Capacitando os utilizadores para os seus direitos de privacidade na *Internet of Things*

Nelson Vieira
Faculdade de Ciências Exatas e da Engenharia
Universidade da Madeira
Funchal, Portugal
2080511@student.uma.pt

Mary Barreto (Orientadora)
Faculdade de Ciências Exatas e da Engenharia
Universidade da Madeira
Funchal, Portugal
mary.barreto@staff.uma.pt

***Abstract*—Os dispositivos da *Internet of Things* (IoT) estão em toda parte, desde o nascimento da computação ubíqua que a vida quotidiana humana é imaginada contendo milhões de dispositivos que controlam todos os aspectos de nossas vidas. Hoje em dia temos carros inteligentes, casas inteligentes, cidades inteligentes, *wearables* entre outras coisas que usam vários tipos de dispositivos e vários tipos de redes para comunicarem. Estes dispositivos criam novas formas de recolher e processar dados pessoais de utilizadores e não utilizadores. A maioria dos utilizadores finais nem sabem ou têm pouco controlo sobre as informações que estão a ser recolhidas por estes sistemas. Este trabalho faz uma abordagem holística deste problema, fazendo primeiro uma revisão da literatura, depois realizando um questionário para saber mais sobre o conhecimento geral do público e, finalmente, com base nas informações recolhidas, é proposto um sistema que fornece aos utilizadores informações sobre o dispositivos que estão próximos e como proteger os dados que não desejam compartilhar com estes dispositivos, este sistema é capaz de detectar que tipo de dispositivos estão próximos, que tipo de dados são recolhidos por estes dispositivos, mostrar opções de privacidade ao utilizador quando é possível fazê-lo e o que pode ser feito para evitar que dados indesejados sejam recolhidos.**

***Index Terms*—privacidade, Internet of Things, computação ubíqua, assistente de privacidade**

I. Introdução

A privacidade como a conhecemos é um conceito relativamente recente [1], [2], antes da era digital quase não havia a noção de privacidade para a maioria das pessoas. Durante muitos séculos, a maioria das pessoas residia em pequenas comunidades onde estavam continuamente envolvidas na vida umas das outras. Ainda mais recente é a ideia de que a privacidade é um componente crucial da segurança pessoal, em contraste com a inegável necessidade da segurança pública, incluindo a exigência de muros vigiados e portas fechadas. Há muito vista como um luxo, a privacidade ainda costuma ser vista como um bem de se ter e não como um requisito essencial, embora seja reconhecida como um direito humano, conforme consta no artigo 12 da Declaração Universal dos Direitos Humanos [3]: “Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei”. A privacidade pode ser definida [4], [5] como o direito de governar como as informações e dados pessoais são recolhidos, armazenados e usados, frequentemente envolve o uso de informações confidenciais com cuidado e, como tal, as organizações devem ser abertas e honestas sobre o tipo de dados que planeiam recolher, por que precisam deles e onde e com quem planeiam partilhá-los. Os utilizadores devem ter o direito de controlar como as suas informações são partilhadas.

Esta definição pode causar alguma confusão com a ideia de segurança [6] e embora a privacidade e a segurança estejam interligadas, a segurança envolve medidas tomadas para salvaguardar os dados de risco, ameaça ou perigo, frequentemente alude à protecção. É a prática de manter a informação pessoal dos utilizadores e dados seguros e prevenindo o acesso não autorizado aos mesmos. O principal contraste entre privacidade e segurança é que o primeiro trata de informações pessoais aos indivíduos e como querem que os seus dados sejam utilizados e mantidos, enquanto este último trata da sua protecção contra possíveis ameaças. A segurança pode existem sem privacidade, mas o oposto não é verdade. Para a gestão de dados sensíveis e pessoais, privacidade e segurança informática são igualmente cruciais. Os utilizadores devem estar cientes dos procedimentos internos relativos à recolha, processamento, retenção, e partilha de informação pessoal.

As preocupações com a privacidade digital têm vindo a crescer [7]–[9] nos últimos anos, especialmente depois dos ataques informáticos do grupo descentralizado de hackers *Anonymous*, *WikiLeaks* e da divulgação de documentos ultra secretos da Agência de Segurança Nacional dos Estados Unidos por Snowden. Estas preocupações podem ser notadas com o aumento da literatura escrita sobre o assunto, ao procurar termos como “privacy”, “online privacy”, “digital privacy” no Google Scholar, ACM Digital Library ou Science Direct, pode ser visto que, nos últimos 5 anos, retornam cerca de 5000000, 650000 e 80000 documentos, respectivamente, incluindo artigos, livros, artigos de conferência, etc.

A maioria da investigação tem-se concentrado na *web*, enquanto a privacidade nos sistemas IoT não tem sido tão explorada. Uma vez que os dispositivos IoT estão a tornar-se mais predominantes, surgem novos métodos de comunicação, recolha, e análise de dados. Porque já existe uma quantidade substancial de investigação centrada em privacidade na *web* em vez de privacidade na IoT, é um terreno muito mais fértil para explorar a questão da privacidade no contexto da IoT.

