Privacy and Ethical Considerations of Smart Environments: A Philosophical Approach on Smart Meters

Kamer Vishi[1,2(✉)]

[1] South-Eastern Norway Regional Health Authority, Sykehuspartner CERT, Oslo, Norway
[2] Department of Informatics, University of Oslo, Oslo, Norway
kamer.vishi@sykehuspartner.no
https://sykehuspartner.no/

Abstract. This paper delves into the privacy and ethical concerns related to smart devices in IoT, particularly smart meters. It explores the regulatory framework governing data protection through the lens of GDPR. Our analysis identifies relevant GDPR articles and presents a case study that exposes the privacy risks associated with smart meters. Ethical considerations are explored using deontology and consequentialism, offering a thorough analysis of privacy and ethical issues for consumers, manufacturers, and policymakers. The paper emphasizes the complexity of these concerns and the need for a comprehensive assessment of potential benefits and harms to individuals and society. It also stresses the importance of ethical considerations and compliance with GDPR requirements when designing smart building systems to guarantee adequate privacy measures. Our concluding remarks advocate that manufacturers and suppliers prioritize consumer privacy and security over profit and consider stronger privacy protections, increased transparency, and alternative business models to address these concerns. The importance of IoT privacy concerns cannot be underestimated, given their impact on personal and organizational privacy.

Keywords: Privacy · GDPR · Security · Ethics · IoT · Smart meters · Data protection · Data leakage · Malware

1 Introduction

The digital revolution has brought about transformative and irreversible changes to our society, with effects comparable to the upheavals of nineteenth-century industrialization or the invention of printing in the sixteenth century. One key driver of this revolution is the Internet of Things (IoT), which fosters the digitization of our lives by connecting everyday "things" (internet-enabled devices), making our environments or homes "smart" (intelligent). These everyday objects become informative, acting as physical access points to internet services. The internet expands invisibly into our familiar environment, integrating into our

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
O. Gervasi et al. (Eds.): ICCSA 2023 Workshops, LNCS 14112, pp. 303–313, 2023.
https://doi.org/10.1007/978-3-031-37129-5_25

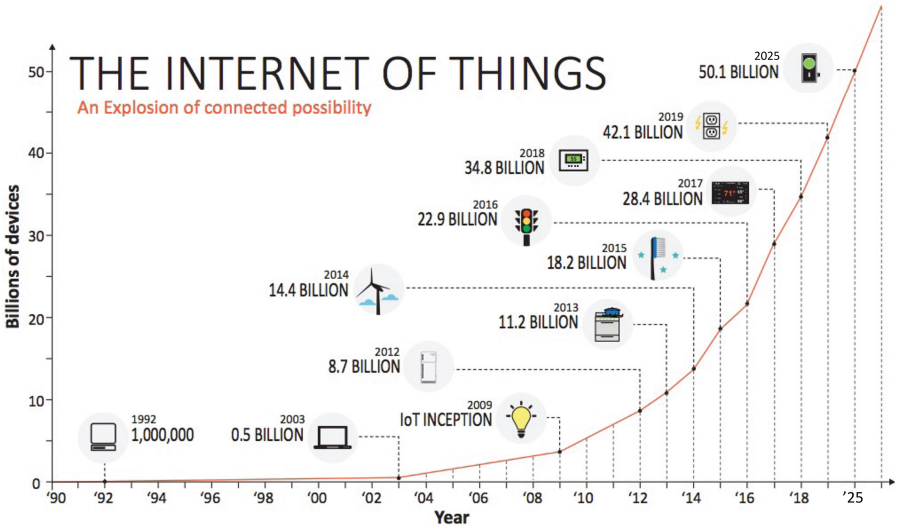

Fig. 1. The evolution timeline of the Internet of Things 1990–2025 (adapted from [19]).

homes and even "attaching" to our bodies through smart clothes, smartwatches, or fitness bracelets [18].

Different people may have varying interpretations of the IoT, but one undeniable aspect is the sheer number of connected devices and the vast amount of data generated.

Figure 1 illustrates the forecast provided by nternational Data Corporation (IDC) indicating that by 2025, there will be a total of 50.1 billion IoT devices, each capable of creating 79.4 zettabytes (ZB) of data individually. This explosion in connectivity and data production presents new ethical, legal, and social concerns [12,15].

