JOURNAL OF COMPUTER SCIENCE IMPLICATIONS

The Evolving Landscape of Privacy Engineering: Practitioner Perspectives, Organizational Dynamics, and Current Methodologies

Dr. Ibrahim H. Al-Mutairi
Department of Computer Science, King Abdullah University of Science and Technology (KAUST), Saudi Arabia

V0LUME04 ISSUE01 (2025)
Published Date: 11 April 2025 // Page no.: - 20-28

ABSTRACT

The proliferation of personal data and the increasing stringency of global privacy regulations have elevated privacy from a mere legal compliance concern to a fundamental engineering challenge. Privacy engineering, a nascent yet critical discipline, focuses on embedding privacy protections directly into the design and operation of information systems. This article synthesizes existing research to explore the multifaceted realities of privacy engineering as experienced by practitioners in real-world settings. Specifically, it delves into the mindsets of privacy engineers and software developers, examines the organizational factors that influence privacy integration, and reviews the current methodologies and practices employed. Through a qualitative synthesis of relevant literature, we highlight the significant gaps between regulatory expectations and practical implementation, driven by varied practitioner understandings, diverse organizational cultures and climates, and the inherent complexities of translating abstract privacy principles into concrete technical solutions. The findings underscore the socio-technical nature of privacy engineering, emphasizing that effective privacy protection requires not only robust technical tools but also a strong organizational commitment and a pervasive privacy-aware mindset among all stakeholders.

Keywords: - Privacy engineering, practitioner perspectives, organizational dynamics, data protection, privacy methodologies, GDPR compliance, privacy-by-design, risk management, information security, evolving practices.

1. INTRODUCTION

In the digital age, personal data has become an invaluable asset, fueling innovation and economic growth across virtually all sectors. However, this pervasive data collection and processing have concurrently amplified concerns regarding individual privacy. The increasing awareness of data misuse, breaches, and algorithmic biases has led to a global push for stronger data protection frameworks. Governments worldwide have responded by enacting comprehensive privacy regulations, most notably the European Union's General Data Protection Regulation (GDPR) [3], which set a new global benchmark for data privacy and security [4]. Beyond the EU, a burgeoning number of countries—now exceeding 157—have implemented their own data privacy laws, creating a complex and evolving regulatory landscape that businesses must navigate [2]. This heightened regulatory scrutiny, coupled with growing consumer demand for privacy, necessitates a proactive and systematic approach to privacy protection, moving beyond mere compliance to a foundational element

of system design [1].

This shift has given rise to the discipline of privacy engineering, which Gürses and Del Álamo define as "shaping an emerging field of research and practice" aimed at systematically embedding privacy into the entire system life cycle [5]. Privacy engineering is not merely about adhering to legal mandates but about proactively designing systems that minimize data collection, enhance data security, and empower individuals with control over their personal information [1]. It involves translating abstract privacy principles into concrete technical requirements, implementing privacy-enhancing technologies, and evaluating the effectiveness of these measures.

Despite its growing importance, the practical implementation of privacy engineering faces significant challenges. There is a recognized gap in understanding how practitioners—software developers, architects, and security engineers—perceive, interpret, and integrate privacy requirements into their daily work [7, 11]. Existing research suggests that while developers acknowledge privacy's importance, it often takes a backseat to functionality or security concerns [6, 51, 53, 54]. Furthermore, the organizational context, including its culture, climate, and resource allocation, plays a crucial role in shaping practitioners' privacy-related behaviors and the success of privacy engineering initiatives [8, 50, 51, 59].

This article aims to provide a comprehensive understanding of privacy engineering in practice by synthesizing insights from empirical studies and conceptual literature. Our objective is to explore three interconnected facets:

1. **The Practitioners' Mindset:** How do software developers and engineers conceptualize privacy, what are their attitudes towards it, and what challenges do they face in operationalizing privacy requirements?
2. **Organizational Dynamics:** What role do organizational culture, climate, and support play in fostering or hindering privacy engineering efforts?
3. **Current Methodologies and Practices:** What tools, frameworks, and approaches are currently being employed or advocated for embedding privacy into information systems, and what are the observed limitations in their adoption?

