Securing the Internet of Things (IoT) Data Ownership

Mikko Vermanen [1], Juhani Naskali [2], Ville Harkke [3] and Jani Koskinen [4]

[1] *University of Turku, Rehtorinpellonkatu 3, Turku, Finland*
[2] *University of Turku, Rehtorinpellonkatu 3, Turku, Finland*
[3] *Åbo Akademi University, Tuomiokirkontori 3, Turku, Finland*
[4] *University of Turku, Rehtorinpellonkatu 3, Turku, Finland*

Abstract

As the commercial use of IoT (Internet of Things) technology keeps spreading rapidly, so does the involvement of individuals as data sources. Thus, it is crucial to understand the nature and implications of data property factors in the IoT context to enable organisations to apply ethically sustainable practices when defining data ownership. The study is based on Richard O. Mason's PAPA framework from 1986, in which the question of intellectual property rights is described as one of the most complex issues we face as a society. Based on our findings, this statement still applies in modern IoT ecosystems. In this paper, the ownership and control of information is clarified on conceptual and practical levels. We investigate the topic from the following three perspectives: 1) organisational level, 2) technical level, and 3) ethical ownership. Furthermore, we offer development proposals for the current IoT protocols, aiming to support defining data ownership.

Keywords

Internet of Things, Ethics, Data Ownership, PAPA

1. Introduction

In this paper, the ownership and control of information is investigated in the context of IoT based on two key reasons. Firstly, the paper contributes to a larger study, in which a framework addressing the ethical issues of IoT deployment is created. In the ethical model, the four original issue categories introduced by Mason [1] are applied in IoT context, in addition to potential additional issue categories intended to enhance the model's coverage. Secondly, IoT presents an interesting technological environment, in which a vast amount of data can be gathered from objects that are often linked to individuals, either directly or indirectly [2]. While IoT provides its users with a multiplicity of achievable benefits, it brings along a variety of potential ethical threats towards the position and/or privacy of individuals.

While PAPA [1] provides a solid basis for investigating the ethical matters related to data ownership, it lacks the depth necessary for providing practitioners and researchers with sufficient tools for examining these matters on a concrete level, and especially in the context of a specific technology. Hence, the purpose of this paper is partly to deepen the understanding on data ownership issues on theoretical level and to provide practical ideas for implementing ownership information in data protocols. By this, we facilitate further discussion on the complex issues involved in data ownership on different abstraction levels. While the data ownership paradigms have already been studied in extant literature[3],this paper provides further knowledge on the topic by investigating the phenomenon in the context of commercial use of IoT, which involves unique nuances in terms of underlying functional mechanisms and the role of individuals. More specifically, IoT forms a complex ecosystem where the data is collected by machines, yet is dependent on human involvement, thus forming challenging foundations for defining data ownership.

Conference on Technology Ethics - Tethics, October 18–19, 2023, Turku, Finland
EMAIL: mikko.vermanen@utu.fi (A. 1); juhani.naskali@utu.fi (A. 2); ville.harkke@utu.fi (A. 3); jasiko@utu.fi (A. 4)
ORCID: 0000-0003-3500-6974 (A. 1); 0000-0002-7559-2595 (A. 2); 0000-0003-3743-2686 (A. 3)); 0000-0001-8325-9277 (A. 4)


The paper is structured as follows. In chapter 2, we set the context by introducing three key areas considered in this paper: Internet of Things, PAPA framework, and ownership of data including the theoretical level aspects and matters related to property ethics. Chapter 3 covers two dimensions of data property: organisational level and technical level. In chapter 4 we focus on the ethical issues of data ownership and introduce potential ownership models. In chapter 5 we consider the potential limitations of this paper and introduce opportunities for further research. In chapter 6 we end up with conclusions.

2. Background

2.1. Internet of Things

The term IoT (Internet of Things) was coined by Peter T. Lewis already in 1985 and described as follows:

"*The Internet of Things, or IoT, is the integration of people, processes and technology with connectable devices and sensors to enable remote monitoring, status, manipulation and evaluation of trends of such devices.*" [4]

Throughout the years, the meaning of the term has become further defined [5]. However, the core idea remains the same; collection and delivery of data from various monitorable and measurable objects to users via the internet.

