Ethical framework for IoT deployment in SMEs: individual perspective

Mikko Vermanen, Minna M. Rantanen and Ville Harkke
University of Turku, Turku, Finland

Received 31 August 2019
Revised 30 September 2020
15 August 2021
Accepted 17 August 2021

Abstract

Purpose – This study aims to investigate the ethical issues related to the internet of Things (IoT) deployment in small- and medium-sized enterprises (SMEs) from an individual employee's perspective. To provide researchers and practitioners with concrete tools for examining these matters, an ethical framework dedicated to IoT is introduced.

Design/methodology/approach – First, the applicability of Mason's original privacy, accuracy, property and accessibility (PAPA) framework is studied in the IoT context. Second, issue category additions are proposed based on the identified coverage limitations of PAPA.

Findings – While the original PAPA framework can be utilised as a generic ethical evaluation tool, it lacks coverage of several IoT-specific issue areas. To thoroughly address the ethical risks associated with IoT, two additional categories are introduced.

Research limitations/implications – The new framework requires further validation to ensure its applicability and to identify potential modification requirements in continuously evolving IoT ecosystems.

Practical implications – Considering the lack of ethical IoT frameworks, this study provides organisations with a practical framework for analysing the ethical issues in IoT deployment.

Social implications – Ethical standards for IoT have not been sufficiently addressed in the current literature and frameworks, making the ethical considerations dependent on subjective stances. Thus, there is an acute demand for a practical framework that outlines the general ethical standards, helping its users to thoroughly address the potential ethical issues.

Originality/value – While the use of IoT keeps growing in SMEs, there is an apparent lack of ethical guidelines. This study contributes to the gap by introducing a preliminary framework for both practical use and further theoretical development.

Keywords Ethics, Internet of things, Small- to-medium-sized enterprises, PAPA

Paper type Research paper

1. Introduction

The Internet of things (IoT) is a relatively new and rapidly evolving platform for technical development, enabling its users to observe and measure various material and immaterial targets based on collected digital information. As the number of encouraging examples of successful IoT implementations keeps growing and the price level of the solutions declines, even small- or medium-sized enterprises (SMEs) are starting to introduce IoT to their businesses (Vermanen and Harkke, 2019). While there are numerous benefits to be achieved with IoT solutions, some potential risks are involved as well. Due to SMEs' size and related resource limitations (Hoyer *et al.*, 2006), both benefits and risks differ from those of large enterprises. In this study, we will examine these risks mainly from an individual employee's standpoint. More specifically, our focus will be targeted towards the ethical factors to be considered when implementing and utilising IoT solutions in SMEs. Ethical issues related to

Internet Research
Vol. 32 No. 7, 2022
pp. 185-201
Emerald Publishing Limited
1066-2243
DOI 10.1108/INTR-08-2019-0361

the utilisation of IoT have rarely been examined, especially from the perspective of employees of SMEs. Due to the anticipated benefits and the potential risks, ethical implications for these stakeholders should be considered. However, there is also a need to find practices that guide the ethical utilisation of IoT in SMEs. Thus, in this study, we provide a framework to navigate towards ethical practices.

The European Commission defines SMEs as companies with less than 250 employees, an annual turnover of under 50 million euros or an annual balance sheet total of 43 million euros (Hoyer *et al.*, 2006). SMEs represent the majority of companies worldwide (Desouza and Awazu, 2006), and based on Eurostat's analytics from September 2015, they represent at least 97.5% in most European countries. The SME sector provides an interesting object for our study, as the companies tend to be managed in a rather unstructured and heterogeneous manner (Storey, 2016; Martin and Staines, 1994), which is likely to affect their approach to IoT as well. The SMEs are a special case in their handling of both technology and data. Previous studies have indicated that once introduced to the opportunities provided by affordable IoT solutions, SMEs can identify potential practical benefits and use cases to proceed to the concrete implementation phase in an agile manner (Vermanen and Harkke, 2019). However, while a fast and linear approach may provide instant benefits, the potential lack of planning gives reason to question whether sufficient investigation regarding risk factors occurs – including the ones of ethical nature. One of the factors limiting the actions of SMEs is naturally the lack of resources – financial, knowledge and personnel. This has, in its part, led to the creative use of the tools available as well as dependence on solutions procured from outside. The tools used for handling data tend to be traditional and the practices used are not necessarily specifically intended for managing information but serve some intertwined purposes (Cerchione and Esposito, 2017). Furthermore, the practices often evolve on an ongoing basis, and the principles are not explicitly defined (Begg and Caira, 2012). This further supports our view that convenient, context-specific practical tools and methods could provide SMEs with a better basis to operate in a more deliberate manner. What makes this setting interesting is that while the produced framework needs to cover the relevant ethical aspects thoroughly, it also has to be formulated considering the companies' potential lack of technical knowledge, resources and independent planning capabilities.

Another specific and relevant attribute of the SMEs is the people-centred knowledge management style; much knowledge in the organisation is distributed socially or as common knowledge (Desouza and Awazu, 2006) as opposed to the formal and documented approach. These attributes influence the SMEs' ability and motivation to handle ethical questions in their data and information systems and practices.

The internal processes and ethical behaviour in SMEs may not always be in compliance with the common ideals and best practices when it comes to the relationship between IoT solutions and employees. Due to the different characteristics of SMEs as organisations and IoT as a specific form of information technology, there is a need to consider their ethical issues together. Currently, few studies have been conducted within the SME context about ethical issues of IoT. Thus, our study is the first attempt to ignite further interest in examining and defining ethical best practices of IoT deployment in the SME environment. This study aims to provide a theoretical and practical basis for discussion about the implementation of IoT in SMEs. This study will first familiarise the reader with the meaning and purpose of IoT solutions, after which some of the most important ethical challenges will be addressed into four interest areas originally introduced by Mason (1986): privacy, accuracy, property and accessibility. Finally, the contributions of this study are to analyse the aforementioned areas' capability to cover the ethical challenges relevant to the IoT and share our customisation proposals to construct an updated model aimed to better serve its purpose in the IoT environment. Consequently, we will produce a preliminary framework of ethical challenges related to IoT solution deployment in the SME environment, which could also serve as a basis

for negotiating a social contract for the future use of IoT. The framework aims to support, complement and guide the implementation and development of data management models and practices for IoT usage.