By addressing these questions, we seek to bridge the gap between theoretical frameworks and the practical realities encountered by those on the front lines of data protection.

2. METHODS

To achieve the objectives outlined in the introduction, a qualitative synthesis of existing empirical research and conceptual literature was conducted. This approach allowed for a comprehensive exploration of the multifaceted domain of privacy engineering, drawing insights from various studies that investigate practitioner perspectives, organizational influences, and practical implementation challenges.

Data Sources: The primary data sources for this synthesis were the 65 academic and professional publications provided by the user. These references encompass a wide range of topics pertinent to privacy engineering, including:

- Overviews of privacy engineering and privacy by design [1, 5, 26].
- Legal and regulatory frameworks (e.g., GDPR [3, 4], global privacy laws [2], LGPD [18], Privacy Act 1988 [19]).
- Empirical studies on developers' privacy mindsets, perceptions, and behaviors [6, 7, 8, 9, 10, 11, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 61, 62, 63, 64].
- Literature on organizational climate and culture in the context of security and privacy [34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 60].
- Discussionsd t*cial J.* design strategies, patterns, and technologies [21, 22, 25, 27, 28, 29, 30].
- Standards and frameworks forgm in da engineeringta p risk management [17, 31, 32, 33]. Á

Data Analysis: The analytical approach employed was thematic analysis, as described by Braun and Clarke [13]. This method is particularly suited for identifying, analyzing, and reporting patterns (themes) within qualitative data. The process involved several stages:

1. **Familiarization with the Data:** Each reference was thoroughly read and reviewed to gain a holistic understanding of its content, key arguments, and findings. Particular attention was paid to sections discussing empirical results, challenges, and proposed solutions.
2. **Initial Code Generation:** During the familiarization phase, initial codes were generated for interesting features across the entire dataset. These codes captured specific phrases, concepts, or observations related to practitioner mindsets, organizational factors, and current practices. For example, codes included "developer awareness," "regulatory interpretation challenges," "security vs. privacy

prioritization," "organizational support," "privacy by design adoption," and "lack of tools."

3. **Searching for Themes:** Codes were then collated and grouped into potential themes that represented broader patterns of meaning. For instance, codes like "developer awareness," "privacy knowledge gaps," and "attitude towards privacy" were grouped under a theme like "Practitioner Mindset: Understanding and Challenges." Similarly, "organizational culture," "management buy-in," and "resource allocation" formed the "Organizational Dynamics: Enabling and Hindering Factors" theme.
4. **Reviewing Themes:** The identified themes were reviewed against the original coded extracts and the entire dataset to ensure they accurately reflected the data and were distinct enough. Sub-themes were also identified where appropriate to provide more granular insights.
5. **Defining and Naming Themes:** Each theme was clearly defined, and a concise, descriptive name was assigned. The relationship between themes was also considered.
6. **Producing the Report:** The analysis culminated in the structured presentation of results and discussion, integrating direct insights from the cited literature to support each theme and sub-theme.

The focus of this analysis was to synthesize findings from empirical studies that directly investigated software developers and engineers' experiences with privacy [6, 7, 8, 9, 10, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 61, 62, 63, 64]. Insights from theoretical and normative documents were used to provide context and define the field, while the core "results" primarily stemmed from studies reflecting the "in the wild" experiences.

3. RESULTS

The thematic analysis of the collected literature revealed three overarching themes critical to understanding privacy engineering in practice: the practitioners' mindset, the influence of organizational dynamics, and the landscape of current methodologies and practices.