By utilising IoT solutions, companies commonly aim for enhanced performance and reduced manual labour through digital and potentially more accurate information collection tools. Through encouraging success stories and better usability, reliability and affordability, even the less technologically oriented and smaller companies are able to implement these solutions into their daily practices.[6]

However, the use of IoT has consequences and possibilities that are not all ethically positive. Ng and Wakenshaw[7] noted that information is ubiquitous, liquefying everywhere, thus allowing more possibilities, but also resulting in vulnerabilities for individuals. The datafication and use of personal information constitute a new kind of information society where people are objectified and this has raised ethical challenges[8], Personal information — collected through IoT — has risks associated with access, ownership, privacy and confidentiality [7]. These issues are those that the PAPA model has shown over thee decades ago but still it has not been widely adopted in the context of IoT except for a few occasions [9].

2.2. PAPA framework

In 1986, Richard O. Mason introduced the ethical PAPA framework addressing the potential issues of the information age, especially from the data perspective. PAPA is an acronym for the four key categories included in the framework: privacy, accuracy, property, and accessibility. [1] These issues have maintained their relevance to this day and can rather fluently be applied in the IoT context as well [9], even thought there is a need for critical investigation on how the model could be modified or upgraded to meet challenges that the current information age brings within. According to Mason [1], some of the most central questions regarding the data property are who owns the information, how its pricing should be defined, who owns the data transmission channels and how the access to data should be allocated. Through the IoT perspective, the property issues we have so far considered from both individual and organizational perspectives are how the data ownership should be shared within an organization and throughout the IoT ecosystem and, furthermore, are there any alternative ownership approaches to be considered, such as mastery of data [10,11,12]

However, in this article, we will focus on concrete foundations in terms of investigating the actual implementation potential of ownership of data in the case of IoT. It is notable that even with legislation such as the GDPR the ownership of data itself has been and is a problematic issue to solve[13,14,15]. That said, this paper is built around the hypothesis that a fundamental idea of ownership can be applied to data. This approach dismisses the problem of whether ownership itself can be applied to data in this

context and leaves it to future research endeavours. Therefore, our premise is that data can be owned and the owner(s) can be defined.

2.3. PAPA framework

We have previously identified several open questions related to data ownership in the vein of considerations introduced in PAPA [9]. In terms of data management, we have found questions such as where and for how long the IoT data should be stored and who is responsible for its disposal to be worthy of further investigation. Regarding the relationship between ownership and communication, we encourage further discussion on how the individuals within the IoT ecosystem should be informed about their rights to the data and its ownership. Finally, understanding the regulatory and societal implications require deeper understanding on how the involvement of multiple organisational stakeholders affect the ownership, and moving further, can the data be legally and ethically monetised, by whom and for what price. Based on this background, we take into account these question by providing usable, yet simple, foundations in form of a generic and universally applicable IoT protocol update. However, to fully comprehend the basis of how property will be addressed, it is important to also understand the key functions of the other three PAPA categories, which also partly intertwine with property. Briefly explained, the privacy category of PAPA covers the matters related to what information the individuals can or cannot seclude about themselves [16] and to what degree can the individuals control what, how, when, and why data is collected [9]. Accuracy, sometimes also referred to as accountability, aims to investigate whether the collected data is aligned with reality, which is of great importance when considering the possible consequences towards employees. As an example, when the gathered location data indicates that an employee hasn't arrived at the worksite, while in reality, the interpreted data was inaccurate due to a technical failure. Finally, the accessibility category primarily covers matters such as who can access the collected data, as well as who it can be distributed to.[1]

In this paper, we mainly focus on the property perspective, and more specifically on data ownership and how it can be retained throughout the data life cycle. Considering the holistic nature of the PAPA framework, it is important to acknowledge that the presented issue categories intertwine with each other and thus shouldn't be entirely separated. It is also worthy of noting that the original PAPA model has its limitations as it does not give attention to some other relevant aspects, such as motives behind data collection [17]. However, despite criticism, PAPA-model is a fruitful approach and thus suitable for this paper, which focuses on property and ownership issues. The most important issue areas to be reviewed in relation to the property are the accessibility and privacy of data which will also be observed to a necessary degree. While relevant literature addressing the personal data ownership in the context of IoT does exist [15], we see that so far the ethical perspectives have not been addressed to a sufficient degree. Thus, we focus on investigating and building ethically sustainable foundations for how the ownership can be communicated to each stakeholder throughout the IoT data life-cycle in practice and on protocol level.