Internet of Things é um termo que surgiu pela primeira vez nos anos 90, e pode estar ligado ao artigo de Mark Weiser sobre a computação ubíqua [10] e o crescimento de dispositivos de todos os tamanhos que comunicam entre si para realizar várias tarefas, tornando o sonho de Weiser uma realidade. A primeira utilização do termo *Internet of Things* foi em 1999 pelo pioneiro da tecnologia britânica Kevin Ashton [11], director executivo do Auto-ID Center no Massachusetts Institute of Technology (MIT), para descrever um sistema em que os itens podem ser ligados à Internet por sensores. Ele inventou a frase enquanto fazia uma apresentação para a Procter & Gamble para realçar o valor de ligar etiquetas de Identificação por Radiofrequência (RFID) utilizadas em cadeias de fornecimento corporativas à Internet, a fim de contar e rastrear bens sem a necessidade de assistência humana. Estes dispositivos são utilizados em várias aplicações, começando em casa [12] com termostatos, frigoríficos, microondas, etc., passando para carros inteligentes [13], o sistema educacional [14], as nossas roupas e os nossos relógios [15] e mesmo para o espaço exterior [16]. Os recursos da IdC podem incluir equipamento IoT (como assistentes domésticos inteligentes e veículos autónomos), serviços IoT (como serviços de análise de vídeo ligados a câmaras inteligentes e sistemas de localização de posição interior), ou aplicações IoT (como aplicações remotas de televisão inteligente) que localizam e utilizam informação sobre nós. A Internet of Things é agora amplamente utilizada para descrever situações em que uma gama de objectos, gadgets, sensores, e itens comuns estão ligados à Internet e têm capacidades computacionais.

A ideia de utilizar computadores e redes para monitorizar e gerir dispositivos não é nova, apesar do termo *Internet of Things* ser relativamente recente. As melhorias da tecnologia sem fios nos anos 90 permitiram a adopção generalizada de soluções máquina-a-máquina (M2M) corporativas e industriais para monitorização e operação de equipamentos. Muitas das primeiras soluções M2M, por outro lado, baseavam-se em redes proprietárias ou em normas específicas da indústria, em vez de normas da Internet. Ligar outros dispositivos que não computadores à Internet não é um conceito novo. Uma máquina de Coca-Cola no Departamento de Informática da Carnegie Mellon University [17] foi o primeiro dispositivo ubíquo a ser ligado à Internet. O sistema, criado em 1982, observou remotamente as luzes de esgotamento de stock nos botões de pressão da máquina de venda automática e difundiu o estado de cada fila da máquina de venda automática na rede para que pudesse ser acedido utilizando o protocolo Nome/Dedo através de um terminal. Em 1990, uma torradeira que podia ser ligada e desligada através da Internet, criada por John Romkey [18], foi demonstrada no programa Interop Internet Networking.

A *Internet of Things* pode ser definida como: "Uma rede aberta e abrangente de objectos inteligentes que têm a capacidade de se auto-organizarem, partilhar informação, dados e recursos, reagindo e agindo face a situações e mudanças in the environment" [19].

IoT é uma das tecnologias de crescimento mais rápido [20], prevê-se que cresça para os triliões de dispositivos até 2030 [21], e com esta expansão surgem novas vulnerabilidades de segurança e perigos de recolha de dados, a falta de segurança nestes dispositivos torna-os alvos ideais para violações da privacidade e divulgação inadequada das capacidades dos dispositivos por parte dos clientes e práticas de dados agrava as questões de privacidade e segurança.

A privacidade nos sistemas IoT não é vista como um factor crucial no desenvolvimento [22]. Normas específicas para opções de privacidade foram impostas pela privacidade dos dados regulamentos incluindo o Regulamento Geral de Protecção de Dados (GDPR) e California Consumer Privacy Act (CCPA), mas mesmo estes regulamentos têm foi criticado [23]–[27].

II. ESTADO DA ARTE

Esta secção fornece uma visão geral da literatura recente com os temas que foram consideradas mais relevantes para este trabalho.

A. *Paradoxo da Privacidade*

A utilização de uma variedade de dispositivos digitais tem inúmeras vantagens, mas eles trazem também consigo a ubiquidade do equipamento de captura de dados, é compreensível que a maioria dos utilizadores em linha tenha sérias preocupações sobre a privacidade dos seus dados pessoais. No entanto, as opiniões expressas estão em total desacordo com a realidade, segundo Thomson et al. [28] relatório sobre o estado da privacidade, que apenas um em cada quatro utilizadores europeus lê os termos e condições na sua totalidade antes de efectuar uma compra on-line ou subscrever um serviço, 59% admitiram apenas a digitalização rápida do termos e condições antes de concluir uma compra, enquanto 14% admitiu a nunca os lendo de todo, 30% dos inquiridos até trocariam os seus endereço de e-mail para ganhar uma recompensa, ou entrada numa rifa, enquanto 17% faria por isso, para obter uma aplicação e 30% fá-lo-ia por dinheiro.

This is what is called a privacy paradox, there have been multiple papers written on this subject [29]–[33], 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 [34]–[36] apply the theoretical concept of the *homo economicus* [37], 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 [38]–[41]. According to several articles [42], [43], 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 [44] argues that peer pressure is the reason people have this contradictory behavior, Norberg et al. [45] 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 [41], [46] rely on quantum theory. Brandimarte et al. [47] 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 [42], [48]–[50], online privacy practices are founded on separate privacy mindsets and so they are not inherently paradoxical.

