Empowering Users' Privacy Rights in the Internet of Things

NELSON VIEIRA*, University of Madeira, Portugal
MARY BARRETO†, University of Madeira, Portugal

Since the advent of ubiquitous computing, the idea of millions of connected devices controlling every aspect of our lives has become a reality. These devices are known as Internet of Things (IoT) devices. Today, we have smart homes, smart cities, smart wearables, smart vehicles, and many more items that connect through a variety of networks and devices. New methods of gathering and processing personal data from users and non-users are made possible by these devices. The majority of end users have little or no control over the data that these systems are gathering about them. This work adopts an holistic approach to the issue by first conducting a literature review, then a survey to find out more about the public's general knowledge, and subsequently, utilizing the information gathered, a system is proposed that provides users information about the nearby devices and how to protect the data they do not want to share with these devices. This system is capable of detecting what kind of devices are nearby, what kind of data is being shared, and how close the devices are to the user.

CCS Concepts: • **Security and privacy → Privacy protections**; **Social aspects of security and privacy**.

Additional Key Words and Phrases: privacy, Internet of Things, ubiquitous computing, privacy assistant

ACM Reference Format:
Nelson Vieira and Mary Barreto. 2023. Empowering Users' Privacy Rights in the Internet of Things. 1, 1 (May 2023), 11 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Privacy as we know it is a somewhat recent concept [63, 41], before the digital age there was barely any notion of privacy for most people. Long seen as a luxury, privacy is still usually regarded as a good to have rather than an essential requirement, even though it is acknowledged as a human right, as present in article 12 of the Universal Declaration of Human Rights [49]: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks". Since handling sensitive information requires discretion, privacy can be defined [21, 56] as the right to control how it is gathered, stored, and used. As a result, businesses must be upfront and honest about the types of data they intend to collect, why they need it, and where and with whom they intend to share it. Users ought to be able to manage how their information is shared.

This definition can cause some confusion with the idea of security [29] and although privacy and security are interconnected, security involves measures taken to safeguard data from risk, threat or danger, it frequently alludes to safety. It is the practice of keeping users' personal information and data safe and preventing unauthorized access to it. The primary contrast between privacy and security is that the former deals with personal information to individuals

*Work done as part of the master's thesis of Nelson Vieira.
†

Authors' addresses: Nelson Vieira, 2080511@student.uma.pt, University of Madeira, Faculty of Exact Sciences and Engineering, Campus Universitário da Penteada, Funchal, Madeira, Portugal, 9020-105; Mary Barreto, mary.barreto@staff.uma.pt, University of Madeira, Faculty of Exact Sciences and Engineering, Campus Universitário da Penteada, Funchal, Madeira, Portugal, 9020-105.

2023. Manuscript submitted to ACM

and how they want their data used and maintained, whilst the latter deals with its protection from possible threats. Security can exist without privacy, but the opposite is not true.

The previous few years have seen an increase in concerns about online privacy [16, 45, 72], particularly in the wake of the cyberattacks by the decentralized hacker group Anonymous, WikiLeaks, and Snowden's release of top-secret papers from the US National Security Agency. When searching for terms like "privacy," "online privacy," or "digital privacy" in Google Scholar, ACM Digital Library, or Science Direct, it can be seen that the number of documents have increased.

The term *Internet of Things* initially originated in the 1990s, and it is possibly related to Mark Weiser's work on ubiquitous computing [67] and the proliferation of devices of all sizes that connect with one another to do various activities, making Weiser's dream a reality. The term *Internet of Things* was coined in 1999 by British technology pioneer Kevin Ashton [9], executive director of the Auto-ID Center at Massachusetts Institute of Technology (MIT), to describe a system in which devices with sensors may be connected to the internet. While making a presentation for Procter & Gamble, Ashton coined the phrase to emphasize the need of connecting Radio-Frequency Identification (RFID) tags.

These devices are employed in a variety of applications, for instance at home [39] with thermostats, refrigerators, microwaves, and so on, to smart vehicles [8], the educational system [17], our clothing and watches [42], and even outer space [3]. IoT resources can include IoT equipment (such as smart home assistants and autonomous cars), IoT services (such as video analytics services linked to smart cameras and indoor location monitoring systems), or IoT apps that track and use information about us. The term "Internet of Things" refers to scenarios in which a variety of objects, gadgets, sensors, and everyday items are linked to the internet and have computational capabilities.

The Internet of Things can be defined as: "An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment" [38].