2. Background: Internet of things

On a high level, the still rather ambiguous concept of IoT (Wortmann *et al.*, 2015) can be described as a network binding together the end-users and different monitorable or measurable entities or targets, ranging from physical objects, such as buildings and vehicles (Miorandi *et al.*, 2012), to immaterial interests, for instance, collective traffic and consumer behaviour (Gubbi *et al.*, 2013). The link between the actors in the IoT ecosystem is the information gathered from these targets and delivered to the end-users in a comprehensible form (Jin *et al.*, 2014). The added value achieved from the data produced by IoT solutions can appear in many forms, including personal, professional and economical, and can serve as a multiplicity of groups or actors, including academia, industry and government (Khan *et al.*, 2012). By utilising modern IoT solutions, companies can aim for higher performance and reduced manual labour through more efficient and accurate data collection capabilities. Through encouraging success stories and developing usability, reliability and affordability, even the less technologically oriented and smaller companies are able to implement these solutions into their daily practices (Vermanen and Harkke, 2019). Combined with the aforementioned unique characteristics and limitations of SMEs and the lack of practical tools supporting them to conduct ethically sustainable IoT implementations, we aim our focus towards the SME sector.

IoT solutions can simultaneously bring along various risks related to the privacy and safety of their users. Referring to Conti *et al.* (2018), the safety of every IoT device, sensor and unit of information can become increasingly compromised, partly due to the vulnerabilities resulting from the rapid growth of IoT, where the security measures may not keep up with the risks (Giaretta *et al.*, 2016). These issues can have significant consequences from an individual's perspective, as IoT solutions often collect identifiable data related to, as stated by Lee and Lee (2015), an individual's location and movements, health conditions and purchasing preferences. However, they continued to state that the consequences of heightened privacy protection may not be solely positive, as this can limit the benefits that could be achieved from IoT solutions, which rely upon the collected data and its availability. This leads us to an intersection where a satisfactory balance between the individuals' and organisations' benefits and needs has to be achieved. Considering the vastness of the IoT ecosystems, including the involved hardware, software, networks and inter-organisational actors, we face a level of complexity difficult to comprehend even by the large companies and dedicated experts, let alone the SMEs – not only from the technical but also the social standpoint. Hence, we must acknowledge that building an all-encompassing, yet not exhaustive or unusable, ethical framework is not a realistic expectation. Rather, our goal is to provide understandable guidelines on an abstraction level that fits the purpose of remaining practical.

3. Ethical challenges of IoT

Ethical issues of the IoT have not gained much attention despite the vast interest in the ethicality of information technology in general (Royakkers *et al.*, 2018). While regulations, and perhaps most notably, the General Data Protection Regulation (GDPR), do protect the rights and privacy of individuals, we claim that to thoroughly address and comprehend the nature and role of ethics in IoT ecosystems, more fundamental and principled ethical guidelines are needed. It must be acknowledged that the ethicality of technology depends on many issues, such as the nature of the technology, the context of its use and its potential implications. Thus, ethics and especially applying it to information technology requires careful analysis

context, and there are no "one-size-fits-all" solutions. There are several tools and methodologies that are designed to help in the ethical design of technologies. For instance, Ethics Canvas (Reijers *et al.*, 2018) is a simple tool that could be used to map potential ethical concerns in projects. Similarly, there are more complex methodologies, such as Value Sensitive Design (Friedman *et al.*, 2017), which focus on moral values and ethics in technology design. These tools and methodologies could, of course, be used in the ethical design of the IoT. However, in this study, we focus on ethical considerations related to IoT in the context of SMEs. Thus, there is no specific instance of IoT to evaluate or develop with the stakeholders.

In practice, some existing frameworks for implementation of the IoT consider ethical issues at the general level. However, there is a lack of a comprehensive ethical framework that is grounded in actual ethical considerations rather than just best practices. This could be considered the formation of the ethically justified social contract of the "good" use of IoT. As Mason, one of the first contributors to the ethics of technology, stated:

> "Our moral imperative is clear. We must ensure that information technology and the information that it handles are used to enhance the dignity of mankind. To achieve these goals, we must formulate a new social contract, one that ensures that everyone has the right to fulfil his or her own human potential" (Mason, 1986, p. 11).

In 1986, Mason (1986) published an issues and opinions piece in the MIS Quarterly and drafted a framework for formulating a new social contract that ensures individuals' right to fulfil their human potential. He argued that we have entered the era of the information age, which brings forth unique challenges that should not be neglected if we want to ensure that the society that is created is what we want. Mason noted that these challenges stem from the nature of the information itself and how it affects the building of intellectual capital. He saw that building social capital is vulnerable in many ways in the information age and we should be prepared to tackle challenges that pose a threat to human dignity.

Although Mason's work is decades old, it is still a good starting point for consideration of ethical issues of information technology despite the rapid changes. Changes bring forth unique challenges that could be easily neglected, although they should be considered carefully if we want to ensure that technology enhances mankind. As SMEs have more limited resources to consider the ethical issues of the IoT, we argue that there is a need for a framework of ethical issues of IoT's unique characteristics in SMEs. We start the development of this framework from Mason's work, as it provides a simple and still relevant categorisation of ethical issues of information technology.

Mason (1986) focused on four ethical issues that information age creates: privacy, accuracy, property and accessibility – often summarised as an acronym PAPA. Notably, although PAPA divides ethical issues into four categories, these categories are partly overlapping. Thus, one issue can be ethically problematic from multiple perspectives. Similarly, Mason was not claiming that these four are the only ethical issues in the use of information and communication technology. Mason's PAPA has later been contested and complemented, but in this study, the original version of PAPA is leveraged as the foundational framework due to its more widely proven validity. By investigating the phenomena through these four categories, we aim to develop our understanding of not only the original categories' applicability in the IoT context but also their sufficiency regarding coverage. Based on this understanding, we propose two PAPA expansion categories: motivation and security.

