Privacy in Internet of Things Ecosystems – Prerequisite for the Ethical Data Collection and Use by Companies

Mikko Vermanen, Minna M. Rantanen, Jani Koskinen

Privacy in Internet of Things Ecosystems – Prerequisite for the Ethical Data Collection and Use by Companies

Mikko Vermanen[1][0000−0003−3500−6974], Minna M. Rantanen[1][0000−0001−8832−5616], and Jani Koskinen[1] [0000−0001−8325−9277]

[1] Information System Sciences, Turku School of Economics,University of Turku
mjverm@utu.fi

Abstract. The abstract should summarize the contents of the paper in short terms, i.e. 150-250 words. The expansion of IoT implementations in organisations has resulted in more and more people getting involved in technical ecosystems not only as users but also as data sources. While the surveillance capabilities of IoT solutions grow in terms of scale and accuracy, it is inevitable that individuals end up in a position where information involving them is collected, either directly or indirectly. While the motives behind data collection and distribution may not be malicious, the availability of personal information always produces an opportunity for intentional or unintentional misuse. However, ensuring complete privacy in highly surveilled environments is practically impossible to achieve. While legislation appears to provide a comparatively safe environment for employees, regulations alone do not guarantee that sufficient focus is directed towards ethics. Rather, we focus on proposing constructive approaches to ensure ethicality by deliberative and transparent cooperation between customers and companies likewise between employees and employers.

Keywords: Customers, Employees, Employers, Ethics, Internet of Things (IoT), Privacy, Surveillance

1 Introduction

Internet of Things (IoT) is a term originally introduced by Kevin Ashton in 1999 [14]. IoT 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 [16], to immaterial interests, for instance, collective traffic and consumer behaviour [6]. The added value achieved from the data produced by IoT solutions can appear in many forms, including personal, professional, and economical. Data gathered through IoT can be used by various groups or actors, including academia, industry, and government. [11] As an example from the business perspective, companies can aim for higher performance and reduced manual labour through more efficient and accurate data collection capabilities by utilising modern IoT solutions [26].

However, the consequences towards employees or customers – from whom the data is collected directly or indirectly – may not be unambiguously positive.This is partly due to the observation that the developed monitoring capabilities and the possession of personally identifiable data can provide opportunities for both intentional and unintentional misuse [26]. In addition to the human element, technological issues have a significant role in IoT privacy and security. The safety of every IoT device, sensor, and unit of information can become increasingly compromised, partly due to the vulnerabilities resulting from the rapid development of IoT as the security measures may not keep up with the risks. [5] Thus, a large variety of privacy-threatening factors need to be acknowledged and addressed when implementing these solutions - not only related to the current practices but also in terms of potential long-term risks resulting from gathering, storing, and distributing identifiable data.

To tackle this conflict between benefits and negative consequences of data collection [4, 20], we need new kinds of procedures how to control data collection and use to achieve privacy that e.g. the General Data Protection Regulation act (GDPR) demands [22]. Koskinen et al. [12] proposed an ethical governance model for data economy ecosystems where all stakeholders are creating the rules for the data ecosystem by rational discourse to ensure fair, ethical data use and supervision over the ecosystem [12]. This kind of approach for data use helps to see the different viewpoints and demands for data use practices in a networked environment where a wide perspective is essential, instead of focusing on single views or merely fulfilling the demands of regulations.

This paper focuses on examining the potential issues related to the privacy of individuals involved in IoT ecosystems as directly or indirectly identifiable information sources the from the perspective of employees and employers. On a practical level, the ethical sustainability of IoT implementations is supported by introducing guidelines aiming to help companies to retain the benefits of IoT while protecting the privacy of their employees, customers or other individuals.

The paper is structured as follows. In Chapter Two, we introduce the concepts of surveillance and privacy in the context of IoT. Chapter Three provides further insight into the connection between surveillance and privacy, and what are the actions required to ensure privacy. In Chapter Four, we introduce topics for further investigation. Finally, conclusions are provided in Chapter Five.

2 IoT, surveillance and privacy

We have entered into an information society where mass surveillance has been realised through the possibilities offered by modern information technology [7]. For example, AI that uses the data collected via IoT offers new kinds of monitoring possibilities for companies but with the cost of the privacy of the people connected with IoT devices if data is retrieved from them or traceable to them. Thus, implementing IoT devices in a working environment in an ethical manner is a matter of balancing needed surveillance and privacy demands.