IoT is one of the fastest growing technologies [28], it is predicted that it will grow into the trillions of devices by 2030 [51], and with this expansion new security vulnerabilities and data gathering dangers appear, the lack of security in these devices makes them ideal targets for privacy violations and inadequate customer disclosure of device capabilities and data practices aggravates privacy and security issues.

Privacy in IoT systems in not seen as a crucial factor in development [5]. Specific standards for privacy options have been imposed by data privacy regulations including the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), but even these regulations have been criticized [46, 24, 22, 26, 12].

2 STATE OF THE ART

This section provides an overview of the recent literature with the themes that were found to be more relevant for this work.

2.1 Privacy Paradox

The use of a variety of digital devices have numerous advantages, but they also bring with them the ubiquity of data capturing equipment, therefore, it is understandable why the majority of online users have serious concerns about the privacy of their personal data. However, the opinions expressed are starkly at odds with the reality, according to Thomson et al. [62] report on the state of privacy, that just one in four European users read the terms and conditions in their entirety prior to making an online purchase or subscribing to a service, 59% admitted to only quickly scanning the terms and conditions before completing a purchase, while 14% admitted to never reading them at all, 30% of the

respondents would even swap their email address to win a reward, or entry into a raffle, while 17% would do so to get an app and 30% would do it for money.

This is what is called a privacy paradox, there have been multiple papers written on this subject [55, 68, 36, 25, 23], some papers attempt a theoretical explanation while others attempt an empirical one. There has been very different interpretations or explanations of this paradox, a few papers [69, 65, 35] apply the theoretical concept of the *homo economicus* [71], which is the representation of people as beings who constantly act in a way that is logical and self-interested, not worrying about morality or ethics, and who do so to the best of their ability, to the context of privacy. Different cognitive biases and heuristics can influence how consumers make decisions, according to several studies on consumer choice behavior [1, 32, 64, 20]. According to several articles [15, 10], this paradox might be explained by the fact that some people have genuinely experienced online privacy assaults and that most privacy views are therefore based on heuristics or secondhand accounts. Taddicken's study [60] argues that peer pressure is the reason people have this contradictory behavior, Norberg et al. [43] explains this paradox by suggesting that while perceived risk affects reported attitudes and behavioral intentions, trust has a direct impact on privacy behavior, while others [20, 33] rely on quantum theory. Brandimarte et al. [11] have explored the idea that when it comes to their data privacy, users have an *illusion of control*.

This paradox has been proven to be vitiated by a number of empirical studies [15, 70, 52, 50], online privacy practices are founded on separate privacy mindsets and so they are not inherently paradoxical.

2.2 Privacy in IoT: Approaches

There have been a number of systematic literature reviews (SLR) [27, 34, 53, 37] and systematic mapping reviews [47, 2] done to study privacy and security issues in IoT.

Based on Ziegeldorf's [74] analysis of the literature, the following are the most prominent privacy concerns in IoT:

(1) The most prominent concern is *identification*, which binds an identifier, such as a name and location, with an individual's identity, this also enables and aggravates other threats;
(2) *Localization and tracking* is the threat of detecting an individual's locations through numerous techniques, such as GPS, internet traffic, or smartphone location. This threat requires *identification* of some kind;
(3) In e-commerce, *profiling* is often used for personalization. Organizations collect information about individuals in order to deduce their interests via association with other profiles and data sources.
(4) *Interaction and presentation* allude to the sharing of private information with an unintended audience while doing so through a public medium. IoT applications often need extensive user interaction, it is expected that users of these systems will obtain information via smart devices in their immediate surroundings and that users will interface with systems in creative, natural ways. However, many of those modes of communication and presentation are already available to the broader public, making them apparent to anybody around. When personal information is transferred between a system and its user, privacy is breached.
(5) *Lifecycle transitions* occur when an IoT device is sold, utilized by its owner and eventually disposed of. There may be an expectation that the object deletes all information, yet smart devices frequently keep massive volumes of data about their own past throughout their entire existence. This might contain personal images and videos, which are not always erased following ownership transfer.
(6) *Inventory attacks* involve unauthorized entry and the acquisition of information about the presence and characteristics of personal things. Malicious users might use inventory data to profile the property and break in.

(7) *Linkage* is the process of connecting disparate systems, when systems are connecting different data sources, there is a higher danger of unauthorized access and data leakage.

2.3 Proposed solutions

This section list seven solutions that emerged from the structured literature review to improve the gap between privacy and security concepts among systems and users.

2.3.1 Creating new ways for user awareness. There has been some work done to determine the users awareness of their actions online regarding their privacy. Skirpan et al. [54] built an interactive theatre experience, this was created to try to prove that a simulated experience with a credible privacy problem may encourage people to take action before actually encountering a catastrophe. The authors had interviews and surveys done after the plays with audience members however they only did interviews halfway through production and only a small fraction of the audience actually participated in this data collection, they also noted that after contacting people months after the interviews that they did not really changed their behaviour regarding their privacy rights.