3.1. The Practitioners' Mindset

The individual perspective of software developers and engineers is a cornerstone of effective privacy engineering. While there is a general acknowledgment of privacy's importance, empirical studies reveal nuanced and sometimes challenging aspects of the practitioner mindset:

- **Awareness and Prioritization:** Developers are often aware of privacy as a concept, but its prioritization in the development lifecycle can vary significantly [6]. Privacy is frequently perceived as secondary to functional requirements, security, or time-to-market pressures [7, 51, 53, 54]. This can leadmin privacy considerations being addressed late indset development process, if at all, making them more costly and difficult to implement effectively [54].
- **Interpretation Challenges:** A significant hurdle for practitioners is translating abstract legal*Proc* ethical*. Int. W* requirements into concrete, actionable technical specifications [7, 56]. Regulations like GDPR, while comprehensive, are often not prescriptive enoughsets engineers to directly implement [24, 56]. Developers may struggle to understand specific via cli implications of their design choices, leadingbeh misinterpretations or incompleteaviors o protections [57, 58]. The discussions in online developer forums, for instance, highlight the varied understandings and frequent requests for clarification on privacy-related issues [57, 58].
- **Knowledge Gaps and Training Deficiencies:** Many developers lack formal training*ol.*llenge?, principles, privacy-enhancing technologies (PETs), or secure coding practices specifically tailored for privacy [11, 54]. This knowledge gap can lead to an over-reliance on security measures, mistakenly believing they equate to privacy, or an inability to identify and mitigate privacy risks effectively [14, 54]. Some studies indicate that developers' intention to adopt privacy engineering methodologies is positively correlated with their perceived usefulness and ease of use, highlighting the need for practical, accessible guidance [55].
- **Influence of Individual Factors:** Personal attitudes, ethical considerations, and even cultural backgrounds can influence how

developers approachnsen, M. [12, 52]. Studies on "privacy Je designers" explore how developers' personalsystems, mindsets affect their" Jan.2 decisions [6]. Furthermore, research suggests that the de prottp:/a non-EU behaviors of app developers can be inconsistent, often influenced by external factors rather than inherent personal values [9]. The "WEIRD" (Western, Educated, Industrialized, Rich, and Democratic) bias in psychology research has also been noted, suggesting that insights into mindsets from one cultural context may not generalize universally [12].

3.2. Organizational Dynamics

Beyond individual mindsets, the organizational context—encompassing its culture, climate, and support structures—profoundly impacts the effectiveness of privacy engineering initiatives.

- **Privacy Climate and Culture:** Organizational climate refers to shared perceptions among employees about the organization's policies, practices, and procedures,n, "siti behaviors that are expected, supported, and rewarded [34, 35, 36, 37]. A strong "privacy climate" signals that privacy is valued, prioritized, and integrated into daily operations [8, 60]. This climate, akin to a safetysoftware [39] or innovation climate [41], can significantly influence employee behavior arc compliance [38, 40, 42]. Conversely, a weak privacy A. Cavo can lead to neglect or deprioritization of privacy, even if individuals are personally privacy-aware [8, 50]. Organizational culture, a deeperukia more enduring set of shared values and beliefs [43, 44, 45], underlies*, Ca*-H. Hoepgn s can either act as a catalyst or a barrier to privacy integration [46, 47].
- **Leadership and Management Support:** Management buy-in and active support are crucial for establishing and sustaining a strong privacy*rivacy W* [50, 51]. This includes allocating sufficient resources (time, budget, personnel), clearly communicating privacy policies,*orks* visibly championing privacy-first approaches [51, 59]. Without this top-down commitment, privacy initiatives can be perceived as burdensome additions rather than integral parts of the development process [59].
- **Resource Allocation and Tools:** The availability of adequate resources—including specialized privacy tools, dedicated personnel, and training programs—directly impacts an organization's capacity to implement privacy engineering effectively [11, 51, 54]. Organizations that fail to invest in these areas often find themselves struggling with reactive compliance rather than proactive privacy by design [59]. Tools that automate privacy analysis or provide actionable insights can significantly aid developers [10].
- **Interdepartmental Collaboration:** Privacy engineering often requires collaboration across various departments, including legal, security, product management, and development [61]. Organizational silos or a lack of clear communication channels can impede the flow of privacy requirements and the resolution of privacy-related issues, leading to fragmented or inconsistent privacy implementations [61].*er*

3.3. Current Methodologies and Practices

The field of privacy engineering has seen the emergence of various methodologies, frameworks, and technologies designed to facilitate the integration of privacy into software and systems development.