B. Privacidade em IoT: Abordagens

There have been a number of systematic literature reviews (SLR) [51]–[54] and systematic mapping reviews [55], [56] done to study privacy and security issues in IoT.

In Gupta and Ghanavati's [51] SLR, the authors review papers with methodologies and techniques that identify privacy risks or notify users about these risks. They divide the literature into the following categories: 'Ontological Modeling and Semantic-based Approaches', 'Data-Driven Approaches', 'Source Code Analysis-based Approaches', 'User Studies and Survey-based Approaches', 'Blockchain-based Approaches' and 'Architectural and Framework-based Approaches'. They then examine current literature on these three prerequisites. The findings show that: most works concentrate on single IoT devices when addressing privacy threats; When analyzing privacy issues, key privacy factors such as data reduction and data aggregation are overlooked; existing studies ignored the sensitivity of the obtained information; most useful studies did not include a diverse range of users when assessing privacy problems; no work has been done to discover compliance difficulties between an IoT application and different privacy rules; and current research does not place a premium on providing consumers with real-time privacy notices. However, this SLR has the following limitations: the authors only chose articles and not thesis or books and from the selected papers, only the ones written in english were considered.

Kühtreiber et al. [52] evaluate the frameworks and tools established for developers, specifically in the case of IoT, and find that current solutions are difficult to use, only successful in limited scenarios, and insufficient to handle the privacy problems inherent in IoT development. This study lacks a comprehensive gap review of the chosen literature, along with research questions establishing the significance of the articles chosen.

Sicari et al. [53] examine current research and ongoing activities that focus on IoT privacy and security solutions. The authors start by describing the requirements for IoT privacy and security, such as access control, confidentiality, and authentication. The authors then conduct a literature study in connection to these three needs. The authors came to the conclusion that IoT privacy issues have only been partially examined and that further attention is required. The study, however, has flaws: the prior research analysis focuses primarily on security needs while ignoring privacy considerations; the authors do not conduct a thorough gap analysis on the publications examined; and they do not provide a comprehensive summary of future research topics in the field of IoT privacy that require more attention.

Lin et al. [54] undertake a literature review to identify security and privacy vulnerabilities in the three IoT architecture layers: network, perception, and application. The authors describe the first six fundamental security properties for these tiers as confidentiality, integrity, availability, identification and authentication, privacy, and trust. Then, the authors look at a variety of security threats for each of the three stages. The authors wrap up by giving a succinct summary of many privacy-preserving data techniques, including the stages of data collection, data aggregation, and data analysis. The authors do, however, largely focus on the IoT's security components and, as was already said, consider privacy to be one of the most crucial security aspects, rather than viewing privacy as a distinct concern. Furthermore, the research does not conduct a thorough gap analysis to discover the weaknesses of prior efforts.

Based on Ziegeldorf's [57] 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 char-

acteristics 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.

Another concept worth analyzing is differential privacy which relates more closely to the survey that will be conducted but also to the general collection and analysis of user data by applications and systems.

C. Privacidade Diferencial

The notion of differential privacy, according to Michael Kearns [58], is based on three important principles. The first being that "differential privacy requires that adding or removing the data record of a single individual not change the probability of any outcome by much". The second principle being that "no outside observer can learn very much about any individual because of that person's specific data". The third important principle being that "for every individual in the dataset, and for any observer no matter what their initial beliefs about the world were, after observing the output of a differentially private computation, their posterior belief about anything is close to what it would have been had they observed the output of the same computation run without the individual's data".

Differential privacy has the potential to significantly increase individual privacy protection, by purposefully adding noise into a dataset, it gives plausible deniability to any individual who may have had their data exploited while still being able to calculate statistics with relatively high precision. Although algorithms that deal with notions of fairness, ethics, and privacy are hard to implement because of the subjectivity of these concepts, and differential privacy algorithms are no different, they can still help in regards to addressing technology's inherent moral quandaries.

There exist other algorithms that aim to preserve privacy in the same way as differential privacy such as Google's box blurring algorithm [59] that is used in the Google Map's street view, Microsoft's Visor [60] which is a video-analytics-as-a-service tool and Shokri and Shmatikov's [61] system for collaborative deep learning, however, in general, these algorithms struggle with high computational cost, internal attacks, or non-provable privacy.

Zhao et al. [62] conduct a SLR on differential privacy for unstructured data. The authors present differential privacy methods for sensitive content in image, audio, video, and text data. They compare the various methods and perform utility analyses for each method, highlighting the benefits and drawbacks of each, the utility loss is measured in experimental evaluations between the actual data and its obfuscated variant. They come to the conclusion that differential privacy as well as its variations give stringent privacy protections for unstructured data against attackers with unpredictable background knowledge. They also suggest potential future study subjects that have yet to be investigated.

D. Soluções Propostas

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.

1) Criando Novas Formas de Conscienlização para o Utilizador: There has been some work done to determine the users awareness of their actions online regarding their privacy. Skirpan et al. [63] 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 plot of the play consist in a fledgling tech company that unveiled its revolutionary AI technology while dealing with a company whistleblower and an untimely zero-day hack on their system. The public is able to interact with the actors and influence how the story plays out. Audiences and actors were given the chance to try on roles, behaviors, and opinions that they would not normally have access to in ordinary life. 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) Legislação: Some papers seek to improve legislation [64], [65] 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.

