PRIVACY BY RESEARCH AND DESIGN. FROM LITERATURE TO APPLICATION

Nimród Mike

Corvinus University of Budapest, Institute of Information Technology

Abstract: Privacy by Design (PbD) has been defined in many ways by the academia. It was seen as a design philosophy to improve the overall privacy friendliness of IT systems, a competitive business advantage, a set of technical solutions for privacy engineering and ultimately a legal obligation. The aim of this paper is to offer an overview on the origins and layers of PbD. Concluding remarks are provided on the growing attention PbD is receiving by a triangularization of the three forces shaping this concept.

Key words: Privacy by design, privacy patterns, design strategy.

1 INTRODUCTION

In the numerous attempts of conceptualizing privacy[1], nobody has yet determined it in such a way that describes all of its components. In 1967, Westin defined someway the privacy as the claim of an individual to determine what information about himself or herself should be known to others[2]. On the other hand, Bok claimed that privacy is "the condition of being protected from unwanted access of others – either physical access, personal information or attention. Claims to privacy are claims to control access[3]. Warren and Brandeis provided in 1890 that privacy should be understood as the right to determine to what extent an individual's thoughts and emotions should be communicated to others[4]. This was further developed by Westin in 1970[5], and empirically tested by Marshall in 1974[6]. Altman also introduced the units of privacy in 1976[7] as privacy of (a) person-to-person; (b) person-to-group; (c) group-to-person; (d) group-to-group. Based on the concept of control, Wolfe also provided a distinction between privacy as (a) control of communication with other people; and (b) control of information or knowledge about oneself[8].

Throughout history, privacy protection has received growing attention. This phenomenon is not revolutionary, rather evolutionary. The guiding principles and mechanisms of privacy protection had been reflected in the evolving legislation. In the early stages, Marshall provided the dimensions of privacy[9]. Others argued that the four prominent dimensions are the physical, psychological, social and informational dimensions[10].

Additional literature reviews of information privacy literature revealed possibilities for future work. Smith et al.[11], and Belanger and Crossler[12] preformed systematic literature reviews of the informational privacy literature. Their works are addressing the research community with recommendations on how informational privacy could benefit from specific research. Belanger and

[1] In detail, see Acquisti et al. 2016, pp. 2-48.
[2] Westin 2003, p.3.
[3] Koops et al. 2016, p 561.
[4] Warren – Brandeis 1890, pp. 193-220.
[5] Westin 1970.
[6] Marshall 1974, pp. 255-271.
[7] Altman 1976, pp. 7-29.
[8] Wolfe 1978, pp. 175-222.
[9] Marshall 1974, pp. 255-271.
[10] Burgoon et al. 1989, pp. 131-158.
[11] Smith et al. 2011, pp. 989 – 1015.
[12] Belanger – Crossler 2011, pp. 1017-1041.

Crossler provide that there is a need to move beyond the individual level of analysis and to utilize a broader diversity of sample populations[13]. They also argue that more design and action research should be conducted and more studies on the why related to privacy as opposed to the how[14]. Smith et al. recommended that empirically descriptive studies are deemed to have the potential to add value to the literature and that these should focus on antecedents to privacy concerns and on actual outcomes[15].

Both works argue that most researches have been focusing on privacy at an individual level, whereas group and organizational levels are still under-researched. Indeed, this is an important remark, since with the advent of machine learning and data analytics, the discussion has been shifting from individual privacy to collective privacy[16].