3.1 Privacy

The first category of ethical issues of information age presented by Mason is privacy (Mason, 1986). Information privacy is generally understood as a right to seclude information about oneself. Assuring privacy means that one should have a right to determine whether, when,

how and to whom one's personal information is to be revealed (Mason, 1986; Smith *et al.*, 2011). Lately, privacy issues related to information technology have attracted much interest from policymakers. For example, the European Union is enforcing one's right to privacy through the General Data Protection Regulation Act, which has affected the ways that personal data can be collected and used, for instance, by organisations (The European Parliament and the Council of the European Union, 2016). Currently, the European Union is preparing a proposal for the ePrivacy Regulation Act that aims to regulate, for example, online marketing (European commission, 2017).

Mason (1986) described privacy as an ethical issue that revolves around questions, such as what information should be revealed, under what conditions and with what safeguards? Similarly, questions about the right not to reveal information or forcing people to reveal some information are at the core of privacy. Mason saw privacy being threatened by technological advances that make it possible to gather more data, simultaneously increasing the value of information in decision making (Mason, 1986). Both of these are in close relation to IoT. IoT is a piece of technology that makes data gathering easier and more efficient and can be utilised as a tool supporting decision making. Thus, ethical issues regarding privacy must be considered carefully.

One of the most significant privacy threats is the growth of information technology, including the developed surveillance, communication, computation, storage and retrieval capabilities (Mason, 1986). Although IoT is not designed to be a surveillance tool in a traditional sense, it makes it possible to gather much data that can threaten the privacy of an individual. There are examples of smart devices, such as TVs, that gather audio to "approve services" without proper permission from the users, invading the privacy of the users without their knowledge of it (Royakkers *et al.*, 2018). This shows that the invasion of privacy is not always dramatic or noticeable, as Mason (1986) noted. Such cases indicate that as IoT is often rather invisible, it must be assured that the individuals with whom the data are collected are aware of the data collection and willing to be observed.

Many privacy issues regarding IoT in SMEs arise from the nature of data collected. If the information is in direct relation to individual employees, it can violate their privacy. Although the information of individual employees can be seen as a valuable asset for the company, it must be considered whether it is really worth the trade-off, since it could mean the endangerment of employee's privacy. Since privacy is the right of an individual, gathering and using data about individuals should only be done if the individuals give their permission (Kainu and Koskinen, 2012). This means that the individual employees should thoroughly understand what data is collected, how it is used and stored and for what purpose before giving their informed consent.

In SMEs, the individuals with the highest controlling power over the use of IoT, typically CEOs, commonly have the ability to decide what information gets collected and processed, as well as how the use and storage of data are explained to the employees. However, individual employees may not have the authority to control what information related to their work will be collected, except for what is set by law. However, whether an average SME employee can be assumed to possess a thorough understanding of one's legal rights in the context of IoT is questionable. Combining this with the immaturity of IoT security measures and regulations, there is a high possibility that privacy-related misuse exists.

It must also be noted that in SMEs, where there are fewer people working, using IoT to gather even general data can lead to privacy loss. When a sensor-based IoT solution collects temperature data from a storage space, there is usually no risk to privacy based on the data that is gathered, whereas other types of data are more likely to form a privacy risk. Subjective interpretation of such seemingly anonymous data can endanger the privacy of employees because of the existing knowledge of the people viewing the data. For instance, when a vehicle tracking solution collects data related to route selection and driving habits, there is a

high possibility that the driver can be identified and observed. As an example, in our previous study, a Finnish car rental company deployed an IoT device to track the location of their vehicles. Drivers were informed about this procedure by the company and their motivation behind it, but some drivers ended up disconnecting the device once they entered the vehicle to protect their privacy (Vermanen and Harkke, 2019).

One of the few ways to gain visibility and control over whether ethical values are respected could be adding transparency, where the employees can access all the collected data about themselves and be aware of what is collected and how it is being used and by whom. However, as pointed out, information has become an increasingly valuable resource for decision-makers, and it can be seen as more valuable than the protection of employees' privacy. This could encourage the misuse of sensitive information. To avoid potential misconceptions and conflicts, we strongly encourage companies to collect the employees' informed consent before any data is collected or distributed.

3.2 Accuracy

The second ethical issue of Mason's framework is accuracy. He described it with questions about responsibility for authenticity, fidelity and accuracy of information and questions about accountability for errors and harmful events. Mason's definition of accuracy includes both system accuracy and information accuracy, and he highlighted that it should be the developers' responsibility to ensure that errors are avoided (Mason, 1986). However, as technological systems are becoming increasingly complex, questions relating to responsibility are becoming more complex as well: they are no longer matters of data accuracy, but of the accuracy of the whole socio-technical system.

Lately, these kinds of questions have often been handled under the topic of accountability. Accountability of IoT has raised many discussions due to the nature of IoT being a ubiquitous and autonomous "system of systems" (Brill and Jones, 2016; Singh *et al.*, 2018). Since accountability is often based on laws, it is not surprising that many authors have addressed the legal dimensions of IoT and accountability as obligations and liabilities (Brill and Jones, 2016; Singh *et al.*, 2018; Kirtley and Memmel, 2018). Although what we should do or not is stipulated in the law, they do not frequently follow ethical considerations.

Accountability is also often seen as something that incorporates challenges regarding governance and responsibility, privacy and surveillance and safety and security (Singh *et al.*, 2018). Thus, it overlaps with Mason's other categories. Singh *et al.* (2018) stated that questions of accountability of IoT revolve around who should be held accountable for the way that the system of systems works as it should and that it is used as it is designed to. Since IoT can also be used as a piece of surveillance equipment, it should be balanced with actions, such as empowering individuals regarding their personal data use and by making data transfer and usage more transparent.

Assuring safety and security is important since failures can occur and can lead to physical harm (Singh *et al.*, 2018). Thus, accountability regarding IoT is a question of who is held responsible for the system working correctly and without creating harm. This is especially important in cases where autonomous systems have physical manipulation capabilities. The issues surrounding physical manipulation have been discussed extensively in the field of robotics (e.g. Kernaghan, 2014). In an SME with limited resources and limited division of authority, the responsibility may lie on a single employee or a small group, and they should be aware of the risks.