3) Privacidade Através da Segurança: Sun et al. [66] 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.

4) Propostas de Arquitetura / Frameworks: Antunes et al. [67] 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 [68]. 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.

Opara et al. [69] present a system for spotting possible problems with privacy or security regulations in the early stages of development, this approach is intended at developers. The paper proposes a domain-specific ontology for modeling IoT security and privacy policies, a notation for representing and validating IoT security and privacy policies, a set of guidelines and rules for detecting IoT policy errors, and a tool for visually modeling and capturing IoT security policies and discovering policy problems. Although the framework that is presented is theoretically promising it has not been tested in a real environment so the effectiveness can't yet be measured. The authors also do not compare their proposal with others already available.

5) Blockchain: Blockchain is an option to guarantee privacy in IoT because of zero-knowledge proofs, ring signatures and mixing [70].

Yu et al. [71] shows various implementations of blockchain that provide privacy through security, based on different categories like data integrity, data sharing and authentication and access control. The authors use privacy as a proxy for security, they also do not discuss the weak and strong points of each implementation or make any comparison, they also do not provide further research questions.

Ali et al. [72] suggest a software stack that combines peer-to-peer file sharing with blockchain smart contracts to offer IoT users control over their data and do away with the necessity for centralized IoT data management. Blockchain smart contracts are used in the proposed 'modular consortium' architecture to regulate access while establishing responsibility for both data owners and other parties that users grant access to.

6) Outras Propostas: 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.

7) Assistentes de Privacidade: There exists a number of privacy assistants in the market. Privacy assistants have the objective of giving the user flexibility in choosing the preferred privacy options in available applications, most are used in smartphones, very few are made for devices in the IoT.

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) [74], 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 interviews were divided into three sections: exploratory, anchoring and the PPA; While the exploratory phase's purpose was to learn about participants' attitudes and understanding of IoT, the anchoring phase aimed to normalize participants' basic understanding of how IoT functions. In order to get people to think about potential privacy concerns towards the end of the anchoring section, the authors asked participants about their opinions on data privacy. In the PPA section, it was proposed the idea of a PPA for IoT as a potential future project. The authors clarified that the PPA could distinguish between active data requests such as a gadget asking biometric information from the user's health tracker and passive data collection such as a smart device with a microphone that could record people's utterances while they were nearby. The Notification, Recommendation, and Auto implementations of an IoT PPA were the three that the authors and attendees discussed. Notification PPAs can determine which adjacent devices are requesting data and alert users to those devices' presence and requests so that users can approve or reject each request. Building on notification PPAs, recommendation PPAs offer consumers advice on how to share their data based on their preferences. The user's data sharing decisions would be made by auto PPAs. This would lessen the cognitive load on consumers but also take away their ability to influence the process. They 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) [75], the authors called it IoT Assistant. Because the predominant approach of "notice and choice" for data privacy protection, they 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. The authors define meaningful privacy choices as "the capabilities provided by digital systems for users to control different data practices over their personal data", They extend the notion of privacy choices with five facets: effectiveness (the opportunity to establish privacy preferences that precisely and completely match the data collection and use methods that a user is okay with), efficiency (the capacity to specify these options with the least amount of effort and time), user awareness (where significant privacy options should be prominently and clearly communicated to users), comprehensiveness (users should understand their options, how they affect the gathering and potential use of their data, as well as what conclusions might be drawn from this data and the potential repercussions of these conclusions) and neutrality (meaningful privacy decisions should not be subject to manipulation or bias). The IoT Assistant offers four privacy settings, giving end users a variety of alternatives to better suit their varied privacy preferences and as a result, privacy options are more effective in the IoT environment. The IoT Assistant acts as a centralized privacy choice platform by implementing various privacy options, allowing consumers to more effectively govern their data privacy in IoT. The three IoT system discovery modes that the IoT Assistant supports are QR codes, push notifications, and location-based map interfaces. These discovery tools are probably going to make users more aware of the installed IoT devices and the privacy options they have. Additionally, the united viewpoint of the integrated notification and option in the the IoT Assistant gives succinct yet thorough information regarding IoT data practices to help users better understand the implications of their privacy choices. Additionally, the authors work to implement the integrated notice and option in the IoT Assistant without bias or framing, attempting to offer consumers a neutral space to execute their privacy choices. Although the authors view the IoT Assistant as a significant step towards "meaningful privacy options" in IoT, this assistant still has many problems, such as the fact that it is still in its early stages of development and that there hasn't been much growth given that it was created in 2020 and we are in 2023. Maybe the main reason this application was not able to be developed further is that the application itself serves to show the user the data that is already in the IoT infrastructure that was created before, and as such it is not capable of identifying new IoT devices without the end users themselves create on the infrastructure's main webpage [76] a new entry for the device in question that the user wants to interact with. Another reason that cripples this application as well as others that seek to provide better privacy in IoT systems is that many systems do not offer any type of privacy choices to the end user or to other users that are not the intended end users but the devices are still collecting data about.

The IoT infrastructure that was developed [76] is built on an open, distributed design that allows for the deployment and management of IoT resources to be carried out by any number of actors. Part of this infrastructure is the Internet of Things Resource Registry, it is a web platform that enables resource owners to declare not only the place where a resource is deployed but also data practices like the reason(s) for a particular data collecting process, the level of detail in the data being gathered, retention, the recipients of the data, and more. Additionally, it discloses any user-configurable privacy settings that might be connected to a particular resource.

