Privacy Engineering: Why Standards Are Still Out of Reach?

Abhishek Tiwari

Citation: *A. Tiwari*, ”Privacy Engineering: Why Standards Are Still Out of Reach?”, Abhishek Tiwari, 2024. doi:10.59350/6j2z7-ncs50

Published on: December 12, 2024

In contemporary technology environments, organisations are increasingly challenged with the complexities of privacy engineering. The evolving data governance and regulatory ecosystems demand not only technical ingenuity but also a deep understanding of legal frameworks and organizational dynamics. The role of the privacy engineer, though still emerging, sits at intersection, translating abstract privacy principles and compliance mandates into tangible technical controls and meaningful organisational practices. The article covers research findings reported by Zachary Kilhoffer and Devyn Wilder from University of Illinois at Urbana–Champaign in their recent presentation in 2024 USENIX Conference on Privacy Engineering Practice and Respect(see [1]). Their research findings derived from in-depth interviews with experienced privacy engineers, providing insight into their responsibilities, the ways in which they engage with standards and frameworks, and the challenges that shape this emerging profession.

Research Objectives and Methodology

The core research focus involved an exploratory inquiry into what privacy engineers do, how and whether they use privacy standards, and what opportunities and obstacles arise in their professional environments. The investigation interpreted the term “standard” broadly, recognizing that the notion of a standard is not itself standardized. Interviewees were encouraged to reflect on various formalised frameworks, principles, and approaches that guided or influenced their work, including widely recognised privacy principles like the Fair Information Practice Principles (FIPPs), OECD privacy principles, and methodologies such as privacy-by-design.

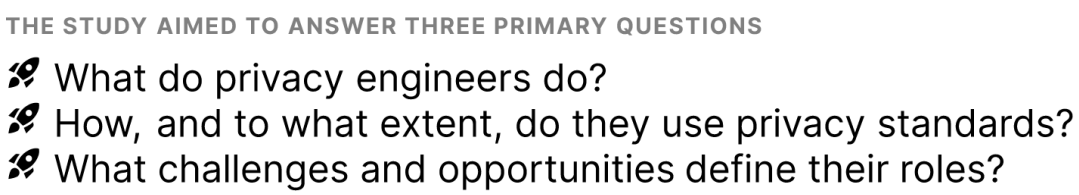

Figure 1: Research objectives

The study adopted a semi-structured interview approach to gather qualitative data from fourteen privacy engineers, each with at least two years of professional experience and all of whom claimed familiarity with privacy standards. Although sample size is relatively small, the participant sample included professionals working as employees or consultants across multiple industries and organisations. Nearly all respondents had extensive backgrounds in privacy, security, or engineering, often accumulating more than fifteen years of hands-on experience.

Role of standards

One of the study's most significant insights emerged from examining how privacy engineers view the role of standards in their practice. The interviews indicated that many privacy engineers spend a majority of their time on baseline compliance tasks, often dominated by legal imperatives and regulatory constraints. Rather than using recognized frameworks or industry standards as a core guiding force, these engineers frequently found themselves consumed by the day-to-day labor of meeting foundational legal requirements. Only when an organization reached a certain level of "maturity" in its privacy program did more aspirational uses of standards become feasible. Maturity in this sense meant that the organization had already mastered basic compliance and could start looking toward more ambitious goals, such as adopting the NIST Privacy Framework, implementing ISO standards, or utilizing other formal privacy structures to demonstrate continuous improvement and evolution beyond mere legal obligations.

This divide in organizational maturity also influenced who within the firm could effectively deploy or advocate for privacy standards. More senior or strategically placed privacy engineers, often those situated closer to management and legal teams, had greater autonomy to introduce or interpret standards. They could use these frameworks to communicate clearer expectations to engineers or product teams and to anchor discussions about best practices. In contrast, privacy engineers lower in the organizational hierarchy, or those not sufficiently resourced or trusted, struggled to implement anything beyond the minimum necessary to achieve compliance. Even seasoned professionals acknowledged that organizational cultures resistant to change or reluctant to allocate sufficient privacy budgets hampered the effective application of privacy standards. Privacy engineering teams needed both political capital and financial support to incorporate more rigorous frameworks. Without these resources, the role of recognized standards often devolved into a patchwork of internally developed guidelines, selectively borrowed controls, and other ad-hoc measures that lacked the recognized credibility and influence of formal certifications.

Interviewees recounted scenarios where privacy standards provided a valuable communication and persuasion tool, helping to align cross-functional teams around shared goals and consistent terminology. Managers, legal counsel, and product developers often spoke different professional languages, and privacy engineers served as bridge. Standards, when invoked, offered a common reference point

to explain what “good” looks like in the domain of privacy, and to set realistic, objectively defined targets for improvement. Yet the uptake of standards was not always an easy sell. In some contexts, referring to frameworks like ISO 27001 or the NIST Privacy Framework helped create organizational buy-in and secure additional resources. In others, the internal audience viewed the pursuit of standards as a luxury or a distraction, providing no meaningful competitive advantage and imposing additional burdens on already stretched teams.

Piecemeal Adoption

Several structural and contextual factors further complicated the adoption of standards. Budget constraints were a frequent source of frustration. Tools and automation platforms that could simplify privacy management and data governance were often beyond the reach of privacy engineers who could not secure funding. Without the proper software and technology stack, tasks like managing access requests or verifying vendor trustworthiness became cumbersome and error-prone. Organizational culture also played a decisive role. As stated earlier, many privacy engineers felt as though they operated under the close supervision of legal teams, with limited autonomy or freedom to shape privacy strategy. The complexity of legal environments, especially at scale in large multinational organizations, introduced another layer of difficulty. Dozens or hundreds of products deployed across multiple jurisdictions, each with its own privacy regime, demanded a level of orchestration and interpretation that standards could theoretically clarify. Yet without a mandate and capacity to go beyond basic compliance, the promise of standards often remained unrealized.

The research indicated that certain industry segments found more direct utility in privacy standards, particularly in areas where certification is a prerequisite to do business, such as cloud services integrating with government entities. Yet for many consumer-facing technology companies, the added value of formal privacy certification remained unclear. Although standards can confer reputational benefits, the ultimate reality is that most customers select products based on price, features, and reliability rather than whether a company’s internal privacy controls meet a recognized benchmark.

Taken together, these findings reveal that privacy standards operate in a nuanced environment where legal mandates, organizational culture, budgetary constraints, and communication challenges all affect their practical utility. The majority of privacy engineers struggle to move beyond statutory compliance due to lack of resources, limited authority, or insufficient organizational buy-in. Those who do manage to draw on standards primarily treat them as flexible guides to assemble custom in-house frameworks, rather than as neatly packaged sets of controls to adopt wholesale. Moreover, even seasoned professionals recognized that standards alone are insufficient if the underlying culture and financial support are absent.

Conclusion

While privacy engineers recognize the potential benefits of standards and frameworks for setting goals, mediating communication between legal and technical teams, and signaling privacy leadership, the reality of their usage is limited by practical constraints. The organizational, legal, and cultural complexities overshadow any straightforward adoption of recognized standards, except in those organizations mature enough to move beyond basic compliance. For privacy engineers, the challenge is to advocate not only for adherence to best practices but also for the resources, autonomy, and strategic positioning necessary to leverage standards in a substantive way.

References

[1] Z. Kilhoffer and D. Wilder, “Cache-22: Doing Privacy Engineering with Privacy Standards,” in *2024 USENIX Conference on Privacy Engineering Practice and Respect*, 2024. Available: https://www.usenix.org/conference/pepr24/presentation/kilhoffer