As these devices connect to the internet, we confront various ethical and legal challenges, including security, privacy, transparency, data ownership, ethical and legal usage, data sharing, and the appropriateness of data collection. Smart meters, for instance, exemplify these concerns as the data they collect can potentially invade consumer privacy. Recent studies have highlighted that electricity consumption data may reveal private information such as household occupancy or economic status. In light of these concerns, it becomes increasingly crucial to examine the ethical implications of IoT technologies, particularly smart meters, and develop guidelines to address privacy issues and ensure responsible use [11].

2 Background

A smart environment can refer to a variety of locations, including but not limited to smart homes, businesses, and cities. The fundamental objective of smart

environments is to increase the level of user comfort, access control, and building security, as well as to provide more effective administration of the facility.

According to Article 8 (Respect for your private and family life) of the European Court of Human Rights (ECHR), privacy is defined as follows:

> *"Everyone has the right to respect for his private and family life, his home and his correspondence."* [2]

This right cannot be violated by a public authority, unless it is necessary to do so for legitimate reasons such as protecting national security, public safety, the country's economic well-being, preventing crime, promoting health or morals, or protecting the rights and freedoms of others.

The Global Privacy Network (GPEN) [9], in collaboration with 25 data protection authorities worldwide, conducted international research analyzing over 300 IoT devices, including smartwatches, fitness trackers, smart TVs, game consoles, and smart meters. Their research focused on examining how accurately companies inform their customers about privacy concerns. As these devices collect a significant amount of personal information, some of which is used to create targeted user profiles, companies must provide accurate information about privacy to their customers.

The study focused on how well companies communicated privacy matters to their customers. Furthermore, based on the research analysis, the following issues were identified:

- 59% of the IoT devices did not adequately explain how personal data is collected, processed, and used.
- 68% failed to provide information about how the collected information is stored.
- 72% did not provide information about data deletion.
- 38% did not provide contact information for customers to reach out if they have privacy concerns.

The study also raised concerns about medical devices that sent reports back to GPs via unencrypted email. As a result, data protection authorities considered action against any devices or services thought to have been breaking data protection laws.

According to the head of enforcement at the UK Information Commissioner's Office [9], the Internet of Things (IoT) technology could enhance various aspects of our lives, including our homes, health, and well-being. However, ensuring that privacy was not compromised in the process was essential. Companies that produced IoT devices needed transparency about protecting their customers' data. It was recommended that companies consider the privacy impact on individuals before bringing their products and services to market. Failure to do so could lead to consumer mistrust and reduced adoption rates.

This paper explores the "privacy paradox" [6] in the context of smart environments, with a specific focus on smart meters. Building on previous research, the paper examines the challenges posed by smart environments and investigates

the factors that predict privacy attitude and behavior. The study includes an analysis of international research and industry practices to identify compliance with data protection laws and uphold individual privacy rights. By considering theoretical explanations for the privacy paradox, the paper provides a nuanced analysis of the privacy and ethical considerations of smart environments. The goal of the research is to ensure that privacy and security are prioritized in the development and use of IoT devices [6].

To address privacy concerns related to the Internet of Things (IoT), the European Commission has implemented a new data protection directive known as the *"EU General Data Protection Regulation (GDPR),"* [4] which was enforced on May 25th, 2018. Since IoT devices are all about data, privacy is a significant concern for IoT-related projects. The GDPR applies to the processing, storing, and using of personal data by "smart" devices used by EU consumers. Schouw [16], a leading IoT and Big Data expert, highlights the importance of complying with GDPR and the ePrivacy electronic communications regulation. According to Schouw, compliance with these regulations helps with governance and positively impacts buyers' perspectives. Providers that prioritize data privacy and take measures to comply with regulations can gain the trust of customers and improve their business.

Smart meters and the Internet of Things (IoT) raise important privacy and data protection concerns, which are addressed in the General Data Protection Regulation (GDPR) through several key articles. Specifically, the following GDPR articles are particularly relevant to smart meters and IoT [4]:

1. **Article 5** of the GDPR states that personal data must be processed to ensure appropriate security, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage. Any data collected by smart meters or IoT devices must be secured and protected appropriately.
2. **Article 25** of the GDPR requires data protection by design and default. This means that data protection measures must be built into smart meters and IoT devices from the outset and that default setting must ensure the highest level of privacy for the user.
3. **Article 30** of the GDPR requires organizations to record their processing activities. Companies that collect data from smart meters and IoT devices must keep records of the data they gather, how they process it, and how they protect it.
4. **Article 35** and **36** of the GDPR require organizations using smart meters and IoT devices to conduct data protection impact assessments (DPIAs) to assess and minimize potential privacy risks. DPIAs are necessary to identify risks and implement safeguards to protect individuals' rights and freedoms.