E. *Principais Levantamentos*

There are two main ways to provide privacy in IoT systems, through security or using privacy notices, other ways like through legislation or with the creation/usage of a framework that provides privacy fall into these two categories. Most of the literature assumes that security and privacy are synonyms, for example [65], [66], [69], and so most of the proposed solutions fall under privacy through security. The proposed solutions that use privacy notices, like [75], are implemented in a way that use other devices like smartphones that provide the notices themselves, it is hard to provide privacy notices on the IoT devices themselves because many of these devices do not have a screen or the screen is too small to provide the necessary information to the user. Because there are still no standards for implementing privacy notices, and best practices are scattered throughout the literature, they are mostly implemented haphazardly, little guidance is given to designers and developers on how to make a privacy notice design that is sufficient and acceptable for their particular system and its features. Designers may be unaware of the numerous possibilities for creating acceptable privacy notifications and, as a result, do not systematically explore them.

Aleisa and Renaud [77] 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 [78]. Hitchhiking [79] 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 [80] 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.

III. Desafios de Privacidade

IoT is a composed of a complex web of architectures, applications and technologies. In terms of architectures, it can be decomposed in three layers: the perception layer, the network layer and the application layer.

The perception layer, also known as the sensor layer, interacts with physical objects and components via smart devices (RFID, sensors, actuators, and so on). Its key objectives are to connect objects to the IoT network and to monitor, collect, and analyze status information about these things using deployed smart devices. This layer can often be unreliable, for instance with autonomous vehicles where they find it hard to read road signs or to predict if certain objects are inanimate or not, but this unreliability also brings privacy even though some of the data might be unusable. Noise can also be added in this layer to provide extra privacy.

In the network layer there are many competing networks like ZigBee, Z-Wave, Bluetooth Low Energy, LoRa, Wi-fi, etc., this layer is fragmented specially in regards to wireless networks and that makes it very difficult to create an IoT architecture that can use various networks and have the various devices communicate with each other, even though interoperability is seen as a very important factor in IoT. Some of these networks are open standard protocols while others are proprietary and use different protocols of communication, use different frequencies, different ranges and different data rates. When creating an IoT architecture the designers often think of how to solve specific problems and use what is best for the current needs, and the way that IoT is fragmented doesn't help in providing progress.

The application layer receives data from the network layer and uses it to execute essential services or operations. This layer, for example, can provide the storage service to backup incoming data into a database or the analysis service to analyze received data in order to predict the future state of physical devices. This layer encompasses a wide range of applications, each with its own set of requirements. A few examples are smart grids, smart transportation, and smart cities.

According to Qu et al. [81], 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.

IV. METADOLOGIA

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 [82] 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.

A. *Estágio 1: Percepções do Utilizador*

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 [83]. 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 [84], this was the second survey done on the country's population. It was also inspired by Alves's master's thesis [85], 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.

B. *Estágio 2: Estudo no Contexto, uma Aplicação*

This work proposes an application that gives users information about IoT devices in their surroundings like the type of information these devices collect and what privacy options are available. This application will be developed for mobile phones because it is the most used device that people take everywhere they go, and because the application will use georeferencing to show the location of the IoT devices. The main objective of this application is to give users another option in order to protect their private data. The application will show the geolocation of the IoT devices, what type of device it is, what type of data is being collect by the device. The application will not detect the devices by itself, this will be done by the users themselves, in the first few 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 constraints of this paper. The application will be developed with Flutter, other options could be React Native or a progressive web application, but Flutter uses ahead of time and just in time compilation with Dart as it is programming language while React Native uses the Javascript programming language that was never created for mobile programming so it uses a bridge to convert Javascript to native components for Android or iOS. Flutter has better performance and as such it is the chosen framework for this application.

V. Estado Atual do Projeto

The preliminary results of the study, based on 10 responses, show that everyone agrees that privacy is important to them and some people know that they should not share their personal information with anyone they do not trust (like clicking on random urls or using unprotected websites/software), but most of them think that privacy and security are the same concept, most respondents also do not read privacy notices but accept them to access the information they want to get to, most respondents use their devices mostly to access social networks and for work, when it comes to IoT, there is a dissonance between knowing the term and using devices like smart watches or RFID enabled devices, from the respondents that answered yes to using IoT devices most use because of work. It is also noted that most respondent have a background in engineering, so the responses are skewed. As a result, the survey will remain open to gather a larger number of responses and participants for more significant results and generalizations.

Work plan	January				February				March				April				May			
Week	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Discovery and planning	■																			
Research enquiry	■	■	■	■	■	■	■	■	■	■	■	■								
State of the art	■	■	■	■	■	■	■	■												
Project requirements	■	■	■	■																
Wireframes and user stories					■	■	■	■												
Prototyping and refinement								■	■	■	■									
Development									■	■	■	■	■	■	■	■	■	■	■	■
Tests and iterations												■	■	■	■	■				
Release and documentation																	■	■	■	■

TABLE I
WORK PLAN TIMELINE

As can be seen in Table I, the first months will involve the design of the application and the enquiry of the study followed by the development of the application and the synthesis of the study, and finally testing and refinement of the application. Because of the exploratory nature of this work the application might suffer alterations to the design, specially in the testing stage, and also depending on the results of the study.