2.3.2 Legislation. Some papers seek to improve legislation [66, 18] because otherwise, in their view, privacy rights won't be respected if they are not enforceable legally, they defend that without the express agreement of the individual concerned, private information obtained by IoT devices must not be retained or processed in any form, and necessary procedures must be taken to guarantee that the data collected is not that of an unrelated individual. But better protection laws for the user would also create opposition from most companies that want to extract as much private data from their users without (m)any restrictions in order to increase their profit margins.

2.3.3 Privacy through security. Sun et al. [57] design a lightweight communication strategy for a remote-control system, employing two types of Virtual-Spaces to achieve the aim of identity announcement and data exchange. They constructed a prototype system of the scheme and tested it on the Freenet, demonstrating that the method can effectively resist the influence of flow analysis on communication anonymity while preserving communication data security.

2.3.4 Architecture / Framework Proposals. Antunes et al. [7] do a SLR on federated learning in the area of healthcare and make an architecture proposal. The technique known as federated learning allows for the distributed training of machine learning models using remotely hosted datasets without the requirement for data amplification. The fundamental goal of the proposed architecture is to allow healthcare institutions that have access to sensitive medical information to use it in distributed data analysis and machine learning research while ensuring patient confidentiality. Because information transmitted among institutions need confidentiality guarantees for learning model parameters and analysis results, the architecture can adopt a number of ways based on a zero-trust security paradigm [13]. Furthermore, the institutions develop a learning algorithm verification system that can store and disseminate manifestos, as well as engage in distributed analytic procedures that need unanimous agreement from all participants. This study also demonstrates that previous literature implies that homomorphic encryption and differential privacy are effective approaches for preventing data breaches without incurring prohibitively high computing costs.

2.3.5 Other proposals. Zhu et al. [73] present a hybrid sensor system that safeguards privacy while also monitoring parking availability. The authors merged IoT sensing with crowdsensing and enhanced it with privacy-preserving methods. The authors employed physical hazy filters to mask IoT sensors in IoT sensing, and a cryptographic technique based on cryptographic commitments, zero-knowledge proofs, and anonymous credentials in crowdsensing. In addition,

they used crowdsourcing to create a machine learning model for parking recognition in the presence of foggy filters. Their paper included proof-of-concept prototypes such as a Raspberry Pi system and a mobile app, as well as an evaluation study of the machine learning model and the effects of crowdsourcing.

2.3.6 Privacy Assistants. The Carnegie Mellon University CyLab, which is the university's security and privacy research institute, started developing in 2019 an IoT Infrastructure that intended to be free of privacy leaks and software covered by their Secure and Private IoT Initiative 2019, this project would fall under their main research theme of Trust. In this project they started the design of a Personalized Privacy Assistant (PPA) [14], this would involve the use of semi-structured interviews with 17 participants to examine user perceptions of three hypothetical PPA implementations, each of which is potentially more autonomous, while outlining the advantages and disadvantages of each implementation. The authors found that the participants' attitudes regarding the various implementations were generally favorable, although they also voiced worries, which varied depending on the degree of automation. Given the divergent motivations of participants some desired increased control, while others wished to avoid being overtaken by notifications and the lack of agreement regarding the optimal PPA implementation.

After the design phase, the institute implemented a privacy assistant (PA) [19], the authors called it IoT Assistant. Because the predominant approach of "notice and choice" for data privacy protection, the authors decided the PA would also fall into this approach, but because many systems implement notice as a form of consent, without sometimes offering choices to the end user, they also wanted this work to provide a conceptual framework that views user-centered privacy choice as well as a taxonomy for practitioners to use when designing meaningful privacy choices for their systems.

2.4 Main Takeaways

Security and privacy notifications are the two prevalent approaches to offer privacy in IoT systems; other methods, such as legislation or the development or use of a framework that provides privacy, also fall into these two categories. For instance [44, 18, 57], the majority of the literature presupposes that security and privacy are synonymous, hence the majority of the suggested remedies fit under privacy via security. It is challenging to provide privacy notices on the IoT devices themselves because many of these devices lack a screen or have a screen that is too small to give the user the information they need. Proposed solutions that use privacy notices, like [19], are implemented in a way that uses other devices like smartphones that provide the notices themselves. Little guidance is given to designers and developers on how to create a privacy notice design that is adequate and acceptable for their specific system and its features because there are still no standards for implementing privacy notices and best practices are dispersed throughout the literature. Designers might not systematically examine the many options for coming up with suitable privacy notifications because they are ignorant of them.