2.1 Surveillance

IoT solutions provide companies with a diversity of surveillance tools enabling them to inspect factors such as efficiency and performance of employees [24] or customer behaviour. While this kind of surveillance can be targeted towards material objects, individuals, environment, or a combination of those [25], we focus on settings where individuals are in some way connected to the data collection either directly or indirectly.

For instance, industrial companies can monitor machinery usage by tracking specific attributes, such as their movement, with a simple sensor-based IoT device. In this example, personal information is easily available if the monitored machine does not function fully automatically but is operated by employees. At least, it can be derived by linking IoT-based information to other sources. As another example, a delivery company can track their vehicles with location and movement sensors. In these cases, employees practically always contribute to the created data while the vehicle is moving. What makes these surveillance solutions especially vulnerable in terms of privacy is that individuals can be tracked at any time while operating the vehicle, regardless of whether they are on duty or not.

However, the availability of personal information does not mean that personal information is stored, processed or distributed in an identifiable form, as the party behind the data collection is in many cases capable of determining the level of retaining privacy. For example, an IoT device can be configured so that attributes involving human contribution are not collected. Similarly, timestamps can be either removed, or their sample cycle lengthened, in which cases the data considers aggregate users instead of separate individuals [2]. Additionally, methods such as pseudonymisation [17] can be leveraged to add a privacy layer to the collected information.

Whether the actions and attributes of physical objects, environment or individual users are being surveilled affects how privacy-related matters should be considered [26]. Naturally, information from different sources will be involved in most cases, as it is often possible to track who was using a particular de vice at the given time and given environment. Notable is that surveillance tends to change the behaviour of the person who is under surveillance [7]. Changing the behaviour may be one of the aims that some organisations have in using surveillance technology — to affect e.g. employees or even customers to act efficiently, coherently, and predictable. However, this kind of constant monitoring and emphasise on efficiency is problematic at least from three points.

First, it has a similar problem to Taylorism. Humans are not technical systems that can be boosted by forcing them to be more and more efficient like machinery. This phenomenon was noted, for example, in coal mine studies by Trist and Bamford [23], which led to the realisation of the socio-technical nature of systems [8] where individuals are not seen as a mere technical resource. Secondly, we do not know clearly the effects of surveillance on individual's behaviour or attitude [29]. However, people who are monitored can alter their behaviour that can be judged as suspicious — phenomenon known as chilling effect [19, 7]. However, the question is whether people act differently or just reveal the desired side of their actions, which affects the quality

of the collected data and, therefore, reduces its usability. Thirdly, the constant monitoring of people itself is ethically, and legally problematic [1, 21, 18, 27].

2.2 Privacy

Discussion of privacy is old as mankind and it has roots in protection of ones body and home [10]. The problem is, that privacy is a concept that is not self-evident even if it may look alike in first sight. Brandeis and Warren described privacy The right to the privacy —in their influential article—as a right to be let alone, although not without exceptions [3].

Another well-known article is Alan Westin's Privacy and freedom [28], which describes privacy as self-determination, where individuals, groups, or institutions determine how information about them is revealed [10]. Privacy as a right to be left alone, or self-determination of what information is revealed from one, is an understandable and even justified claim if those are not conflicting with the justified rights of others. However, the nowadays society, which is more and more "online", challenges these views of privacy.

In the context of IoT, the boundaries of what is private and what is not are bending. Especially when technology —here IoT— is pervasive and ubiquitous in our society, via exploding number of artifacts that can monitor us and collect an enormous amount of data, we face the illusion of privacy. It seems that we can be physically alone, but we may be under constant surveillance by the surrounding IoT-artifacts — worn or even implemented in the near future. Once again, this should remind us to consider our privacy from the perspective of the information society era. Therefore frameworks like PAPA [15] are more fruitful as those are created to describe the ethical issues of the information age that we are living in today. We narrow our focus on the Internet of Things (IoT), a topic that represents technology in the sense of how hidden it may be, and usually is, for people.

In this chapter, we introduce central privacy-related implications and questions from the perspective of an individual employee, general management, and data management.

Combining the variety of technical pitfalls with the potential risks resulting from the actions and decisions of human actors, we are facing a highly complicated ensemble of threats towards the privacy of individuals involved in these ecosystems, difficult to comprehend even by the large companies and dedicated experts. Regardless of the potentially catastrophic consequences towards individuals' privacy, little research has been conducted related to the nature and magnitude of human factors, especially from the ethical perspective. Thus, our contribution is to investigate the potential risks and causes thereof by examining the role of ethical factors and the related managerial decisions. However, 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 Securing privacy in IoT surveillance implementations

Finding the balance between maintaining personal privacy and enabling companies to benefit from IoT is crucial when pursuing practical value, compared to conducting a one-sided analysis. In this chapter, we introduce potential advantages and disadvantages related to different approaches to IoT data collection and distribution from the standpoint of employees and management involved in IoT ecosystems.