VI. Trabalho Futuro

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.

VII. Conclusão

This project aims to do an exploratory analysis of privacy in IoT systems. It proposes a survey to better understand user's knowledge on this subject and an application that aims to create more users awareness and better inform about their environment, as well as the IoT devices that inhabit it and how they can respond accordingly.

Hopefully the work conducted on this project will be useful to further support researchers and the application that will be developed will be able to provide greater visibility, thus allowing users to acquire knowledge about the data being collected and how they can adjust their behavior or respond more effectively to protect their privacy rights.

References

[1] D. Vincent, *Privacy: A short history*. John Wiley & Sons, 2016.

[2] B. Moore, *Privacy: Studies in social and cultural history*. Routledge, 2017.

[3] E. Roosevelt, P. C. Chang, C. Malik, W. R. Hodgson, H. S. Cruz, R. Cassin, A. E. Bogomolov, C. D. 1st Baron Dukeston, and J. P. Humphrey. (1948) Universal declaration of human rights. Accessed: 2022-11-05. [Online]. Available: https://www.un.org/en/about-us/universal-declaration-of-human-rights

[4] I. A. for Privacy Professionals. (2021) What does privacy mean? Accessed: 2022-11-04. [Online]. Available: https://iapp.org/about/what-is-privacy/

[5] S. Spiekermann and L. F. Cranor, "Engineering privacy," *IEEE Transactions on Software Engineering*, vol. 35, no. 1, pp. 67–82, 2009.

[6] HIV.gov. (2018) The difference between security and privacy and why it matters to your program. Accessed: 2022-11-04. [Online]. Available: https://www.hiv.gov/blog/difference-between-security-and-privacy-and-why-it-matters-your-program

[7] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor, "Exploring how privacy and security factor into iot device purchase behavior," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–12.

[8] Y. J. Park, "Personal data concern, behavioral puzzle and uncertainty in the age of digital surveillance," *Telematics and Informatics*, vol. 66, p. 101748, 2022.

[9] N. A. Zhang, C. A. Wang, E. Karahanna, and Y. Xu, "Peer privacy concern: Conceptualization and measurement." *MIS Quarterly*, vol. 46, no. 1, 2022.

[10] M. Weiser, "The computer for the 21 st century," *Scientific american*, vol. 265, no. 3, pp. 94–105, 1991.

[11] K. Ashton. (2009) That "internet of things" thing. Accessed: 2022-11-05. [Online]. Available: https://www.rfidjournal.com/that-internet-of-things-thing

[12] D. Marikyan, S. Papagiannidis, and E. Alamanos, "A systematic review of the smart home literature: A user perspective," *Technological Forecasting and Social Change*, vol. 138, pp. 139–154, 2019.

[13] F. Arena, G. Pau, and A. Severino, "An overview on the current status and future perspectives of smart cars," *Infrastructures*, vol. 5, no. 7, p. 53, 2020.

[14] M. Al-Emran, S. I. Malik, and M. N. Al-Kabi, "A survey of internet of things (iot) in education: Opportunities and challenges," *Toward social internet of things (SIoT): enabling technologies, architectures and applications*, pp. 197–209, 2020.

[15] N. Niknejad, W. B. Ismail, A. Mardani, H. Liao, and I. Ghani, "A comprehensive overview of smart wearables: The state of the art literature, recent advances, and future challenges," *Engineering Applications of Artificial Intelligence*, vol. 90, p. 103529, 2020.

[16] I. F. Akyildiz and A. Kak, "The internet of space things/cubesats," *IEEE Network*, vol. 33, no. 5, pp. 212–218, 2019.

[17] C. Everhart, E. Caplan, and D. Nichols, "Re: Interesting uses of networking," https://cseweb.ucsd.edu/~bsy/coke.history.txt, 1990, accessed: 2022-12-14.

[18] J. Romkey, "Toast of the iot: The 1990 interop internet toaster," *IEEE Consumer Electronics Magazine*, vol. 6, no. 1, pp. 116–119, 2017.

[19] S. Madakam, V. Lake, V. Lake, V. Lake *et al.*, "Internet of things (iot): A literature review," *Journal of Computer and Communications*, vol. 3, no. 05, p. 164, 2015.

[20] M. Hasan. (2022) State of iot 2022: Number of connected iot devices growing 18% to 14.4 billion globally. Accessed: 2022-11-04. [Online]. Available: https://iot-analytics.com/number-connected-iot-devices/

[21] S. Al-Sarawi, M. Anbar, R. Abdullah, and A. B. Al Hawari, "Internet of things market analysis forecasts, 2020-2030," in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 2020, pp. 449–453.

[22] N. Alhirabi, O. Rana, and C. Perera, "Security and privacy requirements for the internet of things: A survey," *ACM Transactions on Internet of Things*, vol. 2, no. 1, pp. 1–37, 2021.

[23] D. Peloquin, M. DiMaio, B. Bierer, and M. Barnes, "Disruptive and avoidable: Gdpr challenges to secondary research uses of data," *European Journal of Human Genetics*, vol. 28, no. 6, pp. 697–705, 2020.

[24] A. Gladis, N. J. Hartwich, and O. Salge, "Weaponizing the gdpr: How flawed implementations turn the gold standard for privacy laws into fool's gold," 2022.