Aleisa and Renaud [4] also identify security and privacy awareness as potential solutions to privacy issues in IoT, but also identify data minimization, hitchhiking and introspection. Data minimization entails limiting the collecting of personal information to what is absolutely central and retaining the data just for as long as is required to satisfy the goal of the technology's services [58]. Hitchhiking [61] is a method of protecting the privacy of users who divulge their location, applications regard locations as the object of their attention. The fidelity tradeoff is removed as it is not important to know who is in a certain location. The introspection [30] method examines VM actions to adequately safeguard users' private information. Every VM's CPU status, memory contents, network information provided by the

hypervisor, and any malicious software that may be present on the VM are all collected and analyzed. The privacy of consumers is jeopardized if an IoT device loses integrity due to a hostile assault.

3 PRIVACY CHALLENGES

According to Qu et al. [48], several significant barriers remain, including the lack of a theoretical foundation, the trade-off optimization between privacy and data value, and system isomerism over-complexity. Because there are no mathematical foundations for IoT structure design, IoT system designs are planned and executed using empirical approaches, which have limitations in IoT development. Scientific theory and quantitative analysis must enable trade-off optimization, yet, there are multiple parties with diverse characteristics and requirements, making this optimization highly challenging. A plethora of standards and protocols add to the unneeded complexity of system isomerism. Ensuring effective IoT applications while wasting as little resources as feasible implies less resources available for privacy protection, however, lightweight privacy protection cannot fulfill all of the criteria, and attackers can exploit structural information to launch several concurrent attacks.

4 METHODOLOGY

The overall work will be comprised of two phases which will be described in the following paragraphs. Phase one mainly described throughout this paper, focuses on collecting the state of the art in terms of the most relevant topics, from which main privacy concepts were selected to be explored in the stage 1 of Phase 2 with the preparation of a questionnaire to collect user perceptions regarding privacy and topics collected in the systematic literature review. The second stage of Phase 2 consists in developing an application, partially based on the information generated by the survey, that can identify what sort of devices are around, what kind of data is gathered by these devices, present privacy options to the user when available, and what can be done to prevent undesirable data from being collected.

The Phase 1 Systematic Literature Review gathered the most relevant papers discussing methodologies and techniques for the protection of users' privacy data with special focus on IoT systems. For this SLR, this paper considered focusing only on papers from the last 12 years, from 2010 until 2022, since papers before then become out of date with the evolution of technology. In this SLR, it was reviewed 54 papers published in top computer science, security, privacy and software engineering outlets.

This paper followed Keshav's three-pass approach [31] when choosing which papers to read fully and which ones to ignore, first the title would be read, then the abstract, the introduction and conclusion and briefly skim the rest of the paper and then decide if it was worth reading any further, the focal point in this phase was answering the following question: does the paper present a new methodology or interesting angle to tackle users' privacy concerns? Only then the document would be read in its entirety while ignoring any tables, figures, images or graphs. If the paper failed to present any interesting idea, approach, or technique it would be discarded, but if not, it would be read carefully from the beginning again in order to fully understand what it presents. Having collected the major findings, this work then aims to conduct a throughout study split in several stages and around the specific research questions which will be explored in each phase. For that matter, the research questions listed are:

Phase 1:

RQ1: What approaches are being considered for privacy issues in IoT in the currently available literature?

RQ2: What are user perceptions on online privacy?

Phase 2:
RQ3: How to empower users to protect their privacy rights?
RQ4: What issues are prevalent in IoT that make it difficult to address privacy and security problems?

The second phase will be evaluated on two stages, the first one consists on doing a study on people's general privacy concerns, while using and interacting with IoT devices. This study will abide on preparing a questionnaire to assess general user's knowledge on privacy concepts, their habits and concerns, their understanding of privacy rights, and what they do to safeguard those rights. The goal of this study is to both understand the privacy paradox and collect data on their proposal to address privacy issues with regard to IoT devices.

4.1 Stage 1: User perceptions

This study aims to understand people's perception of IoT and their privacy practices online. It also serves to demystify the privacy paradox and also to help provide a solution to the privacy issue in IoT. The questionnaire consists of 92 questions divided into 7 sections to access users' knowledge, it follows a kind of narrative, the first section being general privacy questions then about the predisposition to data sharing, to concerns with privacy then about daily digital routines, then about profile identification, and then about IoT general knowledge before a section about non-identifiable demographic data. The scale that is used in the questionnaire is based on the work of Philip K. Masur [40]. Great care is taken when it comes to this survey's data collection, in order to not identify any individual or group of individuals, for instance, when it comes to differential privacy, any data that might identify someone will not be disclosed, even though the data might suffer from some inaccuracy because of this.