2 PRIVACY BY DESIGN

Privacy by Design (PbD) has been defined in many ways by the academia. It was seen as a design philosophy to improve the overall privacy friendliness of IT systems[17], a competitive business advantage[18], a set of technical solutions for privacy engineering and ultimately a legal obligation[19]. We notice a transcendence in the regulatory approach towards PbD. The shifting paradigm of the regulatory landscape first proposed these principles as not mandatory guidelines. Later adopted the same regulatory landscape provided these as express legal obligations. The high level principles have been proposed for computer systems in general, but did not provide enough details to be adopted by software engineers when designing and developing applications[20]. This lack of concrete guidelines on the 'how' of the PbD principles was constantly present in discussions. The PbD principles are meant to be technology neutral and therefore their primary goal is to focus on the 'what' and leave the 'how' to the development community. Part of this problem has its source in technicians and designers typically not being fluent in security and privacy[21]. Shapiro described it as:

> *"They may sincerely want security and privacy, but they seldom know how to specify what they seek. Specifying functionality, on the other hand, is a little more straightforward, and thus the system that previously could make only regular coffee in addition to doing word processing will now make espresso too. (Whether this functionality actually meets user needs is another matter.)[22]"*

The PbD philosophy, as denoted by researchers, is suffering from guidelines on how to map legal data protection requirements into system requirements and components[23]. As a response, privacy design strategies have been defined[24]. These strategies are often implemented by privacy patterns, which in turn rely on implementation of Privacy Enhancing Technologies (PETs). Lenhard et al. have summarized the existing literature on privacy patterns recently[25], whereas Senicar et al have extensively studied PETs[26].

---

[13] Ibid, p. 1038.
[14] Ibid.
[15] Smith et al. 2011, p. 1013.
[16] Mantelero 2017, p. 154.
[17] Hoepman 2014, p. 2.
[18] Cavoukian et al. 2010, p. 406.
[19] Rachovitsa 2016, p. 387.
[20] Perera et al. 2016, p. 84.
[21] Shapiro 2010, p. 27.
[22] Ibid.
[23] Baldassarre et al 2019, p. 20.
[24] Hoepman 2014, pp. 446-459
[25] Lenhart et al. 2017, pp. 194-201.
[26] Senicar et al. 2003, pp. 147-158.

3 ORIGINS OF PRIVACY BY DESIGN

Technology, and its rapid advancement thereof, has increasingly received attention from the field of ethics, which has evolved from being focused on theory to focusing on the sensitivity to values "built in" to technology and the process of doing so[27]. This is how the concept Value Sensitive Design (VSD) was born and was defined by Friedman et al. as the theoretically grounded approach to the design of technology accounts for human values in a principled and comprehensive manner throughout the design process[28]. Klitou affirms that VSD emphasizes the social and ethical responsibility of scientists, inventors, engineers or designers when researching, inventing, engineering and/or designing technologies that have or could have a potentially profound effect (negative or positive) on society and thus can create what is known as the normative technology[29]. PbD is essentially both an extension and application of VSD.

The aim of PbD is to develop systems, products and services that are in essence privacy-friendly and not intrusive. The aim of PbD is to give extended control towards users over their personal data and transparency in understanding how these are processed by the named systems, products and services. Hildebrandt and Koops see PbD as the "ambient law" in which the legal norms are articulated within the infrastructure and from a transition is seen from simple legal protection to legal protection by design[30].

Gaurda and Zannone also articulated PbD as an approach to bridging the difficult gap between legal (natural) language and computer/machine language to develop "privacy-aware systems"[31]. One of the goals of PbD, therefore, could be to create devices or systems that are capable of effectively implementing laws and rules that we as humans understand in the form of legal natural language (LNL) and devices, systems, computers, etc. understand in the form of legal machine language (LML)[32]. PbD was termed by Kenny and Borking as privacy engineering, describing it as a systematic effort to embed privacy relevant legal primitives into technical and governance design[33].

Through all the approaches that the research community has produced, one common theme can be identified in terms of PbD being driven by technical solutions rather than organizational approaches. Where in fact informational privacy in general is user-centered and often policy driven, the same cannot be stated for PbD, which is more developer-centered and driven by coding. In any case, PbD is not meant to be the archenemy of innovation. It should not be treated as a barrier towards technological development. In fact, history shows that neither PbD, nor legislation on technology cannot fulfill this role. PbD in reality aims to be a prudent driver of technological development[34] .

4 LAYERS OF PRIVACY BY DESIGN

PbD can have different entry points for embedding privacy, in terms of GDPR embedding "data protection by design and by default", in systems, technologies, and organizations[35]. There are many approaches towards PbD and prominently it is a complex notion with multiple facets. Spiekermann called privacy a fuzzy concept and difficult to protect[36].