Considering the position of employees, we should clarify whether they are given an ability to control what, how, when, and why data is collected and/or distributed [26]. Autonomy is seen as one of the key issues in ethics. Without autonomy, actors do not have the possibility to choose and thus make ethical decisions. When employees are the sources of information, it would be questionable that they do not possess any control over information that might compromise their privacy.

Another relevant question is, can the gathered data be combined and attributed to a specific person within the organisation. In general, the employees involved in IoT ecosystems should be able to approve, prohibit, or control [2] the collection and distribution of any identifiable data which may potentially cause personal harm. We find this important not only from the perspective of ethics but also as a factor affecting the employees' acceptance towards the change.

As a whole, the justification for surveillance must be based on the interest of both parties, the employer and the employee. If the gathered data remains anonymous throughout its life-cycle or can be guaranteed not to cause negative effects on an individual, significant ethical violations are less likely to occur. Even then, we propose that data collection should be kept to a bare minimum in terms of scale, time and location. This is emphasized in settings where individuals can be monitored continuously, for example, when sensors are attached to vehicles or devices that employees carry with them — sometimes on and off duty. This reduces the number of potential ethical pitfalls caused by unnecessary surveillance. Similar issues should be considered between the customer or companies if customers are monitored in similar manners.

From the perspective of general management, conducting ethical IoT implementations requires collecting informed consent from the employees from whom data is collected and distributed. To fulfill this criterion, management should define equitable and documented conditions that employees can voluntarily comply with. For this purpose, the employees should be thoroughly educated about what, how, when, and why data is collected and/or distributed, to whom the data is distributed, and how the privacy and security of the employees are guaranteed. A transparent and well-documented approach will not only provide fair, practical foundations but can also positively affect the employees' voluntary contribution and the aforementioned level of acceptance, which has been questionable in the context of IoT, both technologically and socially [2].

In terms of data management, it is critical for the management, employees and even customers to be aware of what information is revealed to external parties, how the data is protected, and who is responsible for the protection. When sharing data with external parties, the default approach should be to minimize the volume of individuals' information or avoid it altogether. However, to actually reach the benefits of

collaboration with partners and other related parties, companies are forced to distribute information. If and when data sharing cannot be avoided, it should be carefully considered what is truly necessary to distribute and whether it could violate the position of the related individuals.

4 Discussion

While aiming to build socially just implementations and ecosystems, we must acknowledge that technologies such as IoT rely on the collected data. If we were to focus solely on the position of individuals, we would likely end up discouraging data collection and distribution altogether. Hence, the consequences of heightened privacy protection may not be solely positive [13]. In fact, ending up under surveillance is practically inevitable in any area or environment where a sensor network is deployed [2], and as the number of IoT implementations keeps growing, it becomes clear that complete privacy cannot be achieved. This leads us to an intersection where a satisfactory balance between the individuals' and organisations' benefits and needs has to be achieved in order to support technical development.

From a legislative perspective, the challenge is how ethical factors can be regulated in the first place, partly due to the subjectivity in defining what is ethical. While regulations do contribute significantly to enhancing the privacy of individuals, following proper practices from both legislative and ethical standpoint is eventually dependent on the behaviour of the people in control — in this case, the management. As long as no formal ethical regulations exist, it is not possible to force employers to change their approach in terms of respecting individual privacy to a further degree than what is required by law. Hence, we are only able to offer general recommendations and guidelines that eventually require voluntary compliance from the companies. Thus, we see motivation as the strongest utility for driving development towards an ethically sustainable direction.

Therefore we propose using the concept of fair governance model for data economy ecosystem, where the rules are commonly agreed on between all relevant stakeholders [12]. There the rules and procedures — how information is collected, used, and distributed — are decided by the rational discourse that is open and emancipatory by the nature [9]. This kind of discourse is based on respect of people as equal participants; pays attention to peoples' needs, preferences, and socio-cultural circumstances; adopts the individuals' and communities' perspectives; enables people the education and support they need and acts fairly for the common good [12].