This survey was partially based in a study done in the Philippines by the government in the context of their privacy act of 2012 [59], this was the second survey done on the country's population. It was also inspired by Alves's master's thesis [6], which was about citizen's perception about privacy in the wake of GDPR.

This survey was done through the internet, it was created in Google Forms, this way it is guaranteed to reach the most people possible, besides Google Forms itself, it will be used other online venues for distribution and even printing.

4.2 Stage 2: Study in Context, an Application

The proposed application in this work informs users about nearby IoT devices, including the data these devices collect and the privacy settings that are available. Because mobile phones are the most common device that people carry with them everywhere they go and because this application will use georeferencing to display the locations of IoT devices, it will be designed for mobile devices. Giving consumers another choice to protect their personal information is the major goal of this program. The application will display the geolocation of IoT devices, their type, and the kind of data they are collecting. In the initial iterations of this application, it was proposed that the application itself would detect the devices and would categorize what type of device it was and what type of data it was collecting, but it was discovered that this approach was too complex and so it was not feasible to do with the limitations of this paper. Instead, users will be responsible for doing this. The application will be created with Flutter; alternative options include React Native or a progressive web application. However, Flutter uses just-in-time and ahead-of-time compilation with Dart as its primary programming language, while React Native makes use of a bridge to translate Javascript into native components for Android or iOS. Flutter was chosen as the framework for this application since it performs better.

5 CURRENT STAGE OF THE WORK

The study's findings, based on 42 responses, show that everyone agrees that privacy is important to them. Some respondents know they shouldn't share their personal information with third parties they don't trust, but the majority of participants believe that privacy and security are the same thing. Most participants also do not read privacy notices but accept them in order to access the information they need to access. The majority of respondents use their devices primarily to access social media.

The following months will involve the refinement and release of the application along with usability tests, also a more thorough synthesis of the study will be conducted. Because of the exploratory nature of this work the proposals might suffer alterations.

6 FUTURE WORK

Although there are existing hardware solutions that can detect some devices on particular networks, like ZigBee or Bluetooth LE, namely IoT sniffers and there exist some georeferencing applications that try to pinpoint certain IoT devices, there is still a need for some kind of device or framework that is network agnostic and can detect where the devices are located and what kind of data the IoT devices that are around it are collecting. This gadget should also be capable of informing users about the privacy notices of the devices and what can the users do to safeguard their personal data. The IoT sniffers that are available are primarily used in the detection of problems in the communication of devices in the network or to solve problems of interoperability between different IoT networks. There are many obstacles that impede the creation of such a device and the fact that it still does not exist anything like it may be related ton either there iss not enough interest from users or researchers to focus on such an endeavour or the complexity of such a task is greater than the rewards.

7 CONCLUSION

The aim of this work is an exploratory investigation of privacy in IoT systems. It suggests a survey to find out more about users' understanding of this topic and an application that attempts to increase users' awareness of their surroundings, the IoT devices that live in it, and how they may react appropriately.

The work done on this project should hopefully help researchers further, and the application that is being developed should be able to provide more visibility, allowing users to learn about the data being collected and how they can modify their behavior or respond more effectively to protect their privacy rights.

REFERENCES

[1] Alessandro Acquisti, Stefanos Gritzalis, Costos Lambrinoudakis, and Sabrina di Vimercati. 2007. What can behavioral economics teach us about privacy? In *Digital privacy*. Auerbach Publications, 385–400.

[2] Bestoun S Ahmed, Miroslav Bures, Karel Frajtak, and Tomas Cerny. 2019. Aspects of quality in internet of things (iot) solutions: a systematic mapping study. *IEEE Access*, 7, 13758–13780.

[3] Ian F. Akyildiz and Ahan Kak. 2019. The internet of space things/cubesats. *IEEE Network*, 33, 5, 212–218. DOI: 10.1109/MNET.2019.1800445.

[4] Noura Aleisa and Karen Renaud. 2016. Privacy of the internet of things: a systematic literature review (extended discussion). *arXiv preprint arXiv:1611.03340*.

[5] Nada Alhirabi, Omer Rana, and Charith Perera. 2021. Security and privacy requirements for the internet of things: a survey. *ACM Transactions on Internet of Things*, 2, 1, 1–37.