First, it is as a legal requirement, and the importance of PbD being included in the basic principles of data protection was already highlighted Hustinx in 2010[37]. This can be effectively influenced by the law enforcement agencies. Hence, it should constitute a central problem for every law enforcement agency (*e.g.* national data protection authorities) to understand its layers.

---

[27] Albrechtslund in Klitou 2014, p. 260.
[28] Friedman in Ibid.
[29] Klitou 2014, p. 261.
[30] Hildebrandt and Koops in Ibid, p. 262.
[31] Guarda and Zannone 2009 in Ibid, p. 263.
[32] Ibid.
[33] Kenny and Borking 2002 in Ibid.
[34] Ibid, p. 264.
[35] Kurtz et al. 2018, p. 7.
[36] Spiekermann 2012, p. 39.
[37] Hustinx 2010, p. 254.

Second, it is a business interest. In this context, PbD acts as a market incentive and ultimately leads to disruptive innovation. This is influenced by decision-makers in organizations and by users of services and products that have a high incorporation rate of PbD. Existing literature also reflects that organizations may receive the benefits of proper data management, cost reduction and substantial increase in reputation and competitiveness[38].

Third, it is a philosophical stance for system development. This is influenced by developers themselves. Morales-Trujillo et al. conducted a systematic mapping study to determine the extent to which PbD has been applied in software development endeavors[39]. Gustavsson researched PbD as a stipulation in GDPR[40], while Pinto argued about the concept's regulatory effectiveness[41]. Other researchers carried out studies around possible scenarios where PbD and data subject rights seem incompatible[42]. Yet others presented the information system engineers' perspective[43].

In relation to PbD as a philosophy, this paper aims to boil down the fundamental principles into concrete strategies that are implemented with patterns and technologies. There are direct and indirect relationships between the layers of PbD. Figure 1 depicts these in a comprehensive form.

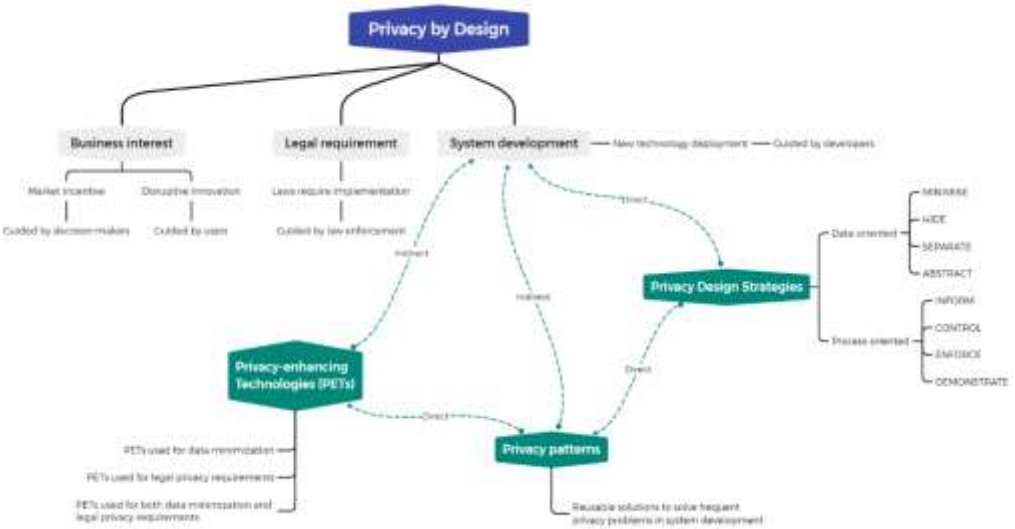

Figure 1. Relationship between PbD layers.