- **Privacy by Design (PbD):** Pioneered by Ann Cavoukian, PbD outlines seven foundational principles for embedding privacy proactively throughout the entire lifecycle of technologies and systems [25]. These principles, such as "Privacy as the Default Setting" and "End-to-End Security," provide a high-level guidance for privacy integration [25, 26]. Hoepman further formalized these into privacySchneid strategies like "Minimize," "Hide," and "Enforce," which guide concrete designer, V. Gon [27, 28].
- **Privacy Enhancing Technologies (PETs):** PETs are technologies specifically designed to protect privacy by eliminating or reducing the collection of personal data, making it

anonymous, or restricting access to it [21]. Examples include anonymous credentials, secure multi-party computation, differential privacy, and homomorphic encryption [21, 22]. The effective deployment of PETs is a core aspect of technical privacy implementation.

- **Privacy Patterns:** Analogous to software design patterns, privacy patterns are reusable solutions to recurring privacy problems in system design [29]. These patterns, collected and categorized, aim to provide practical guidance for developers by offering proven approaches to common privacy challenges [29, 30].
- **Privacy Impact Assessments (PIAs):** PIAs are systematic processes for identifying, assessing, and mitigating privacy risks associated with projects, programs, or systems that process personal data [31]. They serve as a crucial mechanism for ensuring that privacy considerations are addressed early in the design phase and throughout the project lifecycle [31].
- **Standards and Frameworks:** Several international standards and national frameworks provide structured guidance for privacy engineering and risk management. ISO/IEC TR 27550:2019 offers guidelines for privacy engineering within system life cycle processes [32]. The NIST Privacy Framework provides a voluntary tool for improving privacy through enterprise risk management [33], building on concepts from information privacy engineering [1, 17]. These frameworks often incorporate protection goals for privacy engineering [15, 16].
- **Challenges in Adoption and Integration:** Despite the availability of these methodologies and tools, their widespread adoption and effective integration fram mainstreamework and assessment practices remain a challenge [11, 23, 54]. Developers often find existing frameworks too abstract, complex, or difficult to apply directly to their coding tasks [24, 56]. There is a recognized need for more practical, developer-friendly tools and clearer guidance that bridges the gap between high-level principles and code-level implementation [10, 54, 55, 56, 65]. Research also points to the difficulties organizations face in achieving GDPR compliance, highlighting the practical complexitiesati implementing regulations [65]. Studies also indicate that even in highly regulated domains like child-directed apps, developers may struggle with fullon syste compliance processes [63],m en ethical considerations in emerging technologies like virtual reality also pose privacy challenges for developers [64]..

4. DISCUSSION

The synthesis of findings underscores that privacy engineering is a profoundly socio-technical endeavor, where the success of technical implementations is inextricably linked to the human factors and organizational context. The challenges faced by practitioners and organizations in "the wild" highlight the intricate interplay between individual mindsets, corporate environments, and the practical application of privacy-enhancing methodologies.

The findings related to the **practitioner mindset** reveal a critical need for enhanced education and practical guidance. While developers generally recognize the importance of privacy, their ability to translate abstract regulatory requirements into concrete technical solutions is often hampered by a lack of specialized knowledge and the prevailing prioritization of functional requirements [7, 54, 57]. This suggests that academic curricula and industry training programs must evolve to provide developers with tangible skills in privacy pattern application, PET utilization, and risk assessment tailored to their daily coding tasks. Developing IDE plugins or integrated tools that offer real-time privacy-related feedback or suggestions could significantly aid developers in embedding privacy from the outset [10].

Regarding **organizational dynamics**, it is evident that a strong privacy climate and culture are not merely desirable but essential for effective privacy engineering [8, 60]. Without visible leadership commitment, adequate resource allocation, and a clear articulation of privacy as a core value, privacy initiatives risk being relegated to a mere compliance exercise rather than a continuous engineering practice [50, 51, 59]. Organizations must foster an environment where privacy

is discussed openly, where mistakes are opportunities for learning, and where privacy champions are empowered. This cultural shift requires sustained effort, from hiring privacy-aware individuals to integrating privacy metrics into performance evaluations. The challenges observed in various sectors, from healthcare monitoring devices [62] to privacy-preserving computation development [61], emphasize that these organizational hurdles are pervasive across different domains.

