Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 196 (2022) 191–198

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2021

Analysis of critical success factors to mitigate privacy risks in IoT Devices

Sitesh Mohanty, Kathryn Cormican*, Chandrasekhar Dhanapathi

Enterprise Research Centre, School of Engineering and Lero – the Irish Software Research Centre, National University of Ireland, Galway

Abstract

This research aims to ascertain how to effectively mitigate privacy risks in IoT devices. A user-centric approach is employed to increase user control and flexibility. After a detailed analysis of the extant literature, critical success factors that are lauded to alleviate risks in IoT devices were synthesised and collated. These include anonymity, transparency, simplicity, explicit consent and GDPR. An instrument was developed based on these factors to ascertain which of these aspects are considered to be the most effective. Data were collected and analysed from 341 IoT device users, data protection/IT professionals, and IoT device manufacturers in the industry. Findings from this analysis reveal that transparency is the most important critical success factor, followed by GDPR, anonymity, explicit consent, and simplicity, respectively. Based on these findings, a self-assessment scorecard was developed to enable analysts and decision-makers to assess their current performance against best practices and to effectively mitigate privacy risks in IoT devices.

Peer-review under responsibility of the scientific committee of the CENTERIS –International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2021

Keywords: Privacy, Internet of Things (IoT); Smart Devices; User-Centric; GDPR; Explicit Consent; Anonymity; Transparency; Simplicity; Privacy Scorecard

* Corresponding author.
E-mail address: kathryn.cormican@nuigalway.ie

Peer-review under responsibility of the scientific committee of the CENTERIS –International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2021
10.1016/j.procs.2021.12.005

1. Introduction

Privacy is widely seen as a significant barrier to the deployment of internet of things (IoT) technologies [1]. Users are particularly concerned about the recording of their private activities [2], and the collection and sharing of their personal data [3]. Users of IoT medical devices are especially concerned about the privacy threats associated with the collection and sharing of personal data such as the user's dietary habits, exercise information, running routes and sleep patterns with third parties [4]. Safeguarding privacy becomes increasingly challenging when IoT medical devices (such as smart test kits, smart assistive technologies, and smart meters/monitors) are utilized at home [5]. Privacy is subjective in comparison to security, which is more unbiased and less debatable, as it is easier to measure and assess security practices than privacy practices [6]. For example, the type of encryption existing on the device or in the cloud is quantifiable, whereas, in the case of privacy, there is a lot of obscurity/complexity. Consequently, there is a need for relevant privacy protection legislation [7], policies [8], approaches [9] and practice [10].

We advocate that a user-centric approach to privacy in IoT devices is required. In other words, all solutions must be user-focused and right-sized for the individuals. Users require transparency [11, 12, 13], GDPR [14], anonymity [12, 15, 16, 17], explicit consent [9, 12, 14, 18, 19] and simplicity [11,14, 20, 21]. However, there seems to be a lack of consensus or clarity on the elements related to IoT privacy from a user-centric perspective. For example, Wilkowska [22] studied smart home technology users and found that the most important requirements were general data protection and the perceived control over private data. While Kumar [23], advocates that user notification, awareness and permission by users were key requirements for the distribution of personal data. There is a dearth of empirical analysis on the conceptualisation and measurement of user-centricity [21] and user satisfaction [24] in the case of IoT data privacy. It seems that this deficit must be addressed. Therefore, the goal of this research is to identify the critical success factors required to effectively mitigate privacy risks in IoT devices.

This research adds to the body of knowledge in IoT privacy in several ways. Firstly, by presenting a synthesis of the extant literature in an important but under-researched space. Secondly, by capturing and analysing empirical data from users and professionals in the industry, prioritising these preferences, and analysing differences between the cohorts. Thirdly, by operationalising the findings of our analysis onto a user-friendly self-assessment scorecard that can help developers measure their performance against good practice and generate action plans that can be used to improve performance. Synthesis of the literature is followed by research methodology, findings and conclusion.

2. Synthesis of the literature

After an in-depth analysis and categorisation of the extant literature, the following key constructs were identified to effectively mitigate privacy risks in IoT devices.