Consequences of a PbD-centric approach are omnipresent. By its integration in the GDPR, the philosophical stance is converted from a theoretical concept to a legal obligation and an essential principle of data protection that every controller and processor must respect[44]. A strategy for operationalizing PbD was defined by Kroener and Wright[45]. In terms of framework proposals, ElShekeil and Laoyookhong provided the APSIDAL framework[46], which provides potentially promising measures to operationalize the PbD principles, in the lights of a literature review performed by Blix et al[47].

[38] Teixeira et al. 2019, p. 413.
[39] Morales-Trujillo et al. 2018, pp. 1-14.
[40] Gustavsson 2020, pp. 1-46.
[41] Pinto 2017, pp. 1-61.
[42] Veale et al. 2018, pp. 105-123.
[43] Bu et al. 2020, pp. 1-16.
[44] Romanou 2017, p. 4.
[45] Kroener – Wright 2014, pp. 355-365.
[46] ElShekeil – Laoyoohong 2017, pp. 13-21.
[47] Blix et al. 2017, pp. 98-103.

Overall, we resonate and sympathize with the simple idea that came from academia: *technology alone is not inherently a threat to privacy; the main issue is how it is used*[48]. The role of PbD briefly is to guide the technology and development every day.

5 CONCLUSION: THE PBD TRIANGLE

The referenced literature demonstrates that both the industry and the academia mandates a coupled treatment towards the construct of PbD. Safe to say, the two notions of "Privacy" and "Design" became popularly connected into one formal expression: "Privacy by Design". Three competing forces are shaping this concept: laws and regulations, business goals and architecture designs. These forces carry their own influence in terms of ethics, economics and technology. PbD in software architecture is driven by the requirements stemming from privacy and data protection laws, and manipulated by business goals to achieve disruptive innovation. Through such disruptive innovation, society might witness infrastructure inversion as the product of disruptive innovation.

Kung et al. provided that such statement is not restrictive when we consider newly developed technology, which allows replacing personal data by equivalent provable anonymous credentials or data sets[49]. In this sense, technology bears with the highest impact on PbD. Data protection techniques, even when these are replacing personal data, serve one key role: to protect privacy. Perhaps, the efficient replacement of personal data with anonymous data results in avoiding the application of certain data protection laws and regulations. Yet, there are multiple laws to preserve privacy. Excluding one sub-set of it (*i.e.* personal data protection) shall not be interpreted as a "free-for-all" ideology, leaving the door open to massive deployment of privacy-invasive business practices.

In a similar vein, multiple business models incorporate PbD as an incentive. Decision-makers in organizations with such business models are utilizing PbD as a marketing tool. They strive to extrapolate their strategies to capture and accelerate consumer loyalty. Although, organizations are not always interested in protecting privacy. Examples include conflict between the business vision and consumer behavior, or constraints due to market conditions.

System designers are the pivotal factor in how PbD is conceptualized in Information Systems (IS). Developers, on the other hand, are required to implement the ideas drawn by designers. A natural separation between their roles is a need. They have to establish and maintain a coordinated relationship on addressing different organizational aspects (*e.g.* agreed-upon share of responsibilities) tied to Informantion and Communications Technology (ICT).

Senarath and Arachchilage undertook an empirical investigation that resulted in issues like contradiction between the requirements in the design and privacy requirements, lack of assurance that the implementation was undertaken in a complete and sufficient manner, lack of knowledge and confusion relating to requirements in practice[50]. Hadar et al. found another significant problem: that developers are actively discouraged from making informational privacy a priority, being expected to conform to norms and practices dictated by a negative organizational privacy climate[51]. Another finding was denoted by Bednar et al., which suggests developers are required to battle with lawyers and thus they deal with privacy related issues, mostly because they are required to do so[52]. Despite causing frustration, operationalizing informational privacy is mostly dependent on the developer's mindset.