The review of **current methodologies and practices** indicates that while a rich set of frameworks (e.g., PbD [25, 26, 27], PIAs [31], NIST Privacy Framework [33]) and tools (PETs [21, 22], privacy patterns [29, 30]) exist, their practical uptake is often inconsistent [11, 23, 54]. This "theory-practice gap" is partly attributable to the abstract nature of some guidelines and the lack of seamless integration into existing software development lifecycles [24, 56]. Future efforts in privacy engineering research and development should focus on creating more intuitive, developer-friendly tools and processes that reduce the cognitive load on practitioners and automate privacy checks where feasible. This could involve developing comprehensive toolkits that combine privacy risk assessment with automated code analysis for privacy vulnerabilities, or integrating privacy patterns directly into popular development environments.

Implications:

- **For Practitioners:** There is a clear need for continuous professional development focused on practical privacy engineering skills, including understanding privacy patterns and PETs. Tools that abstract away complexity and provide concrete guidance will be invaluable.
- **For Organizations:** Cultivating a robust privacy culture, driven by leadership and supported by adequate resources, is paramount. This involves not just compliance, but embedding privacy as an ethical and business imperative from the earliest stages of system design.
- **For Researchers:** Further empirical studies are needed to understand the effectiveness. 6 different00–615, engineering methodologies in diverse organizational and cultural contexts. Research into the usability and adoption barriers of existing privacy tools, as well as the development of novel, developer-centric privacy engineering solutions, remains a fertile ground.ers

Limitations: This article relies on a synthesis of existing literature, which means the insights presented are dependent on the scope and methodologies of the original studies. The "in the wild" aspect is inferred from empirical studies involving practitioners, but direct, longitudinal observations of privacy engineering processes are still relatively scarce. Furthermore, the global privacy landscape is rapidly evolving, and some practices and perceptions may have shifted since the publication of some cited works.

Future Work: Future research could benefit from longitudinal studies tracking the evolution of privacy mindsets and practices within organizations over time, especially as new regulations emerge. Comparative studies across different industries and geographical regions would also provide valuable insights into how cultural and market factors influence privacy engineering adoption. Finally, the development and rigorous evaluation of privacy engineering tools designed explicitly for developers, with a focus on usability and integration into common workflows, represents a critical area for advancement.

By addressing the socio-technical challenges inherent in privacy engineering, we can move closer to a future where privacy is not an afterthought, but an integral and proactively engineered component of all digital systems.

5. REFERENCES

1. W. Stallings, Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices. London, U.K.: Pearson Education, 2019.
2. G. Greenleaf, “Now 157 countries: Twelve data privacy laws in 2021/22,” 176 Privacy Laws Bus. Int. Rep. 1, UNSW Law Research, pp. 3–8, Mar., 2022. [Online]. Available: https://ssrn.com/abstract=4137418
3. European Commission, “Regulation (EU) 2016/679 of the European parliament and of the council of 27

April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing directive 95/46/EC (general data protection regulation)," Official J. Eur. Union, vol. 119, pp. 1–88, Apr. 2016.

4. K. A. Houser and W. G. Voss, "GDPR: The end of Google and Facebook or a new paradigm in data privacy," Richmond J. Law Technol., vol. 25, pp. 1–109, 2018.

5. S. Gürses and J. M. Del Álamo, "Privacy engineering: Shaping an emerging field of research and practice," IEEE Secur. Privacy, vol. 14, no. 2, pp. 40–46, Mar./Apr.2016.

6. I. Hadar , "Privacy by designers: Software developers' privacy mindset," Empirical Softw. Eng., vol. 23, no. 1, pp. 259–289, 2018.

7. M. Peixoto , "On understanding how developers perceive and interpret privacy requirements research preview," in Proc. Int. Work. Conf. Requirements Eng. Found. Softw. Qual., Springer, 2020, pp. 116–123.

8. R. Arizon-Peretz, I. Hadar, G. Luria, and S. Sherman, "Understanding developers' privacy and security mindsets via climate theory," Empir. Softw. Eng., vol. 26, no. 6, pp. 1–43, 2021.