This kind of deliberative way of defining the rules of how collected data is used is suitable for all stakeholders (here employees and employers) and thus more likely ethically justified. Ideally the situation is like Koskinen et al. [12] state:

> *"fair data economy ecosystem governance model is model that includes the rules, technical and non-technical requirements for actors, controlling bodies and representation of all stakeholders(board) to ensure legal, ethical, transparent, trustworthy, secure and fair data use and supervision of it — in defined data economy ecosystem."*

This approach is applicable in the IoT context, where we are currently building foundations for ethical implementations rather than proposing strict and exact requirements for the ethical use of IoT. In conclusion, we aim to contribute to creating a culture that takes into account the whole IoT ecosystem (here, especially employees and employers) and encourages participating in ethically sustainable development through the common adoption of ethically sustainable practices by the deliberative approach.

A complex dimension besides data distribution itself is the related responsibility. In this paper, we mainly challenge the organisation's responsibilities within a controlled and limited ecosystem, as potential parties forming privacy threats do not end there. While internal data collection and distribution restrictions are crucial, IoT ecosystems can involve a variety of external actors, such as service providers and partners with whom data may be shared. Additionally, phenomena such as rising cybercrime form significant risks, further underlining that gathering and storing personal data comes with high responsibility for the organisations. Be it a result of negligence or becoming a victim of an attack, the outcome for the compromised personal data remains as severe. The responsibility of organisations should cover the use of IoT even when some risks are from outside.

5 Conclusions

Leveraging the surveillance capabilities of IoT solutions while protecting employees' privacy forms a challenging combination because IoT is dependent on collecting data, which in many cases is inevitably linked to individuals either directly or indirectly. Hence, to provide applicable practical recommendations aiming for implementing ethics as an integral part of doing business, it is necessary to build balanced IoT deployment approaches that aim to protect the position of individuals and support the technical development and financial competitiveness of companies. Even as compromises cannot be avoided from the standpoint of either party, foundational ethical principles can be applied without losing the majority of the available benefits. We claim that companies are, in most cases, able to configure the deployed IoT solutions in a manner that respects the privacy of their employees and customers, as a variety of different data collection and distribution approaches are available. Organisation can, for example, limit data gathering to anonymous targets, use aggregated data instead of small sample sizes that allow identification, and utilize pseudonymisation in cases where identification cannot otherwise be avoided. Similarly, we see that majority of privacy risks related to data distribution can be avoided by carefully limiting the group of receivers and defining what specific information is necessary to be shared with each party.

In current circumstances, where the deployment rate of IoT keeps rising rapidly, the collection and distribution of data connectable to specific individuals cannot be entirely eliminated. Rather, we encourage focusing on minimizing redundant surveillance, which could either significantly endanger privacy or does not provide meaningful value to the company. Hence, moderation must be applied when proposing re-

formed procedures, which the companies are in many cases not formally obligated to follow, as the coverage of ethical regulations is reasonably limited. We claim that enhancing the companies' motivation to respect the privacy of their employees and customers through motivation and collective contribution to the fairness of the economy is one of the most efficient methods to support ethically sustainable development.

Modern legislation appears to provide a comparatively safe environment for individuals. However, regulations alone cannot be assumed to result in a holistically ethical mindset. Financial motives may overshadow ethical principles, especially if specific surveillance methods are not prohibited from a legal perspective. From a long-term perspective, we should aim for building practises that prevent misuse and negligence. However, in current reality, the implementation of ethics as an axiomatic feature of doing business is in its infancy.

References

1. 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 (2016)
2. Atzori, L., Iera, A., Morabito, G.: The internet of things: A survey. Computer networks 54(15), 2787–2805 (2010)
3. Brandeis, L., Warren, S.: The right to privacy. Harvard law review 4(5), 193–220 (1890), https://doi.org/10.2307/1341305
4. Celik, Z.B., Fernandes, E., Pauley, E., Tan, G., McDaniel, P.: Program analysis of commodity iot applications for security and privacy: Challenges and opportunities. ACM Computing Surveys (CSUR) 52(4), 1–30 (2019)
5. Conti, M., Dehghantanha, A., Franke, K., Watson, S.: Internet of things security and forensics: Challenges and opportunities. Future Generation Computer Systems 78, 544–546 (2018)
6. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (IoT): A vision, architectural elements, and future directions. Future generation computer systems 29(7), 1645–1660 (2013)
7. Hakkala, A., Koskinen, J.: Personal data protection in the age of mass surveillance. Journal of Computer Security (Preprint), 1–25 (2022)
8. Herbst, P.G.: Socio-technical design: strategies in multidisciplinary research. Tavistock, London (1974)
9. Hirschheim, R., Klein, H.K.: Realizing emancipatory principles in information systems development: The case for ethics. MIS Quarterly 18(1), 83–109 (1994). https://doi.org/DOI: 10.2307/249611
10. Holvast, J.: History of privacy. In: The History of Information Security, pp. 737– 769. Elsevier (2007)
11. Khan, R., Khan, S.U., Zaheer, R., Khan, S.: Future internet: the internet of things architecture, possible applications and key challenges. In: 2012 10th international conference on frontiers of information technology. pp. 257–260. IEEE (2012)