However, placing this responsibility entirely in their hands is an unnecessary burden. In exchange, if the systems designers are actively taking on fulfilling privacy related requirements, the developers feel much safer as being guided by skilled individuals. Continuous and well-designed educational programs for privacy-preserving system designs would ensure preparation of individuals with such profiles. System designer's role should be separated from the rest of developers. This role should focus on displaying a sketch, which considers PbD in its core. Hence, a privacy focused architecture development is realized. During the design implementation, system designers should

[48] Alharbi et al. 2013, p. 703.
[49] Kung et al 2011, p. 2.
[50] Senarath – Arachchilage 2018, p. 4.
[51] Hadar et al. 2017, p. 20.
[52] Bednar et al. 2019, pp. 137-138.

constantly offer guidance to developers. Finally, during the verification and validation, system designers should provide their seal (*i.e.* approval or acceptance), which endorses conformity. A fundamental alteration to take better account from whomever is expected to implement PbD is to change the conjunction in the structure. Thus, what is needed is Privacy *from* Design, not Privacy *by* Design.

The triangularization of PbD refers to the above-mentioned three forces and their influence on the central topic of the thesis. An illustration is provided in Figure 2, which is called the PbD Triangle.

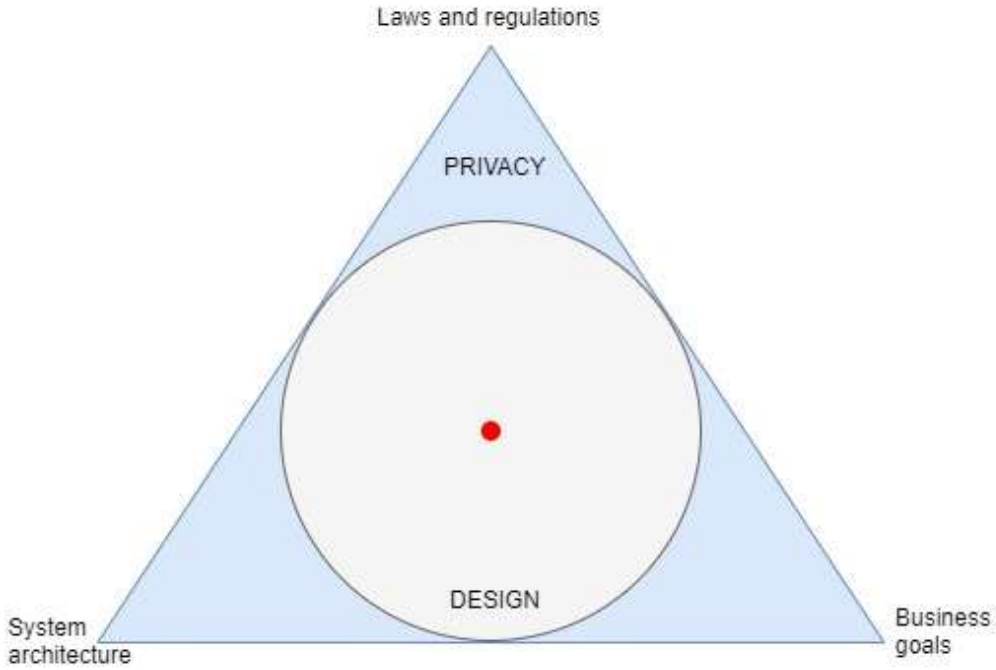

Figure 2. The PbD Triangle.

The triangle represents the concept of privacy as a fundamental human right, which is affected by laws and regulations, business goals and systems architectures. The circle inside the triangle is the 'design' in PbD. Certain designs may facilitate on primary level, business goals, and hence lean towards the right corner of the triangle. Other designs are focused on what the laws and regulations are mandating, which in turn, positions these closer to the top corner of the triangle. Nonetheless, some architectural designs are absolutistic and arbitrary, almost completly ignoring the other two forces. These care more about serving common interest of the public. Such designs are located in the left corner of the triangle.

The red dot in the middle of the circle is representing the privacy-equilibrium[53], which meansbalance, not perfection. Balance between the competing forces, so that privacy as a fundamental right can be effectively ensured. Moving the dot into any direction means a more pronounced ascendence towards a corner of the triangle. Consequently, the red dot is not a perfect state, since such thing, as of today, remains an impossible achievement.