3. Data as Property?

3.1. PAPA framework

From an organisational perspective, there are individuals who collect information and individuals who provide the information, regardless of the mechanism or level of automation used in the data collection [6]. Thus, the distinction between information collected from individuals or other actors and the information that was created by the company itself must be clarified to see the difference between those. It is important to understand the needs and rationales that companies have, or we may end up in a situation where we are developing a regulation that prevents actions of smaller companies because they do not have the resources to solve regulative issues. This can create a market barrier which protects the big corporations that already have too strong a position and negotiation power over the market and individuals. [18,19]

As the deployment rate of IoT solutions keeps rising, so does the amount of data collected from employees. According to Gartner [20], the amount of enterprise and automotive IoT endpoints grows

21 percent between 2019 and 2020 and similar development has been projected to continue in the foreseeable future. Meanwhile, no clear guidelines regarding just distribution of data ownership exist, which makes it difficult for companies to define and implement ethical practices reliably. While regulative guidelines, and perhaps most prominently the GDPR (EU General Data Protection Regulation), aim to set universally applicable rules for data privacy, they don't thoroughly take into account the ethical principles. Combined with the lack of literature addressing the ethical distribution of IoT data in the business environment, there is a clear research gap with concrete business implications to be fulfilled.

The ability of an organisation to handle ethical issues is affected by the specific characteristics of typical SMEs in relation to data and knowledge management, namely the more or less forced usage of systems designed for larger organisations and limited ability or incentive to apply specific data management practices [21] as well as the emphasized role of personal knowledge [22]. This limitation does however not seem to limit the SME's adoption of technologically challenging types of IoT projects [23]. The ethical management abilities of the SME sector could be enhanced by introducing mechanisms for handling property issues within the enabling technologies themselves. This would manifest itself in the form of a meta-data structure of the protocols that contain the information. The purpose of this is to ensure that the responsible individuals and organisations will define the ownership properties of the data and be prepared to react to issues should they arise. Thus the technology would act as a powerful enabler of organisational change.

Given the nature of IoT data, there are naturally a limited number of relevant questions about ownership in some cases. The bulk of sensory data transmitted through the IoT networks does not usually contain anything that could be of concern for any person or subject. In those cases, the question of data property is simply solved as organisational ownership or subject of freely defined rules and inter-organisational contracts. It is outside this realm of ethically neutral data where the questions of ownership have ethical implications.

The GDPR does provide a background for classifying data even for ethical considerations. Palmirani et al. [24] identify in their legal ontology the following types of Sensitive data: health data, ethnic data, genetic data, biometric data, sexual data, and opinion data. Furthermore, any data related to a person, sensitive or not, does fall into the category of personal data. Even the context in which the data is collected and potentially used dictates the need for clarification of data ownership [25]. Some types of data may be used in secondary purposes and be analysed as parts of larger databases, and for these uses, the data can be anonymised in order to protect individual privacy. Even this would require the consent of the data owner, especially as the anonymisation may relatively easily be broken [26].

While it is crucial to provide the SMEs with an ability to implement an ethical approach by setting transparent rules for the property distribution in the data gathering phase, we should also pay attention to how the data will potentially be used afterwards, either internally or by and with an external organisation. We aim to address this issue by introducing a functional meta-data approach, whose purpose is to guarantee that the property information related to certain data will remain throughout their lifetime. Furthermore, this meta-data approach enables us to attach a multitude of other relevant information, such as the original purpose of the data, which enables its users to evaluate its validity in their context and environment. The meta-data approach and its requirements are presented more thoroughly in the next chapter which focuses on the potential of technical standardisation of IoT data especially in terms of ownership.