Generally, GDPR requires that personal data collected by smart meters and IoT devices must be processed in a secure and transparent manner, with appropriate safeguards in place to protect the privacy of individuals.

Apart from classic attack motives such as stealing sensitive data or damaging systems or people, a new trend has emerged in recent years: the blackmail of

money. Cybercriminals are increasingly using Ransomware to prevent access to data or entire devices, only releasing it after receiving payment. This method has proven highly effective in generating funds, prompting cybercriminals to develop aggressive variants that bypass traditional security measures. Both private users and large companies have been victims of these attacks. Cybercriminals often use anonymization networks to hide their identities, making it difficult for law enforcement to tackle large-scale ransomware campaigns [5,17].

This type of threat is expected to continue to be a significant problem in the coming years, especially as the Internet of Things (IoT) becomes more prevalent. Even smart cars, watches, meters, household appliances, or entire homes can be taken hostage to extort a ransom. For instance, unauthorized access to a car's control systems or the front door can be prevented. Cybercriminals could turn off a refrigerator or alter the temperature control of a heating or air conditioning system, releasing it only after payment [10].

Furthermore, it is also worth mentioning that smart meters can support security policies against energy-related home attacks, as demonstrated by the BlackIoT botnet [20].

3 Case Study: Smart Meters

Figure 2 shows a smart meter, which is an intelligent electricity meter that can transmit energy consumption data in real-time to an energy supply company. With this data, the company can promptly respond to changes in energy consumption by adjusting their power plants and electricity storage accordingly. This enables energy providers to manage their energy supply more efficiently and effectively, ensuring a stable energy supply for their customers. Smart meters are an important component of the emerging smart grid infrastructure, which leverages advanced technology to optimize energy use, reduce costs, and minimize environmental impact.

Smart meters measure energy consumption and provide detailed information about an individual, family, or household, according to the Norwegian Data Protection Authority (Datatilsynet) [3]. Energy providers can access and retrieve data from smart meters even when we are at home or on vacation based on power consumption. Additionally, providers can monitor and control third-party devices such as smart TVs, thermometers, refrigerators, and doors. Researchers from Muenster University of Applied Sciences in Germany (Greveler et al. [7]) have demonstrated that smart meters can collect information about the TV channels and shows people watch. Network sniffing skills and tools were used to obtain this information. The data is sent unencrypted every two seconds from the smart meter to the provider server through the internet, potentially exposing user privacy.

Furthermore, according to Greveler et al. [7], companies can use the data collected by smart meters to create personalized ads for marketing or promotional purposes. By analyzing the data, they can determine if an individual is watching an illegal copy of a movie, for example. This highlights the potential



Fig. 2. An example of a smart electricity meter based on Open Smart Grid Protocol (OSGP), used in Norway and produced by Aidon. (Image courtesy of Aidon.com)

privacy implications of smart meters, as personal information can be shared with third-party companies without the user's consent.

Molina-Markham et al. [14] conducted a fascinating study on smart meters, demonstrating that off-the-shelf statistical methods can be used to extract complex user behavior and create user profiles from smart meter data, even without prior knowledge of household activities or training. Figure 3 illustrates power consumption segments for a day from one of the houses used in their experiment, showing variations and high-power consumption levels that indicate human activity, such as preparing food, taking a shower, or sleeping.

As discussed earlier, smart meters enable the monitoring of consumer behavior, which poses significant privacy concerns. These concerns are related to user behavior privacy, as described by Claude Castelluccia in *Chapter 2* of the book *European Data Protection: In Good Health?* [1]. Smart meters can intrude upon the privacy of consumers, and it is essential to address these concerns to ensure the protection of personal data.