2.1 Anonymity

The term 'anonymity' refers to the state of being unidentified [15, 16]. An anonymous network prevents anyone apart from the users to track or trace their identity in a way that information cannot be linked to the subject who provided it [15, 16]. As most communication protocols use unique identifiers to anonymize the users' identities, the possibility of misuse is high due to centralised data analysis [25] or unauthorized access [4]. Additionally, complete anonymity is improbable, as IoT devices can still be abused [26]. According to Zheng [13], end-users will tolerate the access and analysis of their data by producers of IoT devices if there is a perceived benefit associated with the use of their data. However, people do not want Internet Service Providers (ISPs), third parties, or the government to have access to their data [13]. Hence, anonymity is critical to protecting their usage and identity. According to Weber [27], the key elements to consider for IoT device design include unlinkability, undetectability, unobservability, communications content confidentiality and location privacy.

2.2 Transparency

Transparency helps people to obtain a comprehensive understanding of how their personal data is processed and utilised [11]. Transparency of data is crucial for privacy, especially with the growth of big data and the use of machine learning algorithms [11]. Many end-users will consent to the use of their personal data if there is a perceived benefit arising from it [13]. However, they need to know what data is collected, where and how it is used (e.g., through machine learning algorithms [28]), and why it is used (e.g., for targeted advertising by delivering sponsored content tailored to the IoT user's profile). When designing an IoT device, the following transparency-related factors should be considered: data acquisition, data storage, data processing (update), data transfer to the data controller, data transfer under specific guidelines, data access for the users, data processing (clarification) and data counter profiling capabilities [11, 14, 29].

2.3 Simplicity

Simplicity is the state of enabling the user to understand factors such as layout, interface organisation, functionality, structure, workflow, and framework easily through a basic or uncomplicated design [20]. It is a key determinant in creating a positive usability experience. Hence, IoT architectures and protocols must be simple. While IoT devices need to be user-centred and valuable to the user [21], it is equally important that the privacy policies for end-users are easy to understand [14], which is why simplicity is an important construct for safeguarding the privacy of IoT device users. Simplicity involves reduction, organisation, integration, prioritisation [20, 30] and data minimisation [19, 30, 31].

2.4 Explicit consent

Explicit consent is the process of asking for permission or agreement before collecting personal data [19]. While explicit consent is necessary for safeguarding the privacy of IoT device users, it is also imperative that the consent form must state that the data won't be used in a manner that it is not meant to be [18]. There are perceived benefits arising from the sharing of user data, such as providing customised services based on consolidated data [13]. However, individuals may not be comfortable sharing their data without the prior consent of their personal attributes (e.g., data relating to gender, religious beliefs, personal habits, etc.) [12]. Explicit consent involves: consent on data sharing purposes, i.e., personal data of the users will not be used for other purposes than those mentioned; consent on sharing of data, i.e., permission granted to allow relevant agencies to share the user's personal data; sharing of data before the user opts-out, i.e., personal data can be shared before the user opts-out; and no sharing of data before the user opts-in, i.e., personal data will not be shared until the user opts-in [18].

2.5 GDPR

GDPR is an EU legal directive for the collection and processing of personal information. It was implemented throughout the European Union on 25th May 2018. GDPR is an important element in mitigating the privacy risks of IoT device users. Some of the key requirements under GDPR include the right to be informed, the right of access, right of rectification, right to erasure, right to restrict processing, right to data portability, right to object and rights in relation to automated decision making and profiling [14].

3. Research methodology

Relevant literature relating to IoT, data privacy and user-centricity was thoroughly analysed, and constructs were identified. A standardized data collection instrument comprised of 25 questions was then created. A five-point Likert scale was used to assess respondents' attitudes about aspects of anonymity, transparency, simplicity, explicit consent, and GDPR. The instrument was pre-tested to minimise design flaws and establish its validity, accuracy, and acceptability. Reliability and validity were ensured by implementing appropriate sample designs and procedures, the implementation of adequate survey administration procedures, and data verification and correction measures. Probability one-stage cluster sampling was used in the study. Mutually homogenous yet internally heterogeneous groups were created [32], e.g., IoT device users, IoT device manufacturers and data protection/IT professionals. This was done to reflect the actual perception of the different types of respondents that have different experiences, perceptions, skillset, opinions, etc. The questionnaire was then distributed to users and key professionals working in the domain who were contacted through professional networks, communities of practice and snowballing. 341 usable responses were returned, out of which 206 were from the IoT device users, 105 were from data protection/IT professionals, and 30 were from IoT device manufacturers. A combination of cluster analysis; mean, median and mode calculations; weighted average of median values and median split was used to analyse the data. A prioritised list of requirements was then generated, which formed the basis for the development of a scorecard to operationalise the findings.