3.2. Technical Level

With the technical level, we refer to the methods and channels with and through which IoT data is transferred. More precisely, we concentrate on IoT data transfer layer protocols that are capable of handling and controlling larger information flows, containing the information of original data ownership (property), whose purpose is to enable new users to firstly identify and recognise the original owner of the data and to evaluate its applicability in potentially differing contexts.

Considering our ability to implement the additional information, we must take into account the possibilities and limitations set by the available IoT transfer layer protocols. Some known IoT protocols [27,28] are CoAP (Constrained Application Protocol), DTLS (Datagram Transport Layer Security),

UDP (User Datagram Protocol) and TCP (Transmission Control Protocol). The last two run on IP (Internet Protocol), which takes care of routing packets to the recipient. Numerous more protocols exist (e.g. MQTT, XMPP, AMQP), and our ideas can be implemented on many of them. As a whole, data transfer protocols tend to be built to serve a specific purpose and contain capabilities providing optimal performance for specific use cases, considering the common limitations present in IoT solutions, such as power consumption and bandwidth [29]. It is worth noting that these protocols may also intertwine with each other in terms of characteristics and features, an example of such a case being the CoAP, which also utilises the features of UDP. To estimate their capability to fulfill the need for storing new content requires further examination of their features.

Information that is pertinent to the handling of network transfers could be placed in packet headers of the network layer protocol(s) used. For example, when using IP protocol, additional Options (up to 60 bytes) can be included in the header. As Options are included in each packet, even if the transmitted data is fragmented over multiple packets, their content can easily be used for package routing. For example, including a flag for sensitive information would allow routers to (dis)allow routes outside internal company networks or national lines based on this information. This could be useful in securing packet routing for sensitive information.

On a higher application level1 data transfer, with protocols such as HTTP, request and response headers can be used to transmit information related to a higher-level dataflow that can consist of multiple packets. On this level, there is more space for metadata, and it is transferred less frequently (i.e. more efficiently). This can be a boon for energy-efficiency.

The key aspect in terms of selecting a suitable protocol to contain the proposed new data fields is the capability of storing additional information without decreasing the protocol's performance or exceeding its functional and/or content-related limitations. Thus, whether or not including the additional information fields would cause a proportionally significant increase in data to be transferred in each package and/or power consumption must be considered. For example, the CoAP protocol was specifically designed to support devices operating on battery power, and thus its original purpose may be compromised once additional data needs to be transferred. Similarly, the MQTT protocol was specifically designed to support low-bandwidth networks, and thus processing and storing more data could potentially decrease its performance and usability.

Thus, to solve the issue of diminishing acknowledgment of data ownership, we claim that a specific section or field is required to display the property information. Most importantly, new users should be able to identify the original owner. However, the users may also benefit from information such as the original purpose of the data and the context of its collection. This said, the proposed additional information fields would be firstly the owner and secondly the original purpose of the data. Whether or not the existing protocols, and more specifically their capabilities and performance limitations, allow the additions of these fields or if a new protocol is needed requires further technical investigation. However, as technology advances, the inclusion of new metadata fields is hardly a real problem.

4. Ethical Ownership

Defining the concept of "owning" and "property" could be a task for a whole academic career as there has been debate on it over centuries or even millennia and the term itself has been obscured depending on the position of the observer and the aim of the particular discourse [30,31,32].

The property part of Mason's PAPA model is interesting as it intertwines through the accountable access to privacy as "ownership" gives rights to define what is done by information and by whom. This view, of course, is a harshly simplified portrayal of how property is related to the other three ethical issues of the PAPA model. Nevertheless, it still shows the built-in connection between privacy, accuracy, property, and accessibility.

Thus, the property is a multidimensional issue per se and IoT as a limiting context does not make it considerably easier to approach. Even though we have legislation and other regulations considering the concept of (immaterial) property of information, property is complex and problematic from an ethical basis. To clarify the issue we will analyse property from ethical viewpoints on a theoretical level and look at different ownership cases before going to a more practical level in organisational context of SMEs.