4 A Philosophical Approach: Discussion and Critical Reflection

A philosophical approach to examining the privacy and ethical considerations of smart environments, particularly smart meters, provides a framework for understanding the underlying ethical principles and their application in practice. This approach helps to identify and evaluate the moral implications of different actions, and to determine what is morally right or wrong in a given situation. In this section, we discuss the ethical considerations of smart meters by analyzing them using different ethical theories or moral philosophies, including deontology

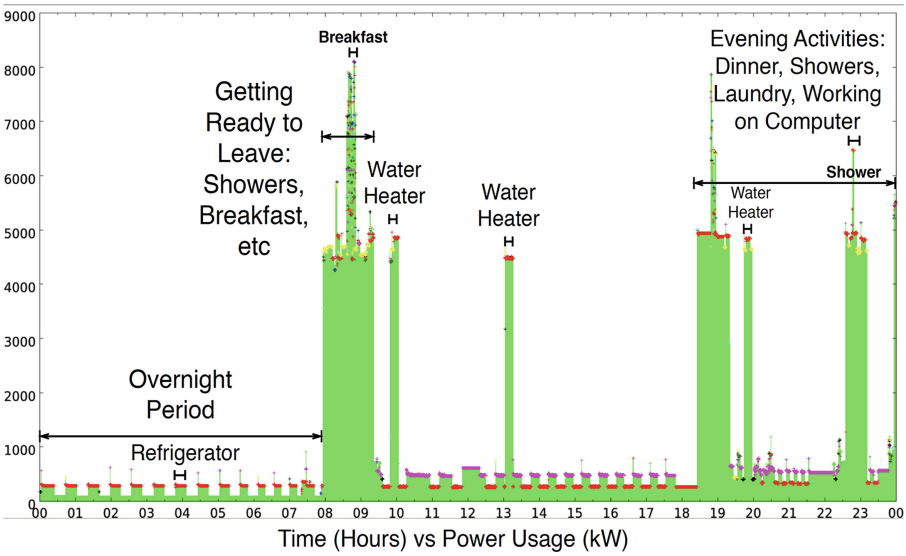

Fig. 3. An illustration of a power consumption trace at a second-level resolution that covers an entire day, including activity labels derived from a day's activity log (adapted from [14]).

and consequentialism. The aim is to provide a comprehensive analysis of the privacy and ethical issues associated with smart meters, and to critically reflect on the implications of these issues for consumers, manufacturers, and policymakers.

Before delving into the discussion and critical reflection sections, it is essential to have a brief understanding of the two ethical theories - deontology and consequentialism - that will be used to analyze the privacy concerns surrounding smart meters. Here is a brief summary of each:

- **Deontology:** This ethical theory, often associated with Immanuel Kant [13], focuses on the inherent moral value of actions rather than their outcomes. Deontological ethics argues that some actions are intrinsically right or wrong, regardless of their consequences. The central principle is the concept of duty, which implies that individuals should act according to moral rules or principles. In this framework, it is essential to adhere to these rules even if doing so might lead to less favorable outcomes.
- **Consequentialism:** This ethical theory focuses on the consequences or outcomes of actions to determine their moral value [8]. The most well-known form of consequentialism is utilitarianism, which posits that an action is morally right if it maximizes overall happiness or well-being for the most significant number of people. In this perspective, the ends justify the means, and an action is evaluated based on its potential to produce the best outcome.

Both deontological and consequentialist theories provide valuable insights for ethical decision-making. Deontology emphasizes the importance of moral duties

and principles, while consequentialism focuses on the outcomes and overall well-being. Understanding both perspectives can help individuals make well-rounded and ethically informed decisions.

4.1 Discussion

Regarding ethical issues related to smart devices, an essential and universal question is: *what is right and wrong?* These questions are significant at both individual and community levels. They provide a framework for how we ought to behave in different contexts, from legal laws and regulations to informal social norms. For manufacturers and providers of IoT services, one of the most challenging ethical dilemmas is whether to collect and use personal information from smart devices to understand better and serve individual consumers. This raises significant privacy concerns, particularly in the Internet of Things, and prompts the question:

> *How ethical and legal is it to collect data from smart (IoT) devices, and do these devices pose a threat to data privacy?*

In this paper, we discuss the ethical and legal considerations surrounding the collection of personal data by smart devices in the context of the Internet of Things (IoT). The question of whether it is ethical to collect data from smart devices is a complex one and can be analyzed through various moral philosophies such as deontology, consequentialism, virtue, and pragmatic ethics. For the sake of clarity and conciseness, we focus on consequentialism and deontology in this discussion.

We examine the relation between privacy and rights, harms, and interests to determine what morally important benefits data protection (privacy) can bring, and what morally important harms or violations of moral rights can result from a lack of data protection. We explore the potential benefits of data protection and the harms and violations that can result from breaches of privacy.

