machine learning models [10].

Why have “PETs” showed up on the radar for midsize businesses, when other privacy technologies might be easier to implement and offer broader protections? One reason may be that policymakers, particularly in the EU, spend effort regulating large tech companies. As firms like Google and Apple have championed PETs [7, 6], regulators have increased their PETs know-how to ensure that these PETs aren’t being used as a mathematical cloak.

In the past few years, academia also appears to be using the term “PETs” more and more. In 2023, the term “PETs” was rare in Call for Papers or computer science publishing venues, outside of the “PETs Symposium”. (Happily, the PETs Symposium, then and now, has a broad range of privacy topics, and is not restricted to the above PETs [9].) However, this may change. As of 2026, several syllabi for advanced courses covering PETs are online, indicating increasing coverage of PETs in academic programs.

To be fair, PETs are not just good at what they do. They are math-heavy, exciting, novel, and therefore fun. Students who want to stay in academia like topics with enough depth to specialize and write papers, which PETs have. However, this focus can leave an awareness and knowledge gap. With a focus on PETs, we are missing out on teaching more pragmatic options that protect privacy and can be implemented with less expertise.

0.1 Pragmatic PETs are better options for most businesses

Midsize businesses need to implement privacy and data protection, and know which tools are available to them. I refer to alternatives for midsize businesses as “Pragmatic PETs.” Pragmatic

PETs are simply technical enforcements of company policies. To be more specific, pragmatic PETs are technical configurations that: rely on well-understood technologies, don't require niche skills, and enhance data hygiene in a company. To make this more concrete, here are some examples of Pragmatic PETs that midsize companies can implement.

- **Automated deletion of old data:** Deleting data and files is not in itself a technical challenge. The command "rm" has been part of Unix for over 5 decades [2]. Almost all file and storage systems have deletion capabilities that can be automated. Removing forgotten data, unneeded, or expired data can reduce the threat surface for companies. The challenge is typically not technical, and usually more a business challenge to agree on retention periods for data.
- **Scrub Personally Identifying Information:** PII detection is the attempt to find information like addresses, phone numbers, or credit card numbers in text. While not trivial to implement from scratch, several commercial tools have existed for years, including those built into cloud provider offerings. More teams should be familiar with how they work and how to configure them.
- **Auto-Redaction Hooks:** Using PII filters or other tools, redact unneeded PII and personal information before it is stored in your system. Sometimes a company receives data from customers, or some tools may automatically log information about customers. Automated tools redact it before it becomes a headache.
- **Rate Limiting User-to-User sharing:** User-to-user sharing features (such as allowing users to share a personal photo directly with other users) is an attractive vector for attackers. Rate limit how much one user can share or request from other users to prevent bots or malicious actors from data scraping users profiles and mass-gathering personal information.

This is not a complete list, but is intended to give a flavor. While purists may categorize these as 'Data Hygiene', they serve the same functional role as a PET: a technical enforcement that reduces privacy risk. These examples fulfill the requirements of pragmatic PETs. They don't require specialist engineers, and can be built using widely available software and technology. Furthermore, these tools are applicable across a company once a company-wide policy is determined.

Pragmatic PETs should be at the tip of the tongue for all companies. But there is a gap between what privacy professionals hear about privacy technologies, and what makes sense for most businesses.

0.2 What can we do now?

We are currently asking businesses to adopt privacy tools designed for the world's largest tech giants, creating a hurdle for companies to get started with privacy engineering. PETs aren't the universal gateway to privacy by design. For a midsize business, they are often over-engineered and specific when scalable privacy engineering is needed. There are roles for educators, policy-makers, and privacy leadership here.

Educators can play a role in expanding discussions of pragmatic PETs. We need to make sure that our course offerings do not ignore the fundamental privacy technologies that help the vast majority of businesses. PETs need to be situated appropriately, and the use cases need to be clear. Conferences and journals can include implementation and usability of pragmatic PETs in their calls for papers. We hope to see more papers that deal with practical data privacy compliance issues.

Policymakers should pivot their guidance to pragmatic PETs. Instead of only highlighting cutting-edge technologies, emphasize for boring data hygiene that reduces risk across the company. This could help direct our privacy hero towards achievable first steps.

Privacy leadership in companies can take a breath. For the privacy heroes out there that are just getting started on privacy by design, or hiring your first privacy engineer, don't worry about the

exotic math behind PETs (yet). First implement the 'Pragmatic PETs' that fit your company's budget and expertise. If done right, these will prevent data leakage and reduce risk at a company-wide level.

PETs are powerful tools, but Pragmatic PETS are a necessary and practical first step for most businesses building up their privacy program. The most effective privacy tools aren't the ones with the most impressive proofs, it's the ones that can actually get deployed.

References

- [1] K Asrow and S Samonas. *Privacy Enhancing Technologies: Categories, Use Cases, and Considerations - San Francisco Fed*. June 2021. (Visited on 04/07/2026).
- [2] D Brock. *The Earliest Unix Code: An Anniversary Source Code Release*. Oct. 2019. (Visited on 03/31/2026).
- [3] ICO ICO. *Privacy-Enhancing Technologies (PETs)*. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/>. Ico.Org.Uk. June 2025. (Visited on 04/07/2026).
- [4] SIMDA. *Leverage Privacy Enhancing Technologies for Data Insights | IMDA*. <https://www.imda.gov.sg/resources/blog/blog-articles/unlock-the-power-of-data-pets>. Imda.Gov.Sg. June 2026. (Visited on 07/03/2026).
- [5] S Kanthasamy and J Jones. *Salary and Jobs Report 2025-26: Privacy, AI Governance and Digital Responsibility | IAPP*. <https://iapp.org/resources/article/salary-survey-summary>. Aug. 2025. (Visited on 05/06/2026).
- [6] J Krämer. *Data Protection by Platform: The Role of Private Actors in Shaping GDPR Compliance in the Mobile Ecosystem*. Rotterdam, Feb. 2026. ISBN: 978-94-6496-531-5.
- [7] MH Murphy and K Shrishak. *Protecting the 'Privacy' in Privacy-Enhancing Technologies: Lessons from Apple's NeuralHash Detection Proposal and Google's Privacy Sandbox*. SSRN Scholarly Paper. Rochester, NY, Mar. 2026. doi: [10.2139/ssrn.6393979](https://doi.org/10.2139/ssrn.6393979). Social Science Research Network: [6393979](https://ssrn.com/abstract=6393979). (Visited on 04/07/2026).
- [8] OECD. "Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches". In: *OECD Digital Economy Papers* (Mar. 2023). doi: [10.1787/bf121be4-en](https://doi.org/10.1787/bf121be4-en). (Visited on 03/31/2026).
- [9] *PETS Symposium*. <https://petsymposium.org/>. Symposium. 2026. (Visited on 04/07/2026).
- [10] N Ponomareva et al. "How to DP-fy ML: A Practical Guide to Machine Learning with Differential Privacy". In: *Journal of Artificial Intelligence Research* 77 (July 2023), pp. 1113–1201. issn: 1076-9757. doi: [10.1613/jair.1.14649](https://doi.org/10.1613/jair.1.14649). (Visited on 02/26/2026).