4.1. Ethical Basis

The ethical basis of the immaterial property itself is a questionable and controversial issue. Even defining the concept of "owning" and "property" is hard. Those have been targets of continuous interest through centuries, and the use of the terms has been obscured depending on the position of the observer and the aim of the particular discourse [12,32,33]. Like Alexander and Peñalver [34] have found, property rights are usually justified based on the following theories: utilitarian-based, person-based, Lockean-based, Kantian-based or based on the Aristotelian concept of human flourishing. Here we will look at the issue in the context of IoT through the ethical views of deontology (intention) and consequentialism (outcome). We do not look at the virtue ethics (human flourishing) in this context as it focuses more on the development of character and the virtues that should be pursued — approach that is not so fruitful in this specific and technology-centred issue.

Deontology is an ethical approach that focuses on duties and rules for actions as those define whether or not the action is ethical. Thus, the focus is on the intention of action, not in the outcome of an action — which is the case in the consequentialistic theories. Here we are focusing on Kantian Deontology as it is regarded to be the central theory for all deontological theories [34]. For evaluating ethicality of the action, Kant presented the Categorical Imperative that sets demands that ethical rules should be universal, rules must be followed voluntarily and we should always respect humans like Kant [35] stated: "*Act in such a way that you treat humanity, whether in your own person or in the person of any other, never merely as a means to an end, but always at the same time as an end*.". In the context of the IoT, the main points are that intention should be good and the individuals should be respected as ends themselves, not used as a mere tool (information source).

Consequentialism is the ethical approach where the evaluation of the ethicality of actions is based on what kind of outcome the action will provide. Utilitarianism (the classical consequentialist theory) is, simplified, the evaluation of different action possibilities by outcome utilities of those alternatives. The term utility refers to "the good" that is evaluated and it can be different in a different context. There are hedonic utilities such as pleasure, happiness, etc. Thus, the use of IoT should aim to act in such a way that the outcome would be resulting as much good as possible for all affected stakeholders and diminish negative ones. This means that only serving the advantage of a particular stakeholder cannot been seen as a justified ethical motivation, as we should seek benefits for all stakeholders and avoid the harm likewise.

4.2. Ownership Models

Different ownership models have been discussed since the beginning of the IoT era [36]. The perspective of ethical issues adds value to these ownership considerations and gives a more justified basis for those. The following is a foundational demonstration of the ownership distribution concepts. Different owners could be found but this is a simplified version of our preliminary analysis that can be conducted here. As Information collected by IoT devices varies so much that we need to analyse it at least from two different bases, what is the type of information and what ethical issues are rising with different models of ownership:

- The collector of information as owner
- The source of information as owner
- Hybrid model

The collector of information as owner is an approach where the work to be done in collecting can be argued to be a justification of ownership. This approach is commonly used to justify IPR [37]. This approach has also gained critiques as the current IPRs do not secure the artistic or intellectual work, but instead secure the corporate exploitation of IPRs. From the utilitarian perspective, if the collector of ownership produces the most good it is a justified approach, especially if the information is not personal.

The whole idea to collect information by IoT is compromised if the company does not gain ownership over it and thus the collected — non-personal information — should be owned by collector or the whole basis of IoT is derogated. From the deontological viewpoint it also seems unjustified to have a situation where the collector of such information does not gain the ownership to that information — it seems like an undesirable intention and rule.

However, the problem is that the benefits for the collector are most likely business-related and information can also contain personal data, which alters the situation. By personal data we rely on the definition by European Commission [38]: "*Personal data is any information that relates to an identified or identifiable living individual*." Additionally, personal data has personal value for people and it may differ based on the person and context of information [11,39], and thus there is no clear way to analyse the goodness in a consequential way. This ownership model neither is compatible with deontology as it limits the people's autonomy (control over their life—here information about them) and treats people as mere sources of data, not ends themselves. Thus, it seems that the ownership of personal information by the collector is not ethically acceptable in a case where information contains personal data of individuals as it objectifies people instead giving them the mastery over their personal information[10,11].