4. Findings

4.1 Profile of respondents

There were three categories of respondents. 60.4% of all respondents were IoT device users, followed by 30.8% of respondents who were data protection/IT professionals and 8.8% who were IoT device manufacturers. 51.6% of all respondents were from the USA, and 35.2% of respondents were from India. The remainder came from the U.K. (2.93%), Ireland (2.63%), Pakistan (1.76%), Italy (0.88%) and the rest of the world (4.98%). 39.1% of respondents had between 2 to 3 years of experience in using an IoT device, while 29.5% of respondents had between 1 to 2 years of experience in using an IoT device. Of the IoT device manufacturers, 43.3% had between 3 to 5 years of work experience, 23.3% of respondents had 1 to 2 years of work experience, and 20.0% had 6 to 8 years of work experience.

4.2 Reliability of data collection instrument

Table 1 presents the reliability analysis of the data collection instrument. Cronbach's alpha was used to assess the reliability of coefficients for each subscale. Reliability coefficients at 0.7 or above demonstrate high validity of the research instruments [33]. From the table below, we can observe that Cronbach's alpha for transparency was the highest at 0.835, followed by GDPR at 0.767, anonymity at 0.709, explicit consent at 0.618 and simplicity at 0.606. The mean inter-item correlations indicate that the scores fall within the ideal range, i.e., 0.15 to 0.50, thus demonstrating the instrument's reliability.

Table 1 Reliability of data collection instrument

Construct	Number of Items	Overall Median (of Average of Median Responses)	Range or Interquartile Range (from the median score for elements on a 5- Point Likert Scale)	Cronbach's Alpha	Mean inter-item correlation
Anonymity	15	4.193	3.62-4.60	0.709	0.200
Transparency	24	4.282	3.64-4.52	0.835	0.162
Simplicity	15	3.833	3.47-4.21	0.606	0.143
Explicit Consent	12	4.183	3.50-4.67	0.618	0.169
GDPR	24	4.273	3.86-4.62	0.767	0.170

4.3 Summary of results

Overall, the constructs considered to be most important were transparency (median = 4.28), GDPR (median = 4.27), anonymity (median = 4.19), explicit consent (median = 4.18), and simplicity (median = 3.83). These results are similar to those found by Wilkowska [22], who discovered that the most important requirements were general data protection, and the perceived control over private data, and with Kumar [23], who found that user notification, awareness and permission by users were key requirements for the distribution of personal data. For IoT device users, the most important constructs were transparency (median = 4.52), explicit consent (median = 4.51), anonymity (median = 4.46), simplicity (median = 4.30) and GDPR (median = 3.88). For IoT device manufacturers, the most important constructs were explicit consent (median = 4.48), transparency (median = 4.48), anonymity (median = 4.36), simplicity (median = 4.32), and GDPR (median = 4.14). While, data protection/IT professionals were found to place the most importance on explicit consent (median = 4.81), anonymity (median = 4.55), transparency (median = 4.50), GDPR (median = 4.34) and simplicity (median = 4.33).

- Regarding anonymity, data protection/IT professionals agreed undetectability (median = 4.60) was the most important element, similar to IoT device users (median = 4.37) and IoT manufacturers (median = 4.17).
- Regarding transparency, data protection/IT professionals placed the most importance on 'IoT devices should supply information to users about the proposed collection of data' (median = 4.52). In contrast, the IoT device users placed the highest importance on 'IoT devices should supply information to users about the storage of data' (median = 4.48), and IoT device manufacturers put the highest importance on 'IoT devices should clarify to the users how their personal data have been processed' (median = 4.36).
- For simplicity, data protection/IT professionals placed the most importance on 'organisation' (median = 4.21), similar to IoT manufacturers (median = 3.86). On the other hand, IoT device users placed the highest importance on 'data minimisation' (median = 4.07).

- For explicit consent, data protection/IT professionals placed the highest importance on ‘personal data of the users will not be used for other purposes than those mentioned’ (median = 4.67), similar to IoT device manufacturers/professionals (median = 4.00). On the other hand, IoT device users placed the highest importance on ‘personal data will not be shared until the user opts-in’ (median = 4.50).
- For GDPR, data protection/IT professionals placed the highest importance on the ‘right of access’ (median = 4.62). On the other hand, the IoT device users placed the highest importance on the ‘right to erasure’ (median = 4.47). IoT device manufacturers placed the highest importance on the ‘right to restrict processing’ (median = 4.17).