[6] Maria Helena da Silva Alves. 2021. *GDPR in Portugal: Analysis of citizens' perception about privacy*. Master's thesis. Universidade Nova de Lisboa, Lisboa, Portugal, Lisbon, PT.

[7] Rodolfo Stoffel Antunes, Cristiano André da Costa, Arne Küderle, Imrana Abdullahi Yari, and Björn Eskofier. 2022. Federated learning for healthcare: systematic review and architecture proposal. *ACM Trans. Intell. Syst. Technol.*, 13, 4, Article 54, (May 2022), 23 pages. DOI: 10.1145/3501813.

[8] Fabio Arena, Giovanni Pau, and Alessandro Severino. 2020. An overview on the current status and future perspectives of smart cars. *Infrastructures*, 5, 7, 53.

[9] Kevin Ashton. 2009. That "internet of things" thing. Accessed: 2022-11-05. Retrieved Nov. 5, 2022 from https://www.rfidjournal.com/that-internet-of-things-thing.

[10] Young Min Baek. 2014. Solving the privacy paradox: a counter-argument experimental approach. *Computers in human behavior*, 38, 33–42.

[11] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced confidences: privacy and the control paradox. *Social psychological and personality science*, 4, 3, 340–347.

[12] Diane Y Byun. 2019. Privacy or protection: the catch-22 of the ccpa. *Loy. Consumer L. Rev.*, 32, 246.

[13] Baozhan Chen, Siyuan Qiao, Jie Zhao, Dongqing Liu, Xiaobing Shi, Minzhao Lyu, Haotian Chen, Huimin Lu, and Yunkai Zhai. 2021. A security awareness and protection system for 5g smart healthcare based on zero-trust architecture. *IEEE Internet of Things Journal*, 8, 13, 10248–10263. DOI: 10.1109/JIOT.2020.3041042.

[14] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2020. Informing the design of a personalized privacy assistant for the internet of things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (CHI '20). Association for Computing Machinery, Honolulu, HI, USA, 1–13. ISBN: 9781450367080. DOI: 10.1145/3313831.3376389.

[15] Tobias Dienlin and Sabine Trepte. 2015. Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology*, 45, 3, 285–297.

[16] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring how privacy and security factor into iot device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–12.

[17] Mostafa Al-Emran, Sohail Iqbal Malik, and Mohammed N Al-Kabi. 2020. A survey of internet of things (iot) in education: opportunities and challenges. *Toward social internet of things (SIoT): enabling technologies, architectures and applications*, 197–209.

[18] Nicola Fabiano. 2017. Internet of things and blockchain: legal issues and privacy. the challenge for a privacy standard. In *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 727–734. DOI: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.112.

[19] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A design space for privacy choices: towards meaningful privacy control in the internet of things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (CHI '21) Article 64. Association for Computing Machinery, Yokohama, Japan, 16 pages. ISBN: 9781450380966. DOI: 10.1145/3411764.3445148.

[20] Christian Flender and Günter Müller. 2012. Type indeterminacy in privacy decisions: the privacy paradox revisited. In *International Symposium on Quantum Interaction*. Springer, 148–159.

[21] International Association for Privacy Professionals. 2021. What does privacy mean? Accessed: 2022-11-04. Retrieved Nov. 4, 2022 from https://iapp.org/about/what-is-privacy/.

[22] Giulia Gentile and Orla Lynskey. 2022. Deficient by design? the transnational enforcement of the gdpr. *International & Comparative Law Quarterly*, 71, 4, 799–830.

[23] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: a systematic review of literature investigating privacy attitude and behavior. *Computers & security*, 77, 226–261.

[24] Alexander Gladis, Nicole Janine Hartwich, and Oliver Salge. 2022. Weaponizing the gdpr: how flawed implementations turn the gold standard for privacy laws into fool's gold.

[25] David Goad, Andrew T Collins, and Uri Gal. 2021. Privacy and the internet of things- an experiment in discrete choice. *Information & Management*, 58, 2, 103292.

[26] Ben Green. 2022. The flaws of policies requiring human oversight of government algorithms. *Computer Law & Security Review*, 45, 105681.

[27] Sanonda Gupta and Sepideh Ghanavati. 2022. Privacy in the internet of things: where do we stand? a systematic literature review, (May 2022). DOI: 10.36227/techrxiv.19874329.v1.

[28] Mohammad Hasan. 2022. State of iot 2022: number of connected iot devices growing 18 to 14.4 billion globally. Accessed: 2022-11-04. Retrieved Nov. 4, 2022 from https://iot-analytics.com/number-connected-iot-devices/.