[25] G. Gentile and O. Lynskey, "Deficient by design? the transnational enforcement of the gdpr," *International & Comparative Law Quarterly*, vol. 71, no. 4, pp. 799–830, 2022.

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

[27] D. Y. Byun, "Privacy or protection: The catch-22 of the ccpa," *Loy. Consumer L. Rev.*, vol. 32, p. 246, 2019.

[28] D. Thomson, D. P. Cochrane, I. Chantzos, P. Carter, S. John, P. U. Helmbrecht, and S. Room, "State of privacy report 2015," Symantec, Tech. Rep., 2015.

[29] D. J. Solove, "The myth of the privacy paradox," *Geo. Wash. L. Rev.*, vol. 89, p. 1, 2021.

[30] M. Williams, J. R. C. Nurse, and S. Creese, "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)*, 2017, pp. 181–18 109.

[31] A.-R. Lee, "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*, vol. 13, no. 19, p. 10679, 2021.

[32] D. Goad, A. T. Collins, and U. Gal, "Privacy and the internet of things-an experiment in discrete choice," *Information & Management*, vol. 58, no. 2, p. 103292, 2021.

[33] N. Gerber, P. Gerber, and M. Volkamer, "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior," *Computers & security*, vol. 77, pp. 226–261, 2018.

[34] D. Wilson and J. S. Valacich, "Unpacking the privacy paradox: Irrational decision-making within the privacy calculus," 2012.

[35] J. Warshaw, T. Matthews, S. Whittaker, C. Kau, M. Bengualid, and B. A. Smith, "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*, 2015, pp. 797–806.

[36] N. Lee and O. Kwon, "A privacy-aware feature selection method for solving the personalization–privacy paradox in mobile wellness healthcare services," *Expert systems with applications*, vol. 42, no. 5, pp. 2764–2771, 2015.

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

[38] A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. di Vimercati, "What can behavioral economics teach us about privacy?" in *Digital privacy*. Auerbach Publications, 2007, pp. 385–400.

[39] B. P. Knijnenburg, A. Kobsa, and H. Jin, "Dimensionality of information disclosure behavior," *International Journal of Human-Computer Studies*, vol. 71, no. 12, pp. 1144–1162, 2013.

[40] R. Wakefield, "The influence of user affect in online information disclosure," *The Journal of Strategic Information Systems*, vol. 22, no. 2, pp. 157–174, 2013.

[41] C. Flender and G. Müller, "Type indeterminacy in privacy decisions: the privacy paradox revisited," in *International Symposium on Quantum Interaction*. Springer, 2012, pp. 148–159.

[42] T. Dienlin and S. Trepte, "Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors," *European journal of social psychology*, vol. 45, no. 3, pp. 285–297, 2015.

[43] Y. M. Baek, "Solving the privacy paradox: A counter-argument experimental approach," *Computers in human behavior*, vol. 38, pp. 33–42, 2014.

[44] M. Taddicken, "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*, vol. 19, no. 2, pp. 248–273, 2014.

[45] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of consumer affairs*, vol. 41, no. 1, pp. 100–126, 2007.

[46] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & security*, vol. 64, pp. 122–134, 2017.

[47] L. Brandimarte, A. Acquisti, and G. Loewenstein, "Misplaced confidences: Privacy and the control paradox," *Social psychological and personality science*, vol. 4, no. 3, pp. 340–347, 2013.

[48] W. Xie and K. Karan, "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*, vol. 19, no. 3, pp. 187–201, 2019.

[49] K. S. Schwaig, A. H. Segars, V. Grover, and K. D. Fiedler, "A model of consumers' perceptions of the invasion of information privacy," *Information & Management*, vol. 50, no. 1, pp. 1–12, 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378720612000754

[50] S. Sannon, N. N. Bazarova, and D. Cosley, "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*, 2018, pp. 1–13.

[51] S. Gupta and S. Ghanavati, "Privacy in the internet of things: Where do we stand? a systematic literature review," 5 2022. [Online]. Available: https://www.techrxiv.org/articles/preprint/Privacy_in_the_Internet_of_Things_Where_do_We_Stand_A_Systematic_Literature_Review/19874329

[52] P. Kühtreiber, V. Pak, and D. Reinhardt, "A survey on solutions to support developers in privacy-preserving iot development," *Pervasive and Mobile Computing*, vol. 85, p. 101656, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574119222000785

[53] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer networks*, vol. 76, pp. 146–164, 2015.

[54] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[55] J. Porras, J. Pänkäläinen, A. Knutas, and J. Khakurel, "Security in the internet of things-a systematic mapping study," 2018.

[56] B. S. Ahmed, M. Bures, K. Frajtak, and T. Cerny, "Aspects of quality in internet of things (iot) solutions: A systematic mapping study," *IEEE Access*, vol. 7, pp. 13 758–13 780, 2019.

[57] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: threats and challenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728–2742, 2014.

[58] M. Kearns and A. Roth, *The ethical algorithm: The science of socially aware algorithm design*. Oxford University Press, 2019.