Differences in perception were found within the respondent categories. There were moderate correlations between different IoT device user respondents when asked about the elements under anonymity. Similarly, there were moderate correlations between IoT device users when asked about the elements under transparency. The same was also true for IoT device manufacturers. Moderate correlations were found within the data protection/IT professional respondent category when asked about the elements under simplicity. However, for explicit consent, there were strong correlations within the IoT device manufacturer respondent category when asked about the elements under explicit consent. Similarly, there were strong correlations within the IoT device user and IoT device manufacturer respondent categories when asked about the elements under GDPR. The details of the correlations are provided in the following sections. These correlations have been added here as they were statistically significant in comparison to others. To summarise, moderate correlations were more likely to be found under anonymity, transparency, and simplicity within the respondent categories. Whereas explicit consent and GDPR were more likely to have strong correlations within the respondent categories.

4.4 Anonymity

When ranking elements in descending order of importance, the most popular elements were; a) undetectability (median = 4.380); b) communications content confidentiality (median = 4.340); c) location privacy (median = 4.193). There were no moderate correlations involving data protection/IT professionals. Moreover, there were no strong correlations within respondent categories.

4.5 Transparency

When ranking elements in descending order of importance, the most popular elements were IoT devices should: a) supply information to users about the storage of data (median = 4.430); b) clarify to the users how their personal data have been processed (median = 4.400); c) supply information to users about the proposed collection of data (median = 4.393); d) allow users to access personal data (median = 4.293). In addition, there were moderate correlations within the data protection/IT professional respondent category that agreed transparency was important and: a) IoT devices should supply information to users about the proposed collection of data ($r_s = 0.516$; $p < .001$), b) IoT devices should supply information to users about the processing of data ($r_s = 0.454$; $p < .001$), c) IoT devices should provide an outline of what users’ data have been disclosed under which specific guidelines ($r_s = 0.437$; $p < .001$), and d) IoT devices should provide an outline of what users’ data have been disclosed to what data controller ($r_s = 0.433$; $p < .001$).

4.6 Simplicity

When ranking elements in descending order of importance, the most popular elements were; a) data minimisation (median = 4.030); b) organization (median = 4.023); c) integration (median = 3.833). There were moderate correlations within the data protection/IT professional respondent category that agreed simplicity was important and: a) reduction is important ($r_s = 0.512$; $p < .001$), and b) organisation is important ($r_s = 0.451$; $p < .001$).

4.7 Explicit consent

When ranking elements in descending order of importance, the most popular elements were; personal data of the users: a) will not be used for other purposes than those mentioned (median = 4.390); b) will not be shared until the user opts-in (median = 4.300). There was a strong correlation ($r_s = 0.788$; $p < .001$) within the IoT device manufacturer respondent category that agreed, ‘personal data of the users will not be used for other purposes than those mentioned’ and ‘personal data will not be shared until the user opts-in’. There were moderate correlations within the IoT device user respondent category that agreed explicit consent was important and: a) ‘personal data of the users will not be used for other purposes than those mentioned' ($r_s = 0.493$; $p < .001$), and b) 'personal data will not be shared until the user opts-in' ($r_s = 0.436$; $p < .001$).

4.8 GDPR

When ranking elements in descending order of importance, the most popular elements were – a) right to erasure (median = 4.390); b) right of access (median = 4.360); c) right to restrict processing (median = 4.337); d) right to object (median = 4.333). Strong correlations were found under GDPR within the IoT device user respondent category that agreed: a) right to erasure is important and right to object is important ($r_s = 0.618$; $p < .001$); b) rights in relation to automated decision making and profiling is important and right to data portability is important ($r_s = 0.607$; $p < .001$), and within the IoT device manufacturer respondent category that agreed: a) right to rectification is important and right to erasure is important ($r_s = 0.727$; $p < .001$); b) rights in relation to automated decision making and profiling is important and right to data portability is important ($r_s = 0.795$; $p < .001$); c) right of access is important and rights in relation to automated decision making and profiling is important ($r_s = 0.714$; $p < .001$).