Let us conclude this chapter with the words of Ugo Pagallo by saying, besides a stricter version of PbD as a way to decrease the "informational entropy" of the system through "digital air-bags," we find a further design mechanism compatible with the rule of law[54]. When encouraging

[53] A state in which opposing forces or influences are balanced.
[54] Pagallo 2012, p. 342.

people to change their behaviour by the means of design, the overall goal should be to reinforce people's pre-existing autonomy, rather than building it from scratch[55].

Acknowledgment:
The present publication is the outcome of the project „From Talent to Young Researcher project aimed at activities supporting the research career model in higher education", identifier EFOP-3.6.3-VEKOP-16-2017-00007 co-supported by the European Union, Hungary and the European Social Fund.

Bibliography:

1. Acquisti, A., Taylor, C. R., and Wagman, L. (2016): The Economics of Privacy. Journal of Economic Literature, Vol. 52, No. 2, 2016; Sloan Foundation Economics Research Paper No. 2580411.
2. Alharbi, I., Zyngier, S., and Hodkinson, C. (2013): Privacy by design and customers' perceived privacy and security concerns in the success of e-commerce. Journal of Enterprise Information Management. 26. 10.1108/JEIM-07-2013-0039.
3. Altman, I. (1976): Privacy. A concept analysis. Environment and Behaviour 8 (1), 7-29
4. Baldassarre, M., Barletta, V., Caivano, D. and Scalera, M. (2019): Privacy Oriented Software Development. 10.1007/978-3-030-29238-6_2.
5. Bednar, K., Spiekermann, S. and Langheinrich, M. (2019): Engineering Privacy by Design: Are engineers ready to live up to the challenge?, The Information Society, 35:3, 122-142, DOI: 10.1080/01972243.2019.1583296
6. Bélanger, F., and Crossler, R.E. (2011): Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly (35:4), 1017-1041
7. Blix, F., Elshekeil, S., and Laoyookhong, S. (2017): Data protection by design in systems development: From legal requirements to technical solutions. 98-103. 10.23919/ICITST.2017.8356355.
8. Bu, F., Wang, N., Jiang, B. and Liang, H. (2020): "Privacy by Design" implementation: Information system engineers' perspective. International Journal of Information Management. 53. 102124. 10.1016/j.ijinfomgt.2020.102124.
9. Burgoon, J., Parrott, R., Poire, B., Kelley, D., Walther, J., and Perry, D. (1989): Maintaining and Restoring Privacy Through Communication in Different Types of Relationships. Journal of Social and Personal Relationships - J SOC PERSON RELAT. 6. 131-158. 10.1177/026540758900600201.
10. Cavoukian, A., Taylor, S. and Abrams, Martin. (2010): Privacy by Design: essential for organizational accountability and strong business practices. Identity in the Information Society. 3. 405-413. 10.1007/s12394-010-0053-z.
11. ElShekeil, S.A. – Laoyoohong, S. (2017): GDPR Privacy by Design. From Legal Requirements to Technical Solutions. Master's Thesis. Stockholm University.
12. Gustavsson, S. (2020): An Assessment of Privacy by Design as a Stipulation in GDPR. Masters Thesis, Uppsala Universitet.
13. Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S. and Balissa, A. (2018): Privacy by designers: software developers' privacy mindset. Empirical Software Engineering. 23. 10.1007/s10664-017-9517-1.
14. Hoepman, J.-H. (2014). Privacy design strategies: (Extended Abstract). IFIP Advances in Information and Communication Technology. 428. 446-459.
15. Hustinx, P. (2010): Privacy by design: delivering the promises. Identity in The Information Society. 3. 253-255. 10.1007/s12394-010-0061-z.
16. Klitou, D. (2014): Privacy-Invading Technologies and Privacy by Design. 25. 10.1007/978-94-6265-026-8.

[55] Ibid.

17. Koops, B.-J., Newell, B.-C., Timan, T., Škorvánek, I., Chokrevski, T., and Galič, M. (2016): A Typology of Privacy. University of Pennsylvania Journal of International Law 38(2): 483-575 (2017); Tilburg Law School Research Paper No. 09/2016.