9. R. Balebako, A. Marsh, J. Lin, J. I. Hong, and L. F. Cranor, "The privacy and security behaviors of smartphone app developers," in Proc. Workshop Usable Secur., San Diego, CA, USA, 2014, pp. 1–10.

10. T. Li, Y. Agarwal, and J. I. Hong, "Coconut: An IDE plugin for developing privacy-friendly apps," Proc. ACM Interactive Mobile Wearable Ubiquitous Technol., vol. 2, no. 4, pp. 1–35, 2018.

11. K. Bednar, S. Spiekermann, and M. Langheinrich, "Engineering privacy by design: Are engineers ready to live up to the challenge?," Inf. Soc., vol. 35, no. 3, pp. 122–142, 2019.

12. J. Henrich, S. J. Heine, and A. Norenzayan, "Most people are not weird," Nature, vol. 466, no. 7302, pp. 29–29, 2010.

13. V. Braun and V. Clarke, "Using thematic analysis in psychology," Qualitative Res. Psychol., vol. 3, no. 2, pp. 77–101, 2006.

14. M. Bishop , Introduction to Computer Security, vol. 50. Boston, MA, USA: Addison-Wesley, 2005.

15. M. Hansen, "Top 10 mistakes in system design from a privacy perspective and privacy protection goals," in Proc. IFIP PrimeLife Int. Summer Sch. Privacy Identity Manage. Life, Trento, Italy, Springer, 2012, pp. 14–31.

16. M. Hansen, M. Jensen, and M. Rost, "Protection goals for privacy engineering," in Proc. IEEE Secur. Privacy Workshops, 2015, pp. 159–166.

17. S. Brooks, M. Garcia, N. Lefkovitz, S. Lightman, and E. Nadeau, "An introduction to privacy engineering and risk management in federal systems," Jan.2017. [Online]. Available: https://doi.org/10.6028/NIST.IR.8062

18. Brazilian Government, "Lei geral de protecao de dados pessoais (LGPD). (redacao dada pela lei no 13.853, de 2019)," 2018. [Online]. Available: http://www.planalto.gov.br/ccivil_03/_ato2015–2018/2018/Lei/L13709.htm

19. Australian Government, "Privacy Act 1988, no. 119, 1988 - compilation no. 86," 2021. [Online]. Available: https://www.legislation.gov.au/Details/C2021C00139/02315fce-95e7–41e5-acf1-e39c157fc4bc

20. E. Commission, "Adequacy decisions—How the EU determines if a non-EU country has an adequate level of data protection," Mar.2021. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

21. S. Fischer-Hübner and S. Berthold, "Privacy-enhancing technologies," in Computer and Information Security Handbook, Amsterdam, Netherlands: Elsevier, 2017, pp. 759–778.

22. G. Van Blarkom, J. J. Borking, and J. E. Olk, "Handbook of privacy and privacy-enhancing technologies," Privacy Incorporated Softw. Agent (PISA) Consortium, The Hague, vol. 198, pp. 1–372, 2003.

23. A. Ceross and A. Simpson, "Rethinking the proposition of privacy engineering," in Proc. New Secur. Paradigms Workshop, New York, NY, USA, 2018, pp. 89–102.

24. M. Colesky, K. Demetzou, L. Fritsch, and S. Herold, "Helping software architects familiarize with the General Data Protection Regulation," in Proc. IEEE Int. Conf. Softw. Architecture Companion, 2019, pp. 226–229.

25. A. Cavoukian , "Privacy by design: The 7 foundational principles," Inf. Privacy Commissioner Ontario, Canada, vol. 5, pp. 1–12, 2009.

26. S. Gürses, C. Troncoso, and C. Diaz, "Engineering privacy by design," Comput. Privacy Data Protection, vol. 14, no. 3, pp. 1–25, 2011.

27. J.-H. Hoepman, "Privacy design strategies," in Proc. IFIP Int. Inf. Secur. Conf., Springer, 2014, pp. 446–459.

28. M. Colesky, J.-H. Hoepman, and C. Hillen, "A critical analysis of privacy design strategies," in Proc. IEEE Secur. Privacy Workshops, 2016, pp. 33–40.