[59] A. Frome, G. Cheung, A. Abdulkader, M. Zennaro, B. Wu, A. Bissacco, H. Adam, H. Neven, and L. Vincent, "Large-scale privacy protection in google street view," in *IEEE International Conference on Computer Vision*, 2009. [Online]. Available: https://research.google.com/archive/papers/cbprivacy_iccv09.pdf

[60] R. Poddar, G. Ananthanarayanan, S. Setty, S. Volos, and R. A. Popa, "Visor: Privacy-preserving video analytics as a cloud service," in *USENIX Security Symposium*, August 2020. [Online]. Available: https://www.microsoft.com/en-us/research/publication/visor-privacy-preserving-video-analytics-as-a-cloud-service/

[61] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2015, pp. 909–910.

[62] Y. Zhao and J. Chen, "A survey on differential privacy for unstructured data content," *ACM Comput. Surv.*, vol. 54, no. 10s, sep 2022. [Online]. Available: https://doi.org/10.1145/3490237

[63] M. Skirpan, M. Oates, D. Byrne, R. Cunningham, and L. F. Cranor, "Is a privacy crisis experienced, a privacy crisis avoided?" *Commun. ACM*, vol. 65, no. 3, pp. 26–29, feb 2022. [Online]. Available: https://doi.org/10.1145/3512325

[64] R. H. Weber, "Internet of things: Privacy issues revisited," *Computer Law & Security Review*, vol. 31, no. 5, pp. 618–627, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0267364915001156

[65] N. Fabiano, "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)*, 2017, pp. 727–734.

[66] Q. Sun, K. Lin, C. Si, Y. Xu, S. Li, and P. Gope, "A secure and anonymous communicate scheme over the internet of things," *ACM Trans. Sen. Netw.*, vol. 18, no. 3, apr 2022. [Online]. Available: https://doi.org/10.1145/3508392

[67] R. S. Antunes, C. André da Costa, A. Küderle, I. A. Yari, and B. Eskofier, "Federated learning for healthcare: Systematic review and architecture proposal," *ACM Trans. Intell. Syst. Technol.*, vol. 13, no. 4, may 2022. [Online]. Available: https://doi.org/10.1145/3501813

[68] B. Chen, S. Qiao, J. Zhao, D. Liu, X. Shi, M. Lyu, H. Chen, H. Lu, and Y. Zhai, "A security awareness and protection system for 5g smart healthcare based on zero-trust architecture," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10 248–10 263, 2021.

[69] A. Opara, H. Johng, T. Hill, and L. Chung, "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*, 2022, pp. 198–201.

[70] W. contributors. (2022) Privacy and blockchain. Accessed: 2023-01-02. [Online]. Available: https://en.wikipedia.org/wiki/Privacy_and_blockchain

[71] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the internet of things," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 12–18, 2018.

[72] M. S. Ali, K. Dolui, and F. Antonelli, "Iot data privacy via blockchains and ipfs," in *Proceedings of the Seventh International Conference on the Internet of Things*, ser. IoT '17. New York, NY, USA: Association for Computing Machinery, 2017. [Online]. Available: https://doi.org/10.1145/3131542.3131563

[73] H. Zhu, S. C.-K. Chau, G. Guarddin, and W. Liang, "Integrating iot-sensing and crowdsensing with privacy: Privacy-preserving hybrid sensing for smart cities," *ACM Trans. Internet Things*, vol. 3, no. 4, sep 2022. [Online]. Available: https://doi.org/10.1145/3549550

[74] J. Colnago, Y. Feng, T. Palanivel, S. Pearman, M. Ung, A. Acquisti, L. F. Cranor, and N. Sadeh, "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*, ser. CHI '20. New York, NY, USA: Association for Computing Machinery, 2020, pp. 1–13. [Online]. Available: https://doi.org/10.1145/3313831.3376389

[75] Y. Feng, Y. Yao, and N. Sadeh, "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*, ser. CHI '21. New York, NY, USA: Association for Computing Machinery, 2021. [Online]. Available: https://doi.org/10.1145/3411764.3445148

[76] A. Das, M. Degeling, D. Smullen, and N. Sadeh, "Personalized privacy assistants for the internet of things: Providing users with notice and choice," *IEEE Pervasive Computing*, vol. 17, pp. 35–46, 07 2018.

[77] N. Aleisa and K. Renaud, "Privacy of the internet of things: a systematic literature review (extended discussion)," *arXiv preprint arXiv:1611.03340*, 2016.

[78] E. D. P. Supervisor, "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.

[79] K. P. Tang, P. Keyani, J. Fogarty, and J. I. Hong, "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*, 2006, pp. 93–102.

[80] C. Kang, F. Abbas, and H. Oh, "Protection scheme for iot devices using introspection," in *2015 6th International Conference on the Network of the Future (NOF)*. IEEE, 2015, pp. 1–5.

[81] Y. Qu, S. Yu, W. Zhou, S. Peng, G. Wang, and K. Xiao, "Privacy of things: Emerging challenges and opportunities in wireless internet of things," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 91–97, 2018.

[82] S. Keshav, "How to read a paper," *SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 3, pp. 83–84, jul 2007. [Online]. Available: https://doi.org/10.1145/1273445.1273458

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

[84] P. Survey and R. Center. (2022) Conduct of privacy survey. Accessed: 2022-12-19. [Online]. Available: https://www.privacy.gov.ph/wp-content/uploads/2022/01/CONDUCT-OF-PRIVACY-SURVEY-Final-Report-v3.pdf

[85] M. H. d. S. Alves, "Gdpr in portugal: Analysis of citizens' perception about privacy," 2021.