12. Koskinen, J., Knaapi-Junnila, S., Rantanen, M.M.: What if we had fair, people centred data economy ecosystems? In: 2019 IEEE SmartWorld, UbiquIntelligenceigence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). pp. 329– 334. IEEE (2019)
13. Lee, I., Lee, K.: The internet of things (IoT): Applications, investments, and challenges for enterprises. Business Horizons 58(4), 431–440 (2015)
14. Madakam, S., Lake, V., Lake, V., Lake, V., et al.: Internet of things (IoT): A literature review. Journal of Computer and Communications 3(05), 164–173 (2015). https://doi.org/http://dx.doi.org/10.4236/jcc.2015.35021
15. Mason, R.O.: Four ethical issues of the information age. MIS quarterly pp. 5–12 (1986). https://doi.org/https://doi.org/10.2307/248873
16. Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I.: Internet of things: Vision, applications and research challenges. Ad hoc networks 10(7), 1497–1516 (2012)
17. Riedl, B., Grascher, V., Fenz, S., Neubauer, T.: Pseudonymization for improving the privacy in e-health applications. In: Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008). pp. 255–255. IEEE (2008)
18. Royakkers, L., Timmer, J., Kool, L., van Est, R.: Societal and ethical issues of digitization. Ethics and Information Technology 20(2), 127–142 (2018)
19. Schauer, F.: Fear, risk and the first amendment: Unraveling the chilling effect. BUL Rev. 58, 685 (1978)
20. Sollins, K.R.: Iot big data security and privacy versus innovation. IEEE Internet of Things Journal 6(2), 1628–1635 (2019)
21. Taylor, L.: What is data justice? the case for connecting digital rights and freedoms globally. Big Data & Society 4(2), 2053951717736335 (2017)
22. Tikkinen-Piri, C., Rohunen, A., Markkula, J.: EU general data protection regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review 34(1), 134– 153 (2018). https://doi.org/https://doi.org/10.1016/j.clsr.2017.05.015, https://www.sciencedirect.com/science/article/pii/S0267364917301966
23. Trist, E.L., Bamforth, K.W.: Some social and psychological consequences of the longwall method of coal-getting: An examination of the psychological situation and defences of a work group in relation to the social structure and technological content of the work system. Human Relations 4(1), 3–38 (1951). https://doi.org/10.1177/001872675100400101, https://doi.org/10.1177/001872675100400101
24. Vermanen, M., Harkke, V.: Findings from multipurpose IoT solution experimentations in Finnish SMEs: Common expectations and challenges. In: Proceedings of the 52nd Hawaii International Conference on System Sciences. pp. 5246–5255 (2019). https://doi.org/10.24251/HICSS.2019.631
25. Vermanen, M., Koskinen, J., Harkke, V.: Internet of things (IoT) data accessibility: Ethical considerations. In: Cacace, M., Halonen, R., Li, H., Orrensalo, T.P., Li, C., Widén, G., Suomi, R. (eds.) Well-Being in the Information Society. Fruits of Respect. pp. 197–208. Springer International Publishing, Cham (2020). https://doi.org/https://doi.org/10.1007/978-3-030-57847-3_14
26. Vermanen, M., Rantanen, M.M., Harkke, V.: Ethical framework for IoT deployment in SMEs: individual perspective. Internet Research (2021). https://doi.org/https://doi.org/10.1108/INTR-08-2019-0361
27. Wachter, S.: Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the GDPR. Computer Law & Security Review 34(3), 436–449

(2018). https://doi.org/https://doi.org/10.1016/j.clsr.2018.02.002, https://www.sciencedirect.com/science/article/pii/S0267364917303904
28. Westin, A.F.: Privacy and freedom. Washington and Lee Law Review 25(1), 166 (1968)
29. Yost, A.B., Behrend, T.S., Howardson, G., Darrow, J.B., Jensen, J.M.: Reactance to electronic surveillance: a test of antecedents and outcomes. Journal of Business and Psychology 34(1), 71–86 (2019)