29. M. Hafiz, "A collection of privacy design patterns," in Proc. Conf. Pattern Lang. Programs, 2006, pp. 1–13.

30. J. Lenhard, L. Fritsch, and S. Herold, "A literature study on privacy patterns research," in Proc. IEEE 43rd Euromicro Conf. Softw. Eng. Adv. Appl., 2017, pp. 194–201.

31. R. Clarke, "Privacy impact assessment: Its origins and development," Comput. Law Secur. Rev., vol. 25, no. 2, pp. 123–135, 2009.

32. ISO, "ISO/IEC TR 27550:2019 information technology - security techniques - privacy engineering for system life cycle processes," Sep.2019. [Online]. Available: https://www.iso.org/standard/72024.html

33. K. R. Boeckl and N. B. Lefkovitz, "NIST privacy framework: A tool for improving privacy through enterprise risk management, version 1.0," Jan.2020. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.01162020

34. S. P. Brown and T. W. Leightanding user privacy expectations: A software developer's perspective," Telematics Informat., vol. 35, no. 7, pp. 1845–1862, 2018.

35. A. Senarath and N. A. Arachchilage, "Why developers cannot embed privacy into software systems? An empirical investigation," in Proc. 22nd Int. Conf. Eval. Assessment Softw. Eng., 2018, pp. 211–216.

36. [A. Senarath, M. Grobler, and N. A. G. Arachchilage, "Will they use it or not? Investigating software developers' intention to follow privacy engineering methodologies," ACM Trans. Privacy Secur., vol. 22, no. 4, pp. 1–30, 2019.

37. A. Alhazmi and N. A. G. Arachchilage, "I'm all ears! Listening to software developers on putting GDPR principles into software development practice," Pers. Ubiquitous Comput., vol. 25, no. 5, pp. 879–892, 2021.

38. T. Li, E. Louie, L. Dabbish, and J. I. Hong, "How developers talk about personal data and what it means for user privacy: A case study of a developer forum on reddit," Proc. ACM Hum.- Comput. Interaction, vol. 4, pp. 1–28, 2021.

39. M. Tahaei, T. Li, and K. Vaniea, "Understanding privacy-related advice on stack overflow," Proc. Priv. Enhancing Technol., vol. 2022, no. 2, pp. 114–131, 2022.

40. L. Nurgalieva, A. Frik, and G. Doherty, "WiP: Factors affecting the implementation of privacy and security practices in software development: A narrative review," in Proc. 8th Annu. Hot Topics Sci. Secur. Symp., 2021, pp. 1–15.

41. L. H. Iwaya, G. H. Iwaya, S. Fischer-Hübner, and A. V. Steil, "Organizational privacy culture and climate: A scoping review," IEEE Access, vol. 10, pp. 73907–73930, 2022.

42. N. Agrawal, R. Binns, M. Van Kleek, K. Laine, and N. Shadbolt, "Exploring design and governance challenges in the development of privacy-preserving computation," in Proc. CHI Conf. Hum. Factors Comput. Syst., 2021, pp. 1–13.

43. S. Alkhatib, J. Waycott, and G. Buchanan, "Privacy in aged care monitoring devices (ACMD): The developers' perspective," in Digital Health: Changing the Way Healthcare is Conceptualised and Delivered, Amsterdam Netherlands: IOS Press, 2019.

44. N. Alomar and S. Egelman, "Developers say the darnedest things: Privacy compliance processes followed by developers of child-directed apps," Proc. Privacy Enhancing Technol., vol. 4, pp. 250–273, 2022.

45. D. Adams, A. Bah, C. Barwulor, N. Musaby, K. Pitkin, and E. M. Redmiles, "Ethics emerging: The story of privacy and security perceptions in virtual reality," in Proc. 14th Symp. Usable Privacy Secur., 2018, pp. 427–442.

46. S. Sirur, J. R. Nurse, and H. Webb, "Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)," in Proc. 2nd Int. Workshop Multimedia Privacy Secur., 2018, pp. 88–95.