The source of information as owner. If we are collecting information from individuals it seems that the individual should be the owner. From a deontological perspective, it emphasises the autonomy of individuals as they gain more control through ownership. Likewise, it forces us to treat people as an end themselves instead of mere means to an end. As an example, from a deontological perspective, the ownership of patient information should be granted to patients, not the healthcare of health professionals [40]. The consequential approach still has the same problem of different valuation types as mentioned above and thus is more debatable.

If an IoT device is collecting data that is combined with personal data the question is more complex. If that information is separate, the question follows logic already presented, but handling mixed information is not straightforward. We give you one example, in which an astronaut collects information through the sensors attached to a spacesuit, which also contains the name of the astronaut. Is the collector NASA or the astronaut? And if we decide that the collector is NASA as the astronaut, is she/he in the role of an employee and is the information personal as it contains personal data related to the astronaut? This example shows that we may need a hybrid model where the ownership is split.

Hybrid model. We see that a hybrid model is needed for situations where IoT systems collect personal information that is combined with non-personal data. If non-personal information is not separable from personal data, it becomes personal data and should be treated as such. However, if data can be separated, also the ownership can be separated. In this situation, we could protect the benefits of both parties, the collector and the individual, and still retain ethical justification presented above. However, this sets demands for technology and protocols if we want to separate these. Likewise, it will be hard to define what data is personal and what is not in the context of IoT. This opens a new research area that needs to be investigated in the future.

5. Discussions

The suggested protocol modifications won't come without further and possibly unforeseeable implications and concerns. Firstly, if an existing protocol will be altered to meet the new functional requirements, consent from the protocol owner must be collected and the potential changes to intellectual property rights related to the protocol itself distributed righteously. Secondly, from a technical perspective, it must be clarified whether the protocol in question can be modified without compromising its performance and compatibility, as well as whether the IoT devices intended to utilise the updated protocol are capable of collecting, storing, and delivering the additional information.

These changes also affect the data ownership on the conceptual level. It must be decided whether the data ownership information should continue evolving and/or accumulating throughout its life-cycle based on the possible functional changes made by the re-users or to be attached only to the original owner. In a similar vein, we should consider whether the ownership could be transferred to a new individual or stakeholder if the original owner so decides.

Additionally, we must consider the consequences of possible malicious acts, such as unauthorised alteration of ownership information. For example, whether someone can steal the property or manipulate the data connected to identifiable persons in a way that will affect their professional or personal positions, especially considering the fact that the original owners will be connected to this information for the foreseeable future. To avoid or reduce the impact of these issues, it should be made possible for the data owners to decide whether they allow their names to be saved and distributed and if there is a way to add ownership information while retaining the owners' anonymity. A possible solution for addressing this issue could be an external service through which the ownership information is communicated anonymously, but with a unique ID.

The changes in the protocols will not have an impact without some changes even in the organisational routines. The handling of property information sets a minimum requirement for data management: the ownership fields will need to be filled with correct data and the data management practices will even have to make use of the ownership data, recognising situations where possible ethical conflicts arise. The changes in the routines need not be substantial, a mere adding of the ownership consideration in the data input and use/analysis stages of the data management cycle, guided by a simple set of rules or preferably some level of automation suggesting the correct handling could be the only change needed. However, as the amounts of data accumulate and the possible uses for it multiply, the organisational practices will have to cope with this added complexity.

Thus, we claim that while the introduced changes may appear rather clear on the functional level, their impacts on the whole IoT and the connected social ecosystems will be widespread and difficult to address thoroughly in a single study. Yet, the considerations presented above can already demonstrate that the implementation of the development ideas introduced in this paper will require a variety of both preparational and preventative considerations and actions, and should be studied to a further degree from both technical and social perspectives before proceeding to the concrete development phase.

6. Conclusions

While the concept of personal data has been addressed in the existing literature and by regulative authorities such as the European Union, the common understanding of the correct and just distribution of data ownership remains vague, especially in the IoT context. Regardless, preemptive measures regarding property-related conflicts can and should already be taken despite the lack of conceptual consensus.