18. Kroener, I. and Wright, D. (2014): A Strategy for Operationalizing Privacy by Design. The Information Society, 30:5, 355-365, DOI: 10.1080/01972243.2014.944730

19. Kung, A., Freytag, J.-C. and Kargl, F. (2011): Privacy-by-design in ITS applications. 1 - 6. 10.1109/WoWMoM.2011.5986166.

20. Kurtz, C., Semmann, M. and Böhmann, T. (2018): Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors.

21. Lenhart, J., Fritsch, L. and Herold, S. (2017): A Literature Study on Privacy Patterns Research. 10.1109/SEAA.2017.28.

22. Mantelero, A. (2016): From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era. 10.1007/978-3-319-46608-8_8.

23. Marshall, N. (1974): Dimensions of privacy preferences. Multivariate Behavioral Research 19 (3), 255-271

24. Pagallo, U. (2021): On the Principle of Privacy by Design and Its Limits: Technology, Ethics and the Rule of Law. 10.1007/978-3-030-54522-2_8.

25. Perera, C., Mccormick, C., Bandara, A. Price, B. and Nuseibeh, B. (2016): Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms. IoT'16: Proceedings of the 6th International Conference on the Internet of Things. 10.1145/2991561.2991566.

26. Pinto, T.-B. (2017): The Regulatory Effectiveness of Privacy by Design. Tilburg University, Tilburg.

27. Rachovitsa, A. (2016): Engineering and lawyering privacy by design: Understanding online privacy both as a technical and an international human rights issue. International Journal of Law and Information Technology. 24. eaw012. 10.1093/ijlit/eaw012.

28. Romanou, A. (2017): The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. Computer Law and Security Review. 34. 10.1016/j.clsr.2017.05.021.

29. Senarath, A., and Arachchilage, N., (2018): Why developers cannot embed privacy into software systems? An empirical investigation. 211-216. 10.1145/3210459.3210484.

30. Seničar, V., Jerman, B. and Klobučar, T. (2003): Privacy-Enhancing Technologies—approaches and development. Computer Standards and Interfaces. 25. 147-158. 10.1016/S0920-5489(03)00003-5.

31. Shapiro, S. (2010): Privacy By Design: Moving from Art to Practice. Commun. ACM. 53. 27-29. 10.1145/1743546.1743559.

32. Smith, H.J., Dinev, T., and Xu, H. (2011): Information Privacy Research: An Interdisciplinary Review. MIS Quarterly (35:4), 989-1015

33. Spiekermann, S. (2012): The Challenges of Privacy by Design. Communications of The ACM - CACM. 55. 38-40. 10.1145/2209249.2209263.

34. Teixeira, G., Mira da Silva, M. and Pereira, R. (2019): The critical success factors of GDPR implementation: a systematic literature review. Digital Policy, Regulation and Governance. 21. 10.1108/DPRG-01-2019-0007.

35. Trujillo, M. E., García-Mireles, G., Matla Cruz, E. O. and Piattini, M. (2019): A Systematic Mapping Study on Privacy by Design in Software Engineering. CLEI Electronic Journal. 22. 10.19153/cleiej.22.1.4.

36. Veale, Michael and Binns, Reuben and Ausloos, Jef. (2018): When Data Protection by Design and Data Subject Rights Clash. SSRN Electronic Journal. 10.2139/ssrn.3081069.

37. Warren, S., Brandeis, L. (1890): The right to privacy. Harward Law Review IV (5), 193-220.

38. Westin, A. (1970): Privacy and Freedom. Athaneum. New York

39. Westin, A. (2003): Social and Political Dimensions of Privacy. 59(2) Journal of Social Issues.

40. Wolfe, M. (1978): Childhood and privacy. In: Human Behavior and Environment. Advances in Theory and Research. Vol 3. Children and the Environment Plenum Press, New York, 175-222.

Contact information:
Nimród Mike LL.M.
nimrod.mike@uni-corvinus.hu
Corvinus University of Budapest
Fővám tér 8
1093 Budapest
Hungary