The most obvious harm that can occur from breaches of privacy is the unauthorized access, collection, use, and disclosure of personal information by smart devices such as sensors, smart meters, and smart TVs. This information may have personal, cultural, or social value that can be lost when the data is corrupted or misused. Moreover, any type of privacy breach is likely to cause some amount of psychological or emotional harm.

Furthermore, most of the information collected by smart devices is gathered without the consumer's knowledge or consent, which raises concerns about invasion of privacy. While some people view IoT devices as a revolutionary method of collecting data, others view it as a complete invasion of individual privacy.

To wrap up our discussion, in the context of smart meters and privacy, the two ethical theories, deontology and consequentialism, can offer different perspectives on data collection and usage:

From a deontological standpoint, collecting and using personal data from smart meters without user consent would be considered morally wrong, regardless of potential benefits. This is because privacy is a fundamental right that

should not be violated. In this view, manufacturers and service providers have a duty to respect user privacy by obtaining consent and implementing robust data protection measures, even if it may impact their ability to optimize services or generate profits.

In a consequentialist analysis, the ethical nature of collecting and using personal data from smart meters depends on the overall consequences of such actions. If the data collection leads to improved energy efficiency, cost savings, environmental benefits, and better services for users, it might be considered morally right. However, if the negative consequences, such as privacy violations, unauthorized data sharing, and potential misuse of information, outweigh the benefits, then the data collection would be seen as morally wrong.

When evaluating smart meters and privacy concerns, it is essential to consider both deontological and consequentialist perspectives. By doing so, manufacturers, service providers, and policymakers can balance the need to respect user privacy with the potential benefits of data collection and usage in the context of smart environments. Implementing privacy-enhancing technologies, obtaining user consent, and ensuring transparency in data collection practices are some steps that can help address the ethical concerns raised by both theories.

4.2 Critical Reflection

In addition to analyzing the ethical considerations of collecting data from smart devices, it is important to consider the broader societal implications of such actions. One of the main concerns is the potential for increased surveillance and control by both private companies and government agencies. With the proliferation of smart devices, there is a risk that individuals may lose control over their personal data, and that this information could be used against them in a variety of ways. For example, data collected from smart devices could be used to create profiles of individuals that could be sold to third-party companies for advertising purposes, or even to insurance companies for risk assessment. This could lead to discriminatory practices that unfairly disadvantage certain groups of individuals.

Another concern is the potential for smart devices to be hacked or otherwise compromised, leading to a loss of privacy and security for individuals. As the Molina-Markham et al. [14] study showed, even seemingly innocuous data collected from smart meters can be used to infer sensitive information about individuals, such as when they are home or what they are doing. This information could be used to target individuals for criminal activity, or even to blackmail them. Additionally, smart devices could be used as a tool for cyber attacks, with hackers potentially able to take control of entire networks of devices and use them to launch large-scale attacks.

Given these concerns, it is important for individuals, companies, and policymakers to carefully consider the ethical and societal implications of smart devices and the data they collect. This may involve implementing stronger privacy protections, such as data minimization and encryption, as well as increased transparency around the types of data being collected and how it is being used. It may also involve exploring alternative business models that do not rely on the

collection and monetization of personal data. Ultimately, any approach to smart devices and data collection must be grounded in a careful consideration of the ethical and societal implications, and a commitment to protecting the privacy and security of individuals.

5 Conclusion

In conclusion, the proliferation of smart environments and the Internet of Things (IoT) raises pressing concerns regarding individual privacy and data protection. Smart meters, in particular, can reveal intimate details about our daily lives, making this information valuable to various entities such as marketers, law enforcement, insurance companies, landlords, and employers.

Through a philosophical analysis of privacy and ethical considerations in smart environments, specifically focusing on smart meters, this paper has highlighted the importance of integrating both deontological and consequentialist perspectives in decision-making. Ethical considerations, in conjunction with the General Data Protection Regulation (GDPR), can guide manufacturers and service providers to ensure compliance with legal requirements and protect consumer privacy.

This paper emphasizes the critical role of consumer awareness and transparency in addressing privacy-related issues. Individuals have the right to know what information is being collected about them and how it is being used. The findings suggest that effective data protection and privacy preservation can be achieved through adherence to laws and regulations, as manufacturers and providers of smart devices often prioritize profit over consumer privacy concerns.