[29] HIV.gov. 2018. The difference between security and privacy and why it matters to your program. Accessed: 2022-11-04. Retrieved Nov. 4, 2022 from https://www.hiv.gov/blog/difference-between-security-and-privacy-and-why-it-matters-your-program.

[30] Chulhyun Kang, Fizza Abbas, and Heekuck Oh. 2015. Protection scheme for iot devices using introspection. In *2015 6th International Conference on the Network of the Future (NOF)*. IEEE, 1–5.

[31] S. Keshav. 2007. How to read a paper. *SIGCOMM Comput. Commun. Rev.*, 37, 3, (July 2007), 83–84. DOI: 10.1145/1273445.1273458.

[32] Bart P Knijnenburg, Alfred Kobsa, and Hongxia Jin. 2013. Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies*, 71, 12, 1144–1162.

[33] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. *Computers & security*, 64, 122–134.

[34] Patrick Kühtreiber, Viktoriya Pak, and Delphine Reinhardt. 2022. A survey on solutions to support developers in privacy-preserving iot development. *Pervasive and Mobile Computing*, 85, 101656. DOI: https://doi.org/10.1016/j.pmcj.2022.101656.

[35] Namyeon Lee and Ohbyung Kwon. 2015. A privacy-aware feature selection method for solving the personalization–privacy paradox in mobile wellness healthcare services. *Expert systems with applications*, 42, 5, 2764–2771.

[36] Ae-Ri Lee. 2021. Investigating the personalization–privacy paradox in internet of things (iot) based on dual-factor theory: moderating effects of type of iot service and user value. *Sustainability*, 13, 19, 10679.

[37] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. 2017. A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, 4, 5, 1125–1142. DOI: 10.1109/JIOT.2017.2683200.

[38] Somayya Madakam, Vihar Lake, Vihar Lake, Vihar Lake, et al. 2015. Internet of things (iot): a literature review. *Journal of Computer and Communications*, 3, 05, 164.

[39] Davit Marikyan, Savvas Papagiannidis, and Eleftherios Alamanos. 2019. A systematic review of the smart home literature: a user perspective. *Technological Forecasting and Social Change*, 138, 139–154.

[40] Philipp K Masur. 2018. *Situational privacy and self-disclosure: Communication processes in online environments*. Springer.

[41] Barrington Moore. 2017. *Privacy: Studies in social and cultural history*. Routledge.

[42] Naghmeh Niknejad, Waidah Binti Ismail, Abbas Mardani, Huchang Liao, and Imran Ghani. 2020. A comprehensive overview of smart wearables: the state of the art literature, recent advances, and future challenges. *Engineering Applications of Artificial Intelligence*, 90, 103529.

[43] Patricia A Norberg, Daniel R Horne, and David A Horne. 2007. The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of consumer affairs*, 41, 1, 100–126.

[44] Anthony Opara, Haan Johng, Tom Hill, and Lawrence Chung. 2022. A framework for representing internet of things security and privacy policies and detecting potential problems. In *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing*, 198–201.

[45] Yong Jin Park. 2022. Personal data concern, behavioral puzzle and uncertainty in the age of digital surveillance. *Telematics and Informatics*, 66, 101748.

[46] David Peloquin, Michael DiMaio, Barbara Bierer, and Mark Barnes. 2020. Disruptive and avoidable: gdpr challenges to secondary research uses of data. *European Journal of Human Genetics*, 28, 6, 697–705.

[47] Jari Porras, Jouni Pänkäläinen, Antti Knutas, and Jayden Khakurel. 2018. Security in the internet of things-a systematic mapping study.

[48] Youyang Qu, Shui Yu, Wanlei Zhou, Sancheng Peng, Guojun Wang, and Ke Xiao. 2018. Privacy of things: emerging challenges and opportunities in wireless internet of things. *IEEE Wireless Communications*, 25, 6, 91–97. DOI: 10.1109/MWC.2017.1800112.

[49] Eleanor Roosevelt, P. C. Chang, Charles Malik, William Roy Hodgson, Hernán Santa Cruz, René Cassin, Alexander E. Bogomolov, Charles Dukes 1st Baron Dukeston, and John Peters Humphrey. 1948. Universal declaration of human rights. Accessed: 2022-11-05. Retrieved Nov. 5, 2022 from https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[50] Shruti Sannon, Natalya N Bazarova, and Dan Cosley. 2018. Privacy lies: understanding how, when, and why people lie to protect their privacy in multiple online contexts. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–13.

[51] Shadi Al-Sarawi, Mohammed Anbar, Rosni Abdullah, and Ahmad B. Al Hawari. 2020. Internet of things market analysis forecasts, 2020-2030. In *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 449–453. DOI: 10.1109/WorldS450073.2020.9210375.