For this purpose, we introduced a meta-data approach for retaining and communicating the data ownership information with and between all involved actors and stakeholders throughout the IoT data life cycle. The analysis was extended to the practical level by investigating the possibility to implement such practices while taking into account the functional limitations set by the currently available IoT protocols. As such, the outlook for the applicability of the suggested meta-data approach seems encouraging, however, it calls for fundamental changes to the existing protocols. Furthermore, even when the current protocols would allow the proposed parameter additions as is, performance-related challenges will potentially arise. This claim is rooted in the fact that in many cases the agility of IoT solutions relies partly upon the limited size of individual data packages, especially in the low bandwidth settings.

Thus, we encourage the proposals introduced in this paper to be taken into account in the long-term development of IoT protocols, as we see that the advanced data transfer capabilities will eventually trivialise the currently standing content restrictions, enabling us to not only deliver larger amounts of data in general, but also to implement a larger variety of parameters with little impact on performance. As a result, we claim that the introduced meta-data approach has the potential to enhance the common ability to avoid misconceptions and misuse related to data ownership, thus providing more sophisticated foundations for building both legally and ethically sustainable IoT solutions.

7. References

[1] Mason, R. O. (1986). Four ethical issues of the information age. *Mis Quarterly*, pages 5–12.

[2] Vermanen, M., Rantanen, M. M., and Koskinen, J. (2022). Privacy in internet of things ecosystems–prerequisite for the ethical data collection and use by companies. In *IFIP International Conference on Human Choice and Computers*, pages 18–26. Springer.

[3] Fadler, M. and Legner, C. (2022). Data ownership revisited: Clarifying data accountabilities in times of big data and analytics. *Journal of Business Analytics*, 5(1):123–139.

[4] Saha, H. N., Mandal, A., and Sinha, A. (2017). Recent trends in the internet of things. In *2017 IEEE 7th annual computing and communication workshop and conference (CCWC)*, pages 1–4. IEEE.

[5] Miorandi, D., Sicari, S., De Pellegrini, F., and Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad hoc networks*, 10(7):1497–1516.

[6] Vermanen, M. and Harkke, V. (2019). Findings from multipurpose iot solution experimentations in finnish smes: Common expectations and challenges.

[7] Ng, I. C. and Wakenshaw, S. Y. (2017). The internet-of-things: Review and research directions. *International Journal of Research in Marketing*, 34(1):3– 21.

[8] Mai, J.-E. (2016). Big data privacy: The datafication of personal information. *The Information Society*, 32(3):192–199.

[9] Vermanen, M., Rantanen, M. M., and Harkke, V. (2019). Ethical challenges of iot utilization in smes from an individual employee's perspective.

[10] Hakkala, A. and Koskinen, J. (2022). Personal data protection in the age of mass surveillance. *Journal of Computer Security*, 30(2):265–289.

[11] Koskinen, J. (2019). The concept of datenherrschaft of patient information from a heideggerian perspective. *Journal of Information, Communication and Ethics in Society*, 17:336–353.

[12] Koskinen, J., Kainu V. & Kimppa K. (2016) The concept of Datenherrschaft of patient information from a Lockean perspective. *Journal of Information, Communication and Ethics in Society*, 14(1), 70-86.

[13] Banterle, F. (2020). Data ownership in the data economy: a european dilemma. In *EU Internet Law in the digital era*, pages 199–225. Springer.

[14] Hummel, P., Braun, M., and Dabrock, P. (2021). Own data? ethical reflections on data ownership. *Philosophy & Technology*, 34(3):545–572.

[15] Janeˇcek, V. (2018). Ownership of personal data in the internet of things. *Computer law & security review*, 34(5):1039–1052.

[16] Weber, R. H. (2010). Internet of things–new security and privacy challenges. *Computer law & security review*, 26(1):23–30.

[17] Conger, S., Loch, K. D., and Helft, B. L. (1995). Ethics and information technology use: a factor analysis of attitudes to computer use. *Information Systems Journal*, 5(3):161–183.

[18] Hyrynsalmi, S. (2014). *Letters from the War of Ecosystems — An Analysis of Independent Software Vendors in Mobile Application Marketplaces*. Doctoral dissertation, University of Turku, Turku, Finland. TUCS Dissertations No 188.