In light of these insights, it is imperative for consumers, manufacturers, and policymakers to adopt a comprehensive and ethical approach to smart environments, particularly smart meters, to mitigate privacy risks and ensure the responsible use of technology.

References

1. Castelluccia, C.: Behavioural Tracking on the Internet: A Technical Perspective, pp. 21–33. Springer, Dordrecht (2012). https://doi.org/10.1007/978-94-007-2903-2_2
2. Council of Europe: Guide on article 8 of the convention - right to respect for private and family life. In: European Convention on Human Rights, pp. 183–233. Bloomsbury Academic (2013). https://doi.org/10.5040/9781472561725.0014
3. Datatilsynet (Norwegian Data Protection Authority): Avanserte måle- og styringssystem (AMS) (June 2018), https://www.datatilsynet.no/personvern-pa-ulike-omrader/overvaking-og-sporing/strommaling/. Accessed 12 Mar 2023
4. European Parliament and Council: 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) (Text with EEA relevance) (May 2016). http://data.europa.eu/eli/reg/2016/679/oj/eng

5. Fabrègue, B.F., Bogoni, A.: Privacy and security concerns in the smart city. Smart Cities **6**(1), 586–613 (2023)
6. Gerber, N., Gerber, P., Volkamer, M.: Explaining the privacy paradox: a systematic review of literature investigating privacy attitude and behavior. Comput. Secur. **77**, 226–261 (2018)
7. Greveler, U., Glösekötter, P., Justus, B., Loehr, D.: M0ultimedia content identification through smart meter power usage profiles. In: Proceedings of International Conference Information Knowledge Engineering (IKE) (January 2012)
8. Horta, O., O'Brien, G.D., Teran, D.: The definition of consequentialism: a survey. Utilitas **34**(4), 368–385 (2022). https://doi.org/10.1017/S0953820822000164
9. ICO: Privacy regulators study finds internet of things shortfalls (September 2016). https://www.aki.ee/en/news/privacy-regulators-study-finds-internet-things-shortfalls. Accessed 12 Mar 2023
10. Jakobi, T., Patil, S., Randall, D., Stevens, G., Wulf, V.: It is about what they could do with the data: a user perspective on privacy in smart metering. ACM Trans. Comput.-Hum. Interact. **26**(1), 1–44 (2019)
11. Kabulov, A., Saymanov, I., Yarashov, I., Muxammadiev, F.: Algorithmic method of security of the internet of things based on steganographic coding. In: 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), pp. 1–5. IEEE (2021)
12. Lucivero, F.: Big data, big waste? A reflection on the environmental sustainability of big data initiatives. Sci. Eng. Ethics. **26**(2), 1009–1030 (2020)
13. Misselbrook, D.: Duty, kant, and deontology. Br. J. Peneral Pract. R. Coll. Gen.l Practi. **63**, 211 (April 2013). https://doi.org/10.3399/bjgp13X665422
14. Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., Irwin, D.: Private memoirs of a smart meter. In: Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building. ACM (July 2010). https://doi.org/10.1145/1878431.1878446
15. Reinsel, D.: How you contribute to today's growing datasphere and its enterprise impact (Mar 2023), https://blogs.idc.com/2019/11/04/how-you-contribute-to-todays-growing-datasphere-and-its-enterprise-impact/
16. Schouw, B.: GDPR and IoT: three things you need to know (July 2017). https://www.linkedin.com/pulse/gdpr-iot-three-things-you-need-know-bart-schouw. Accessed 12 Mar 2023
17. Singh, A.K., Kumar, J.: A secure and privacy-preserving data aggregation and classification model for smart grid. Multim. Tools Appl. **82**, 22997–23015 (2023)
18. Singh, R., et al.: Highway 4.0: Digitalization of highways for vulnerable road safety development with intelligent IoT sensors and machine learning. Saf. Sci. **143**, 105407 (2021)
19. SmartBear: Iot and it's impact on testing. https://smartbear.com/blog/internet-of-things-101/. Accessed 12 Mar 2023
20. Soltan, S., Mittal, P., Poor, H.V.: BlackIoT: IoT botnet of high wattage devices can disrupt the power grid. In: 27th USENIX Security Symposium (USENIX Security 18). pp. 15–32. USENIX Association, Baltimore, MD (August 2018). https://www.usenix.org/conference/usenixsecurity18/presentation/soltan