Another concern is whether the collected information is correct and accurate enough to be relied upon. Storing, processing and releasing erroneous information related to an employee's actions may put the individual's professional and personal position at risk. As an example, a sensor-based IoT solution may track the employee's movements while travelling with a

company vehicle. If in this case, the location sensor gives incorrect values, indicating that the employee has not followed the agreed route or not moved at all, the employer might draw false conclusions, leading to unfounded trust issues. It also should not be ignored that in many cases, it is possible to manipulate the collected IoT data, which provides an additional opportunity for abuse. As a whole, it cannot be assumed that the information provided by IoT solutions is always reliable, and thus data-based conclusions should be made with caution. Based on these remarks, acknowledging the possibility of inaccurate or even false information is crucial to utilising the IoT solution output responsibly and making justified conclusions.

Finally, data accuracy also plays a significant role in avoiding personal discrimination resulting from misused or misinterpreted information. Not only should the employees be aware of and able to control the data collection and distribution, but they should also be protected from discrimination based on erroneous or unethically collected data. That said, discrimination can appear in multiple forms. Some of the most important risk factors to consider are that IoT solutions often enable collecting and combining data that is professionally irrelevant, yet allow the observer to practice profiling (Wachter, 2018) and draw personal conclusions about the observed individuals. Any data that can be interpreted as crossing the border between professional and personal (Oriwoh *et al.*, 2013) is not encouraged to be used in decision-making when its accuracy cannot be fully verified.

3.3 Property

The third category of ethical issues in Mason's PAPA is property. In this case, property refers to questions of ownership. Mason (1986) clarified the issues of this category through questions, such as who owns the information? What are the just and fair prices for its exchange? Who owns the channels through which the information is transmitted and how the access should be allocated? As data has become increasingly valuable and IoT technology can create and collect it even more efficiently, the questions of data ownership and collection should be considered.

However, the questions around data and information as property are rather complex, since data or information do not share the characteristics of physical property. As Mason (1986) stated, information can have many values, and it can be costly to collect but easy to reproduce and transfer. Since information can be replicated without destroying the original information, it makes it hard to safeguard. Although there are many institutions and regulations that aim to protect data and information, such as intellectual property rights and lately attempts to protect individuals' rights to their own personal information, IoT raises many ethical challenges due to its nature of collecting data at a fast pace and vast amounts.

The ownership of information is a rather intangible question, and there have been attempts to reformulate the concept. For example, Kainu and Koskinen (2012) introduced a concept of mastery over data (Datenherrschaft) that could be used instead of owning. Their idea is that an individual should have the mastery to decide about the use of their data and to whom they wish to share it (Kainu and Koskinen, 2012). Later, Koskinen (2016) proved from four ethical perspectives (Locke, Kant, Heidegger and Rawls) that mastery over data is an ethically justified way to address data ownership. Although originally developed for the context of patient information, the concept can also be used in other contexts. It must be acknowledged that the concept is not absolute (Koskinen, 2016), and there are situations where mastery over data can be overwritten (Hakkala, 2017). Despite, as a concept, the mastery over data helps to clarify the issues regarding ownership of data or information.

But who has the ownership or the mastery over data regarding IoT? First, data can be stored on either internal or external servers. In the first case, the distribution of ownership and mastery is likely quite simple to manage and understand but becomes more complex

once an external actor or organisation gets involved. This multi-organisational environment brings along several property-related questions, such as, for what purposes and by whom can the data be used? What can be collected and stored and how can the SMEs deploying the IoT solutions gather knowledge about what information will be collected? Considering the employees' standpoint, it is equally important to clarify approval-related matters. More specifically, how the consent of the monitored personnel should be acquired, considering the ethical risk factors. Regarding the data itself, clear rules should exist about whether the collected data are for business purposes and, if so, by who and for what price.

The data collected by IoT solutions can be stored in servers for various purposes, such as observing the value trends or post-processing the collected data. From the employee's standpoint, it is important to be aware of who owns the data, how long it will be stored, and who will be responsible for its disposal. Additionally, the employee should be aware of one's right to store, process and utilise the same information, or to set limits for the same actions by an external actor. Overall, keeping the employee informed about property-related matters is likely to help avoid and prepare for possible ethical conflicts.

3.4 Accessibility

The fourth category of ethical issues addressed by Mason (1986) is accessibility. This category is all about what information a person or an organisation has the right or privilege to obtain, under which conditions and with what safeguards. Mason (1986) related access to information to literacy, since it has been the main way of gaining information. However, he also highlighted that to truly have access to information, one should have both the means and skills to access the information. Thus, accessibility is a matter of both restraining and giving access. The ethical aspects arise from the questions of how, when and to whom access is given. However, since information can be seen as a valuable property of an organisation or as something that should be shielded due to privacy risks, questions about accessibility become more complex.

Accessibility can be linked to the other three focus areas, perhaps most closely to privacy, whose degree is partly dependent on how the data accessibility has been managed. Thus, it should again be made clear to the employees who have the right to access their personal data and what it will be used for. The more thorough the communication about information sharing is, the more likely potential conflicts can be avoided. An equivalently important factor is the level of safety measures, ensuring that the data can only be accessed by the intended individuals. As seen regularly in the media, information leakages can have dramatic consequences not only for individuals but also for companies which in the SME sector tends to depend on the loyalty of a rather small group of customers and employees. Even the seemingly minor issues can accumulate to large issues, especially when these leakages concern the private information of individuals.

How the access rights and the safety of data are managed can be seen as the management's responsibility. In case the management does not have the required tools or knowledge to ensure thorough consideration of the mentioned factors, it should consult a service provider or another external party capable of carrying out the needed actions. The potential risks in this category are widespread, covering areas such as general device security, communication security, network security and application security. Thus, the safety-ensuring party should be selected carefully and responsibly to avoid any foreseeable issues. Overall, the idea behind this is that the ethical principles and responsibilities do prevail whether their fulfilment can be ensured independently.