[19] Koskinen, J., Rantanen, M. M., Kimppa, K. K., and Hyrynsalmi, S. (2017). Ecosystem ethics: An ethical analysis of orchestrators' ultimate power and the dilemma of ecosystem ruling. In Suominen, A., Jud, C., and Bosch, J., editors, *IWSECO*, pages 43–54.

[20] Goasduff, L. (2019). Gartner says 5.8 billion enterprise and automotive iot endpoints will be in use in 2020. https://www.gartner.com/en/newsroom/pressreleases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io. Accessed: 2020-02-02.

[21] Begg, C. and Caira, T. (2012). Exploring the sme quandary: Data governance in practise in the small to medium-sized enterprise sector. *The Electronic Journal Information Systems Evaluation*, 15(1).

[22] Desouza, K. C. and Awazu, Y. (2006). Knowledge management at smes: five peculiarities. *Journal of knowledge management*, 10(1):32–43.

[23] Ancarani, A., Di Mauro, C., Legenvre, H., and Cardella, M. S. (2019). Internet of things adoption: a typology of projects. *International Journal of Operations & Production Management*.

[24] Palmirani, M., Martoni, M., Rossi, A., Bartolini, C., and Robaldo, L. (2018). Pronto: Privacy ontology for legal reasoning. In *International Conference on Electronic Government and the Information Systems Perspective*, pages 139–152. Springer.
[25] Nissenbaum, H. (2018). Respecting context to protect privacy: Why meaning matters. *Science and engineering ethics*, 24(3):831–852.
[26] Rocher, L., Hendrickx, J. M., and De Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature communications*, 10(1):1–9.
[27] Karagiannis, V., Chatzimisios, P., Vazquez-Gallego, F., and Alonso-Zarate, J. (2015). A survey on application layer protocols for the internet of things. *Transaction on IoT and Cloud computing*, 3(1):11–17.
[28] Kothmayr, T., Schmitt, C., Hu, W., Bru¨nig, M., and Carle, G. (2013). Dtls based security and two-way authentication for the internet of things. *Ad Hoc Networks*, 11(8):2710–2723.
[29] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, 17(4):2347–2376.
[30] Malgieri, G. (2016). 'ownership'of customer (big) data in the european union: Quasi-property as comparative solution? *Journal of Internet Law*, 20(5).
[31] McKeon, R. (1938). The development of the concept of property in political philosophy: a study of the background of the constitution. *Ethics*, 48(3):297– 366.
[32] Waldron, J. (1990). *The right to private property*. Clarendon Paperbacks.
[33] Tavani, H. T. (2005). Locke, intellectual property rights, and the information commons. *Ethics and Information Technology*, 7(2):87–97.
[34] Alexander, G. S. and Pen˜alver, E. M. (2012). *An introduction to property theory*. Cambridge University Press.
[35] Kant, I. (1970). Grundlegung zur metaphysic der sitten [several translations used; main translation: Liddel b. kant on the foundation of morality-a modern version of the grundlegung]. *Indiana: Indiana University Press (1785/1970)*.
[36] Mashhadi, A., Kawsar, F., and Acer, U. G. (2014). Human data interaction in iot: The ownership aspect. In *2014 IEEE world forum on Internet of Things (WF-IoT)*, pages 159–162. IEEE.
[37] Fromer, J. C. (2012). Expressive incentives in intellectual property. *Virginia Law Review*, pages 1745–1824.
[38] European Commission (2020). What is personal data? https://ec.europa.eu/info/law/law-topic/data-protection/reform/whatpersonal-data$_e$*n.Accessed* : 2020 − 02 − 02.
[39] Wagner, A., Wessels, N., Buxmann, P., and Krasnova, H. (2018). Putting a price tag on personal information-a literature review. In *Proceedings of the 51st Hawaii International Conference on System Sciences*.
[40] Koskinen, J. and Kimppa, K. K. (2016). An unclear question: who owns patient information? In *IFIP International Conference on Human Choice and Computers*, pages 3–13. Springer.