5. Scorecard

Table 2 Critical success factors – scorecard

Rank	Statement	Score*
I	**Transparency - Transparency clarifies and helps users understand the control of their data profile**	
1	Transparency of Data Storage: IoT devices should supply information to users about the storage of data	1 2 3 4 5
2	Transparency of Data Processing (Clarification): IoT devices should clarify to the users how their personal data have been processed	1 2 3 4 5
3	Transparency of Data Acquisition: IoT devices should supply information to users about the proposed collection of data	1 2 3 4 5
4	Transparency of Data Access for the Users: IoT devices should allow users to access their own personal data	1 2 3 4 5
II	**GDPR – General Data Protection Regulation**	
1	Right to Erasure: Personal data should be deleted when there is no compelling reason, especially when the individual withdraws consent	1 2 3 4 5
2	Right of Access: Data should be accessible to the individuals free of charge	1 2 3 4 5
3	Right to Restrict Processing: Individuals have the right to block the processing of their data	1 2 3 4 5
4	Right to Object: Individuals have the right to object to sharing of their personal data	1 2 3 4 5
III	**Anonymity - Defined as the state of being unidentifiable**	
1	Undetectability: Hacker unable to detect information	1 2 3 4 5
2	Communications Content Confidentiality: Information restricted, secret, private and not universal or known to a select few	1 2 3 4 5
3	Location Privacy Ability to control the access of current and past location information	1 2 3 4 5
IV	**Explicit Consent - Explicit consent is the process of informing the users and asking for permission or agreement before collecting their data**	
1	Personal data of the users will not be used for other purposes than those mentioned	1 2 3 4 5
2	Personal data will not be shared until the user opts-in	1 2 3 4 5
V	**Simplicity - The quality or state of being easy to comprehend; basic or uncomplicated in form or design**	
1	Data Minimisation: Minimizing the amount of data collected or requested by an IoT application	1 2 3 4 5
2	Organisation: IoT device privacy's functionality, navigation and structure are arranged logically	1 2 3 4 5
3	Integration: Fragmented components of IoT device privacy are categorised and arranged into a coherent framework	1 2 3 4 5

Scorecards help decision-makers, R&D scientists, and managers improve their product design, development, and manufacturing processes [34]. They help ensure that appropriate conditions for user-centric privacy of IoT devices are in place and that the benchmarked practices are used. Self-assessment scorecards can help reduce the impact of risks by prioritising interventions on control systems [35] and governance [36]. This scorecard was designed to assist decision-makers in assessing their current state and measure their activities against best practices. It will help them determine their company's strengths and areas for improvement to focus and prioritise improvements. Moreover, it can also be used to measure progress over time through comparison [37]. The final design of the scorecard is based on that developed by Cormican [37]. A set of 16 aspects, attributes or characteristics have been selected that R&D professionals, managers and scientists can use to make the privacy of IoT devices very user-centric.

6. Conclusion

While considerable research has been undertaken on several of the study's topics namely, privacy, IoT and user-centricity, there is a dearth of research on developing a user-centric framework for effectively mitigating privacy risks in IoT devices [21, 24, 38]. A comprehensive analysis of the literature was conducted to uncover the constructs and associated factors (e.g., anonymity, transparency, simplicity, explicit consent and GDPR) to effectively mitigate privacy risks in IoT devices. From this analysis, a conceptual framework and a data collection instrument were developed and tested. Additionally, a questionnaire was distributed to key professionals working in the domain. 341 responses were received, out of which 206 were from IoT device users, 105 were from data protection/IT professionals, and 30 were from IoT device manufacturers. The analysis concluded that the most critical constructs are transparency, GDPR, anonymity, explicit consent and simplicity. Among the three main respondent categories, data protection/IT professionals were found to place the most importance on anonymity, simplicity, explicit consent and GDPR, while IoT device users felt transparency was the most important construct in comparison to the other two respondent categories. Simultaneously, IoT device manufacturers were likely to place the highest importance on explicit consent, followed by transparency and simplicity. A scorecard was created, taking the most critical elements into account. The scorecard is intended to assist businesses in comparing their performance to industry standards. Gaps can be identified between existing processes and procedures, and between future designs and policies. The scorecard can be used as a checklist to assess the strengths (for exploitation) and weaknesses (for improvement) of the organisation with regards to user-centricity of privacy of IoT devices. While the research findings can serve as a foundation for addressing privacy threats in IoT devices through a user-centric approach, additional research is required. A limitation of this research was that it was primarily conducted in the USA and India. This can be expanded to other regions to validate the findings globally. Further research on user-centric IoT privacy is also recommended using focus groups and experimental lab-based methodologies, as a difference in perception is highly likely. It is hoped that this scorecard will help decision-makers, R&D scientists, and managers strengthen their existing IoT privacy policies and systems to reflect user-centricity, and replicate the improvements in their product design, development, and manufacturing processes.