[52] Kathy S. Schwaig, Albert H. Segars, Varun Grover, and Kirk D. Fiedler. 2013. A model of consumers' perceptions of the invasion of information privacy. *Information & Management*, 50, 1, 1–12. DOI: https://doi.org/10.1016/j.im.2012.11.002.

[53] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. 2015. Security, privacy and trust in internet of things: the road ahead. *Computer networks*, 76, 146–164.

[54] Michael Skirpan, Maggie Oates, Daragh Byrne, Robert Cunningham, and Lorrie Faith Cranor. 2022. Is a privacy crisis experienced, a privacy crisis avoided? *Commun. ACM*, 65, 3, (Feb. 2022), 26–29. DOI: 10.1145/3512325.

[55] Daniel J Solove. 2021. The myth of the privacy paradox. *Geo. Wash. L. Rev.*, 89, 1.

[56] Sarah Spiekermann and Lorrie Faith Cranor. 2009. Engineering privacy. *IEEE Transactions on Software Engineering*, 35, 1, 67–82. DOI: 10.1109/TSE.2008.88.

[57] Qindong Sun, Kai Lin, Chengxiang Si, Yanyue Xu, Shancang Li, and Prosanta Gope. 2022. A secure and anonymous communicate scheme over the internet of things. *ACM Trans. Sen. Netw.*, 18, 3, Article 40, (Apr. 2022), 21 pages. DOI: 10.1145/3508392.

[58] E. D. P. Supervisor. 1995. Directive 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union. (1995).

[59] Philippine Survey and Research Center. 2022. Conduct of privacy survey. Accessed: 2022-12-19. https://www.privacy.gov.ph/wp-content/uploads/2022/01/CONDUCT-OF-PRIVACY-SURVEY-Final-Report-v3.pdf.

[60] Monika Taddicken. 2014. The "privacy paradox" in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of computer-mediated communication*, 19, 2, 248–273.

[61] Karen P Tang, Pedram Keyani, James Fogarty, and Jason I Hong. 2006. Putting people in their place: an anonymous and privacy-sensitive approach to collecting sensed data in location-based applications. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, 93–102.

[62] Darren Thomson, Dr Peter Cochrane, Ilias Chantzos, Philip Carter, Siân John, Professor Udo Helmbrecht, and Stewart Room. 2015. State of Privacy Report 2015. Symantec.

[63] David Vincent. 2016. *Privacy: A short history*. John Wiley & Sons.

[64] Robin Wakefield. 2013. The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems*, 22, 2, 157–174.

[65] Jeffrey Warshaw, Tara Matthews, Steve Whittaker, Chris Kau, Mateo Bengualid, and Barton A Smith. 2015. Can an algorithm know the" real you"? understanding people's reactions to hyper-personal analytics systems. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, 797–806.

[66] Rolf H. Weber. 2015. Internet of things: privacy issues revisited. *Computer Law & Security Review*, 31, 5, 618–627. DOI: https://doi.org/10.1016/j.clsr.2015.07.002.

[67] Mark Weiser. 1991. The computer for the 21 st century. *Scientific american*, 265, 3, 94–105.

[68] Meredydd Williams, Jason R. C. Nurse, and Sadie Creese. 2017. Privacy is the boring bit: user perceptions and behaviour in the internet-of-things. In *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, 181–18109. DOI: 10.1109/PST.2017.00029.

[69] Dave Wilson and Joseph S Valacich. 2012. Unpacking the privacy paradox: irrational decision-making within the privacy calculus.

[70] Wenjing Xie and Kavita Karan. 2019. Consumers' privacy concern and privacy protection on social network sites in the era of big data: empirical evidence from college students. *Journal of Interactive Advertising*, 19, 3, 187–201.

[71] Paul J Zak. 2008. *Moral markets: The critical role of values in the economy*. Princeton University Press.

[72] Nan Andy Zhang, Chong Alex Wang, Elena Karahanna, and Yan Xu. 2022. Peer privacy concern: conceptualization and measurement. *MIS Quarterly*, 46, 1.

[73] Hanwei Zhu, Sid Chi-Kin Chau, Gladhi Guarddin, and Weifa Liang. 2022. Integrating iot-sensing and crowdsensing with privacy: privacy-preserving hybrid sensing for smart cities. *ACM Trans. Internet Things*, 3, 4, Article 31, (Sept. 2022), 30 pages. DOI: 10.1145/3549550.

[74] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. 2014. Privacy in the internet of things: threats and challenges. *Security and Communication Networks*, 7, 12, 2728–2742.