4. Ethical considerations of IoT through the PAPA model

This chapter analyses the coverage of the standard PAPA model in the IoT context, introduces an expanded revision of the PAPA model and analyses whether it could provide a more suitable basis for investigating the ethical challenges based on the readily identified challenge areas.

To clarify the implications of the PAPA in SMEs, we have categorised the implications as follows: the issues may directly affect an individual employee, the organisation or the society. The effect on the organisation is further divided into three sub-categories: general management, data management and communication, according to which specific function of IoT usage the implications affect. The owner-managers considerably control these implications for the organisation; their personal understanding of the issues is critical as they can form these when desirable, and as stated by Fassin *et al.* (2011, p. 425), "*The small-business owner-manager is able to shape the corporate culture and to enact values other than profit*".

The mentioned challenges are just a subset of all ethical factors requiring consideration while deploying IoT solutions in SMEs. Knowledgeably, many of these challenges are applicable in more than one of the four categories, and thus their interrelation will require further investigation. In the revision, we will address this issue by examining whether a category expansion can enable more fluent challenge distribution. Table 1 includes the ethical challenges pointed out in the PAPA model, its purpose being to provide sufficient understanding on which ethical matters can already be evaluated without model customisations.

In Table 1, we have grouped the ethical issues according to the main subject of the considerations. The implications of the ethical considerations are not solely about the responsibility of the owner/manager of the company but can affect numerous levels from a single individual employee to society.

5. The expanded PAPA model

As stated earlier, the original PAPA model manages to cover many of the currently identified ethical challenge areas relevant to IoT. However, IoT ecosystems possess characteristics whose thorough investigation requires a wider issue categorisation. Some useful approaches have been introduced in the earlier literature, which will be leveraged in the expanded model. Like the ones introduced by Mason (1986), the added categories are partly intertwined with the others, aiming at creating a more defined focus area distribution while maintaining a logical continuum.

5.1 Motivation

One significant gap in the PAPA model is the lack of focus on stakeholders affected by or solving these ethical dilemmas. Although harms are mentioned in many of the categories, there is little consideration on intentions and possible potential consequences of unethical actions. For example, Conger *et al.* (1995) have empirically studied ethical attitudes about computer use. Their study confirmed that Mason's themes are valid and that motivation is an equally important factor and extends Mason's themes towards consideration of stakeholders. Motivation is used to describe the ethicality of actions depending on who benefits and who suffers from the actions, thus focusing on the consideration of others, such as beneficiaries and victims of unethical acts and personal motivations (Conger *et al.*, 1995).

Although Conger *et al.* (1995) studied ethical attitudes, thus limiting their view on moral judgments, their study emphasises the need to consider motivations behind IoT use in SMEs. It is clear that in cases where IoT is used unethically, employees easily become victims if the

	Privacy	Accuracy	Property	Accessibility
Implications for an individual employee	Does the employee have the ability to control what, how, when and why data is collected and/or distributed?	Can inaccurate data and/or false interpretations endanger the employee's professional position and/or personal life?	How is the ownership of data shared inside the organisation?	Who can view, edit or delete the data?
	Can data be combined and attributed to a specific person within an SME?	Who can be held accountable for the accuracy and trustworthiness of the data?	Could the ownership of data be substituted or replaced with mastery of data?	Does the employee have control over who has the access to data?
Implications for general management	Has the management collected informed consent for data collection and distribution from the monitored employees?	Can the data or its interpretation cause discrimination or inequality?	How does the organisational culture view the ownership issue?	Has the management studied and defined the data accessibility principles when deploying the solution?
Implications for data management	What information is revealed to external second/third parties?	How is the data accuracy maintained in processes?	Where, and for how long will the data be stored?	How are the access rights defined and shared between different users?
	How is the data protected and who is responsible for the protection?	Has the data been secured from manipulation?	Who is responsible for the disposal of data?	How should the level of privacy and usage of data be balanced?
Implications for communication	How is the functionality of the solution explained to the individuals and can they give an informed consent based on this information?	What kind of consequences are related to the possible inaccuracy of data?	How are the individuals informed about their rights to the data and the ownership of data?	How has privacy been considered?
				How is the safety of information ensured?
Implications for the regulatory environment and society	What laws and regulations enhance or decrease the employee's privacy and how?	Who can be held accountable for the physical actions of independent systems?	How does the involvement of multiple organisational stakeholders affect the ownership?	Will the data access be monitored and regulated?
	Do the current laws and regulations support or hinder following good ethical principles?		Can the data be monetised, by whom and for what price?	

Table 1.
The main ethical considerations for IoT usage in an SME based on the original PAPA model

actions can cause them harm. For example, discrimination, breaches of privacy or even risk of physical harm can victimise employees, although they can benefit their employers. However, employees can become beneficiaries if unethical actions are avoided since IoT can potentially

change work in a more meaningful direction by automating tedious data collection. Benefits should also include financial advantages besides immaterial benefits. Considerations of benefactors and victims should also be extended to other stakeholders, such as customers, business partners, etc., although we focused only on the employees in this study.

Personal motivations or intentions also affect the ethicality of actions in the IoT use. Mason (1986) did not clearly distinguish between intentional and unintended harm, although in reality, these can be separated. Intentional harm without greater good as a consequence is with no doubt an unethical action, whereas unintended harm can be judged either as good or bad action. It is clear that collecting data with IoT to cause harm to others is not ethical. However, more intriguing ethical dilemma is avoidance of unintentional harm. Unintended harm is not merely a question of not meaning to do harm, but whether the harm could have been avoided. Thus, the question is, how can IoT be used in SMEs without producing unintended harm towards employees (or any other stakeholder)?

The role and motivations of management (or similar actors who control the use of IoT) should always be taken into account when considering the ethical risks involved in IoT deployment. To provide any benefits, IoT solutions must gather data to which individuals and their actions are often somehow connected. Supported by Mason's (1986) statements, situations in which the value of this data is particularly high do pose a serious risk to the monitored individuals, as this can make it tempting for the management to seek and use questionable approaches to gain maximal benefit. This can ultimately lead to situations where data is collected without the employees being aware of the procedure (Atzori *et al.*, 2010), let alone giving their consent. Yet, notably, even the management may not always be aware of or able to control these ethical risks; thus, it can be debatable whether they can be held responsible. We claim that this phenomenon is even more emphasised in the SME sector, where the companies' technical and legal capabilities are typically held up by a limited group of people, whereas in large corporations, those areas tend to be managed by dedicated personnel.