References

[1] Tawalbeh, Lo'ai, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider. (2020) "IoT Privacy and Security: Challenges and Solutions." *Applied Sciences* **10** (**12**):1-17.

[2] McCreary, Faith, Alexandra Zafiroglu, and Heather Patterson. (2016) "The contextual complexity of privacy in smart homes and smart buildings." in *International Conference on HCI in Business, Government and Organizations.* Springer: 67–78.

[3] Teltzrow, Maximilian, and Alfred Kobsa. (2004) "Impacts of User Privacy Preferences on Personalized Systems." *Designing Personalized User Experiences in eCommerce. Human-Computer Interaction Series*, Springer, Dordrecht **5**(**1**): 315-332.

[4] Chacko, Anil, and Thaier Hayajneh. (2018) "Security and Privacy Issues with IoT in Healthcare." *EAI Endorsed Transactions on Pervasive Health and Technology* **4** (**14**): 1-7.

[5] Talal, Mohammed, A. A. Zaidan, B. B. Zaidan, A. S. Albahri, A. H. Alamoodi, O. S. Albahri, M. A. Alsalem, C. K Lim, K. L. Tan, W. L. Shir, and K. I. Mohammed. (2019). "Smart Home-based IoT for Real-time and Secure Remote Health Monitoring of Triage and Priority System using Body Sensors: Multi-driven Systematic Review." *Journal of Medical Systems* **43** (**42**)**:** 1-34.

[6] Naeini, Pardis Emami, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. (2020) "Ask the Experts: What Should Be on an IoT Privacy and Security Label?" in *2020 IEEE Symposium on Security and Privacy (SP)*: 771–788.

[7] Bandyopadhyay, Debasis, and Jaydip Sen. (2011) "Internet of Things: Applications and Challenges in Technology and Standardization." *Wireless Personal Communications* **58** (**1**): 49-69.

[8] Phillips, David J. (2004) "Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies." *New Media & Society* **6** (**6**): 691–706.

[9] Kounoudes, Alexia Dini, and Georgia M. Kapitsaki. (2020) "A mapping of IoT user-centric privacy preserving approaches to the GDPR." *Internet of Things* **11** (**1**): 2542-6605.

[10] Notario, Nicolás, Alberto Crespo, Samuel Martín, Jose Del Alamo, Daniel Metayer, Thibaud Antignac, Antonio Kung, Inga Kroener, and David Wright. (2015) "PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology." *2015 IEEE Security and Privacy Workshops*, San Jose, CA: 151-158.

[11] Bertino, Elisa, Shawn Merrill, Alina Nesen, and Christine Utz. (2019) "Redefining Data Transparency: A Multidimensional Approach." *IEEE Digital Object Identifier*, **52** (**1**): 16-26.

[12] Diallo, Mamadou Hassimiou (2018) "User-Centric Security and Privacy Approaches in Untrusted Environments." *UC Irvine PhD Thesis* - Peer Reviewed.

[13] Zheng, Serena, Noah Apthorpe, Marshini Chetty, and Nick Feamster. (2018) "User Perceptions of Smart Home IoT Privacy." *Proceedings of the ACM on Human-Computer Interaction* **2** (**200**): 20.

[14] General Data Protection Regulation. (2016) "Regulation (EU) 2016/679 of the European Parliament and of the Council." *Official Journal of the European Union*: 119/1 - 119/88.

[15] Beresford, Alastair, and Frank Stajano. (2003) "Location Privacy in Pervasive Computing." *IEEE Pervasive Computing* **2** (**1**)*:* 46-55.

[16] Liu, Ling (2007) "From Data Privacy to Location Privacy: Models and Algorithms." *Proceedings of the 33rd International Conference on Very Large Data Bases*, Vienna, Austria, ACM: 1429-1430.

[17] Barhamgi, Mahmoud, Charith Perera, Chirine Ghedira, and Djamal Benslimane. (2018) "User-Centric Privacy Engineering for the Internet of Things." *IEEE Cloud Computing* **5** (**5**): 47-57.