To gain the most benefit from utilising this issue category, motivations should be examined by involving each relevant stakeholder and/or group involved in the IoT ecosystem. This is because the added value of including motivational aspects in the analysis is based on widening our perspectives to the whole organisation, thereby understanding and locating the interactional factors behind the ethical conflicts. This helps us to understand the social structure behind the ethical problems, making it easier to discover their origins and understand how and by whom they can be avoided or corrected.

5.2 Security

Another significant gap when applying the PAPA model to IoT is the lack of focus on employee security. To fill this gap, we propose a new "Security" category to be added to the model. Security should be considered a practical expansion to the "Implications for the regulatory environment and society" category, including the challenges currently situated in less optimal categories and pointing out the matters related to securing the employees' rights and position within the organisation. First, we find it crucial to specify what employment-related actions employers are able to take based on the data collected with IoT solutions. Also, this category will offer a deeper insight into the possible issues related to the invasiveness of the data collection.

Whether the information collected from individuals can be trusted on a technical level (see 3.2), the ethicality of making personal conclusions or profiling based on data is questionable. Laws and regulations set certain boundaries for how an employer can utilise this information in decision-making. However, the actions being allowed by law alone do not ethically justify decision-making where the employee's personal position is at risk. In such cases, collecting

the employees' informed consent is again a mandatory step defining the degree of mutual understanding and agreement. If an employee is only aware of data collection and deployment from a business perspective with no indication of personal consequences, it would be highly unethical for the employer to weaken the employee's position, or in extreme situations, terminate their employment. Even if the employee is made aware of such an approach, the situation remains ethically complicated. Unless ethical standards in this matter have been clearly defined and thus rely purely on regulatory limitations, there is an apparent loophole that will eventually only benefit the employer.

Following this logic, the employers would be able to weaken the employee's security by continuously adding new monitoring solutions, which are correct from a regulatory perspective but against the employee's ethical rights and safety. Being continuously monitored and measured, and thus driven towards an increasingly distressing position, is likely to negatively affect the employees' well-being and create an environment where personal boundaries are repeatedly compromised. This theme is closely related to discrimination, which is addressed in the accuracy category from a more technical perspective.

5.3 The framework of ethical considerations

While the ethical challenges related to IoT deployment are starting to gain more academic attention, the lack of tools dedicated to investigating the individuals' position in IoT ecosystems makes it difficult to gather an encompassing and coherent understanding of the subject. The expanded PAPA framework will contribute to this problem by providing a thorough, yet further expandable, tool for examining ethical matters in both theory and practice.

Table 2 illustrates the content and purpose of the added motivation and security categories from the following perspectives: implications for an individual employee, implications for general management, implications for data management, implications for communication and implications for the regulatory environment and society.

Regarding motivation, the first question related to the implications for an individual employee is why the IoT is used and whom does it benefit. Second, it should be considered whether the collected data can be used to harm employees either intentionally or unintentionally. This provides a foundational understanding of the position of the individuals and informs us about whether the solution's purpose is to provide common benefits or to solely serve the needs of an organisation behind the implementation. From the perspective of general management, we emphasise the management's responsibility to consider the risks and benefits from every involved stakeholder's standpoint, as a multiplicity of both internal and external individuals and organisations are, in many cases, involved in the IoT ecosystems. When risks to any stakeholder are found, their significance should be carefully examined and compared with the achievable benefits before advancing to the deployment phase.

Regarding data management, a thorough understanding should be gathered on which data are collected and why, in addition to what are the risks that the data set itself can lead to. Especially, when individual information is collected, it is crucial to limit the data collection to the minimum, as collecting personal data with or without an actual purpose may result in additional ethical risk factors. The implications for communication mainly concentrate on transparency and explainability. The goal should be to provide the individuals with both thorough and understandable information regarding the purpose of the data collection and the involved benefits and risks from each stakeholder's perspective. Finally, regarding the regulatory environment and society, the actors behind the implementation should ensure that their actions are based on the current regulations and follow the best intentions, avoiding

	Motivation	Security
Implications for an individual employee	Why is IoT used and who does it benefit?	Can the data collection and processing affect the individual's employment?
	Can the collected data be used to harm the employee (intentionally or unintentionally)?	Is the employee able to control the intrusiveness of data collection at work and off duty?
Implications for general management	What are the risks and benefits for each stakeholder of IoT?	How has the management ensured the employee's personal safety and position when deploying IoT?
	Are the benefits greater than risks to all stakeholders?	Is management allowed to practice personal profiling and decision-making based on the collected data?
Implications for data management	Which data are collected and why?	How is the intrusiveness of data collection managed and limited?
	What are the risks that data set can lead to?	How is the data collection and processing restricted to avoid negative consequences towards employees?
Implications for communication	How is the motivation for IoT use explained?	Are the employees thoroughly informed about the possible personal consequences of data collection and processing?
	How are benefits and risks explained in a transparent manner?	What precautionary measures have been taken to avoid harmful information sharing?
Implications for the regulatory environment and society	Are the actions based on not only the current regulations, but also best intentions and risk avoidance?	Does the company follow the current laws and regulations related to ensuring the employees' personal safety?
	Does the IoT cause possible risks to any stakeholders, environment or society at large?	Does the company consider the ethical aspects in addition to the legal limitations?

Table 2. The ethical considerations for IoT usage in an SME based on the PAPA extension categories

risks from the perspective of involved stakeholders, environment or society to the highest possible degree.

From the security standpoint, an individual's position needs to be examined regarding whether the data collection can affect one's employment and whether the individual can control the intrusiveness of data collection both at work and off duty. Furthermore, we claim that technical evolution should not, in principle, weaken the position or autonomy of the involved individuals, but primarily offer common benefits through constructive development. Considering the general management's responsibilities regarding ensuring personal security, it should guarantee that the involved individuals' professional safety and position are protected after the new solution is implemented. Furthermore, practising any kind of personal profiling and decision-making should only be conducted on an ethically justified basis, in addition to providing these individuals with sufficient understanding to give their informed consent. Regarding data management, the party behind an IoT solution implementation must be capable of minimising the intrusiveness, collection and processing of data collection. Regarding communication, employees must be thoroughly informed about the potential personal consequences of data collection and processing. Additionally, sufficient precautionary measures must be taken to avoid harmful information sharing. Regarding the regulatory environment and society, the employees' personal safety must not only be protected by following the current laws and regulations but also considering the ethical aspects potentially not addressed by law.

6. Conclusions and further actions

This study primarily develops a preliminary framework of ethical challenges related to IoT solution deployment in the SME environment. The framework was expanded from the PAPA model, which offers a good starting point but lacks coverage of several IoT specific issues. The proposed framework includes major ethical implications and considerations to be made to ethically utilise IoT solutions without endangering the individuals.

The ethical issues arising from IoT implementation for the SME sector can be analysed through the lens of general IT ethics. However, the diverse characteristics of the SME sector and the nature of IoT, especially the ubiquity, covert invasiveness and potential for excessive control combined with the dangers of powerful autonomous systems, do justify a closer look at the specifics of the relevant ethical factors.

Although some of the issues addressed above may seem rather insignificant, it is worth acknowledging that the cumulative consequences of even perceivably minor negligence can be dramatic, as the outcomes can apply to a wide group of stakeholders. Correspondingly, the extent of effects towards an individual is often difficult to predict, and thus their potential to induce significant problems, both professional and personal, cannot be ruled out. Hence, if the company does not pay sufficient attention to ethical factors internally, can it be assumed that their customers are treated differently? Overall, depending on the overall magnitude of the issues caused by ethical shortcomings, companies may suffer damages regarding internal trust, company image and customer relations.

From a technical perspective, IoT solutions themselves rarely limit unethical practices, as data can typically be collected regardless of time and place. The existing laws and regulations can neither be considered as sufficient safeguards ensuring the employees' protection in the IoT ecosystem, as they cannot be assumed to follow good ethical values. Thus, ethical responsibility still ultimately relies on individuals' moral standards. Simultaneously, IoT use keeps growing rapidly, which creates an acute demand for a comprehensive framework capturing all currently identified ethical risk factors present in complex IoT ecosystems. We initiated this process by introducing an expanded revision of PAPA, which complements the original model by adding the new motivation and security categories to its depth.

Based on this background, we claim that SMEs should pay close attention to ethical risk factors before implementing IoT solutions. As stated above, the responsibility related to ethical matters should not be affected by personal competence or the lack of it. Thus, companies are still obligated to fulfil ethical values, even though it may call for external contribution. This emphasises the complexity behind deploying new technical solutions, whose requirements and consequences can be difficult to predict and understand. However, it is not constructive to hinder the technical development of SMEs, and neither should they be left alone with these duties.

This study has both theoretical and practical contributions. From a theoretical perspective, it conceptualises the ethical issues of IoT in SMEs and paves the way for further research. Thus, this study serves as a starting point for ethical discussions or analyses about both IoT and its use in SMEs. The expanded PAPA model provides a multilevel framework for studying these ethical issues further. From a practical perspective, this study and the framework provide managerial personnel for the SMEs tool for the implementation of IoT as it synthesises the ethical issues and guides towards more ethical use of IoT.

Naturally, this conceptual analysis of the ethical issues of IoT in SMEs has its limitations. However, due to the lack of research in this domain, we argue that this study is needed to pave the way for future research and more ethical practices. Therefore, we suggest that further research be conducted to validate and develop the ethical IoT framework introduced in this study. As the IoT itself keeps evolving, so do various potential ethical challenges. Thus, the introduced model should be considered an evolving system and developed in an iterative

manner. To further validate the updated model, we consider conducting expert interviews and applying the model in real business scenarios as mandatory efforts.

References

Atzori, L., Iera, A. and Morabito, G. (2010), "The internet of things: a survey", *Computer Networks*, Vol. 54 No. 15, pp. 2787-2805, doi: 10.1016/j.comnet.2010.05.010.

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 of Information Systems Evaluation*, Vol. 15 No. 1, pp. 3-13.

Brill, H. and Jones, S. (2016), "Little things and big challenges: information privacy and the internet of things", *The American University Law Review*, Vol. 66, pp. 1183-1230, doi: 10.2139/ssrn.3188958.

Cerchione, R. and Esposito, E. (2017), "Using knowledge management systems: a taxonomy of SME strategies", *International Journal of Information Management*, Vol. 37 No. 1, pp. 1551-1562, doi: 10.1016/j.ijinfomgt.2016.10.007.

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*, Vol. 5 No. 3, pp. 161-183, doi: 10.1111/j.1365-2575.1995.tb00106.x.

Conti, M., Dehghantanha, A., Franke, K. and Watson, S. (2018), "Internet of Things security and forensics: challenges and opportunities", *Future Generation Computer Systems*, Vol. 78 No. 2, pp. 544-546, doi: 10.1016/j.future.2017.07.060.

Desouza, K.C. and Awazu, Y. (2006), "Knowledge management at SMEs: five peculiarities", *Journal of Knowledge Management*, Vol. 10 No. 1, pp. 32-43, doi: 10.1108/13673270610650085.

European Commission (2017), "Proposal for a regulation of the European parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing directive 2002/58/EC. Regulation on privacy and electronic communications", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=EN (accessed 21 April 2021).

Fassin, Y., Van Rossem, A. and Buelens, M. (2011), "Small-business owner-managers' perceptions of business ethics and CSR-related concepts", *Journal of Business Ethics*, Vol. 98 No. 3, pp. 425-453, doi: 10.1007/s10551-010-0586-y.

Friedman, B., Hendry, D.G. and Borning, A. (2017), "A survey of value sensitive design methods", *Foundations and Trends in Human–Computer Interaction*, Vol. 11 No. 2, pp. 63-125, doi: 10.1561/1100000015.