[18] Hossain, Mohammed Alamgir, and Yogesh K. Dwivedi. (2014) "What improves citizens' privacy perceptions toward RFID technology? A cross-country investigation using mixed method approach." *International Journal of Information Management* **34** (**6**): 711–719.

[19] Langheinrich, Marc (2001) "Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems." *Ubicomp 2001: Ubiquitous Computing* – Springer: 273-291.

[20] Lee, Dongwon, Junghoon Moon, Yong Jin Kim, and Mun Y. Yi. (2015) "Antecedents and Consequences of Mobile Phone Usability: Linking Simplicity and Interactivity to Satisfaction, Trust, and Brand Loyalty." *Information & Management* **52** (**3**): 295–304.

[21] Shin, Donghee, and Yujoing Hwang. (2017) "Integrated acceptance and sustainability evaluation of Internet of Medical Things: A dual-level analysis." *Internet Research* **27** (**5**): 1227-1254.

[22] Wilkowska, Wiktoria, Martina Ziefle, and Simon Himmel. (2015) "Perceptions of Personal Privacy in Smart Home Technologies: Do User Assessments Vary Depending on the Research Method?" *HCI 2015 International*, Los Angeles, CA, USA: 529-603.

[23] Kumar, J. Sathish, and Dhiren Patel. (2014) "A Survey on Internet of Things: Security and Privacy Issues." *International Journal of Computer Applications* **90** (**11**): 20-26**.**

[24] Xiao, Li, and Subhasish Dasgupta. (2002) "Measurement of User Satisfaction with Web-Based Information Systems: An Empirical Study." *Washington D.C., Americas Conference on Information Systems*:1149-1155.

[25] Perera, Charith, R. Ranjan, Lizhe Wang, Samee Khan, and Albert Zomaya. (2015) "Privacy of Big Data in the Internet of Things Era." *IEEE IT Professional Magazine* **17** (**3**): 32 - 39.

[26] Nieto, Ana, Ruben Rios, and Javier Lopez. (2017) "Digital Witness and Privacy in IoT: Anonymous Witnessing Approach." *16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2017)*: 642-649.

[27] Weber, Rolf H. (2015) "Internet of things: Privacy issues revisited." *Computer Law & Security Review* **31** (**5**): 618-627.

[28] Al-Rubaie, Mohammad, and J. Morris Chang. (2018) "Privacy Preserving Machine Learning: Threats and Solutions." *IEEE Security and Privacy Magazine* **17** (**2**): 49 - 58.

[29] Hedbom, Hans (2009) "A Survey on Transparency Tools for Enhancing Privacy", in Matyáš V., Fischer-Hübner S., Cvrček D. and Švenda P. (eds) *The Future of Identity in the Information Society. Privacy and Identity 2008. IFIP Advances in Information and Communication Technology*. Berlin, Heidelberg, Springer **298**: 67-82.

[30] Obendorf, Hartmut (2009) "Minimalism: Designing Simplicity." Hamburg, Germany, Springer **1.**

[31] Perera, Charith, Ciaran McCormick, Arosha K. Bandara, Blaine A. Price, and Bashar Nuseibeh. (2016) "Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms." *Proceedings of the 6th International Conference on the Internet of Things*: 83–92.

[32] Jupp, Victor (2006) "The SAGE Dictionary of Social Research Methods." London, Thousand Oaks, New Delhi, SAGE Publications **1.**

[33] Nunnally, Jum, and Ira H. Bernstein. (1994) "Psychometric theory." New York, McGraw-Hill

[34] Cormican, Kathryn, and David O'Sullivan. (2004) "Auditing best practice for effective for product innovation management." *International Journal of Technical Innovation and Entrepreneurship (Technovation)* **24** (**10**): 819-829.

[35] Giudici, Paolo (2008) "Scorecard Models for Operational Risk Management." *University of Pavia*, Pavia: 1-7.

[36] Strenger, Christian (2004) "The Corporate Governance Scorecard: A tool for the implementation of corporate governance", in *Corporate Governance: An International Review*: **12** (**1**): 11-15.

[37] Cormican, Kathryn (2002) "Developing a scorecard for enterprise knowledge management." *8th International Conference on Concurrent Enterprising,* Rome, Italy. 1. Cormican. K and O'Sullivan, D. (2003) "A scorecard for supporting enterprise knowledge management". *Journal of Information and Knowledge Management*, **2** (**3**): 191-201.