Giaretta, A., Balasubramaniam, S. and Conti, M. (2016), "Security vulnerabilities and countermeasures for target localisation in bio-nano things communication networks", *IEEE Transactions on Information Forensics and Security*, Vol. 11 No. 4, pp. 665-676, doi: 10.1109/TIFS.2015.2505632.

Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. (2013), "Internet of Things (IoT): a vision, architectural elements, and future directions", *Future Generation Computer Systems*, Vol. 29 No. 7, pp. 1645-1660, doi: 10.1016/j.future.2013.01.010.

Hakkala, A. (2017), "On security and privacy for networked information society: observations and solutions for security engineering and trust building in advanced societal processes", Doctoral Thesis, University of Turku.

Hoyer, V., Janner, T., Mayer, P., Raus, M. and Schroth, C. (2006), "Small and medium enterprise's benefits of next generation e-business platforms", *The Business Review*, Cambridge, Vol. 10 No. 2, p. 8.

Jin, J., Gubbi, J., Marusic, S. and Palaniswami, M. (2014), "An information framework for creating a smart city through internet of things", *IEEE Internet of Things Journal*, Vol. 1 No. 2, pp. 112-121, doi: 10.1109/JIOT.2013.2296516.

Kainu, V. and Koskinen, J. (2012), "Between public and personal information - not prohibited, therefore permitted", *Proceedings of the 5th International Conference on Information Law and Ethics 2012 Volume: Privacy and Surveillance At: Corfu*, Greek.

Kernaghan, K. (2014), "The rights and wrongs of robotics: ethics and robots in public organizations", *Canadian Public Administration*, Vol. 57 No. 4, pp. 485-506, doi: 10.1111/capa.12093.

Khan, R., Khan, S.U., Zaheer, R. and Khan, S. (2012), "Future internet: the internet of things architecture, possible applications and key challenges", *Proceedings of Frontiers of Information Technology (FIT), 2012 10th International Conference*, IEEE Computer Society, USA, pp. 257-260, doi: 10.1109/FIT.2012.53.

Kirtley, J. and Memmel, S. (2018), "Too smart for its own good: addressing the privacy and security challenges of the internet of things", *Journal of Internet Law*, Vol. 11 No. 4, pp. 18-33.

Koskinen, J. (2016), "Datenherrschaft – an ethically justified solution to the problem of ownership of patient information", Doctoral Thesis, University of Turku.

Lee, I. and Lee, K. (2015), "The Internet of Things (IoT): applications, investments, and challenges for enterprises", *Business Horizons*, Vol. 58 No. 4, pp. 431-440, doi: 10.1016/j.bushor.2015.03.008.

Martin, G. and Staines, H. (1994), "Managerial competences in small firms", *Journal of Management Development*, Vol. 13 No. 7, pp. 23-34, doi: 10.1108/02621719410063396.

Mason, R.O. (1986), "Four ethical issues of the information age", *MIS Quarterly*, Vol. 10 No. 1, pp. 5-12, doi: 10.2307/248873.

Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I. (2012), "Internet of things: vision, applications and research challenges", *Ad Hoc Networks*, Vol. 10 No. 7, pp. 1497-1516.

Oriwoh, E., Jazani, D., Epiphaniou, G. and Sant, P. (2013), "Internet of things forensics: challenges and approaches", *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, IEEE, pp. 608-615, doi: 10.4108/icst.collaboratecom.2013.254159.

Reijers, W., Koidl, K., Lewis, D., Pandit, H.J. and Gordijn, B. (2018), "Discussing ethical impacts in research and innovation: the ethics canvas", in Kreps, D., Ess, C., Leenen, L. and Kimppa, K. (Eds), *HCC13: This Changes Everything – ICT and Climate Change: What Can We Do?*, Poznan, pp. 299-313, doi: 10.1007/978-3-319-99605-9_23.

Royakkers, L., Timmer, J., Kool, L. and van Est, R. (2018), "Societal and ethical issues of digitization", *Ethics and Information Technology*, Vol. 20 No. 2, pp. 127-142, doi: 10.1007/s10676-018-9452-x.

Singh, J., Millard, C., Reed, C., Cobbe, J. and Crowcroft, J. (2018), "Accountability in the IoT: systems, law, and ways forward", *Computer*, Vol. 51 No. 7, pp. 54-65, doi: 10.1109/MC.2018.3011052.

Smith, H., Dinev, T. and Xu, H. (2011), "Information privacy research: an interdisciplinary review", *MIS Quarterly*, Vol. 35 No. 4, pp. 989-1015, doi: 10.2307/41409970.

Storey, D.J. (2016), *Understanding the Small Business Sector*, Routledge, London.

The European Parliament and the Council of the European Union (2016), "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", *Official Journal of the European Union*, Vol. L119, No. 2016, pp. 1-88.

Vermanen, M. and Harkke, V. (2019), "Findings from multipurpose IoT solution experimentations in Finnish SMEs: common expectations and challenges", *Proceedings of the 52nd Hawaii International Conference on System Sciences*, pp. 5246-5255, doi: 10.24251/HICSS.2019.631.

Wachter, S. (2018), "Normative challenges of identification in the Internet of Things: privacy, profiling, discrimination, and the GDPR", *Computer Law and Security Review*, Vol. 34 No. 3, pp. 436-449, doi: 10.1016/j.clsr.2018.02.002.

Wortmann, F. and Flüchter, K. (2015), "Internet of things", *Business and Information Systems Engineering*, Vol. 57 No. 3, pp. 221-224, doi: 10.1007/s12599-015-0383-3.

Further reading

Li, S., Tryfonas, T. and Li, H. (2016), "The Internet of Things: a security point of view", *Internet Research*, Vol. 26 No. 2, pp. 337-359, doi: 10.1108/IntR-07-2014-0173.

Martin, G. and Staines, H. (1994), "Managerial competences in small firms", *Journal of Management Development*, Vol. 13 No. 7, pp. 23-34, doi: 10.1108/02621719410063396.

Corresponding author
Mikko Vermanen can be contacted at: mikko.vermanen@utu.fi