sciendo

MARKETING OF SCIENTIFIC AND RESEARCH ORGANIZATIONS, 2021, Vol. 41, Issue 3, p. 21–38
pISSN 2353-8503
eISSN 2353-8414

ATTITUDES OF YOUNG CONSUMERS ON THE SECURITY OF THEIR DATA COLLECTED BY SMART DEVICES IN THE AGE OF THE INTERNET OF THINGS

MŁODZI KONSUMENCI WOBEC BEZPIECZEŃSTWA SWOICH DANYCH POBIERANYCH PRZEZ INTELIGENTNE URZĄDZENIA W DOBIE INTERNETU RZECZY

Beata Kolny
University of Economics in Katowice, Faculty of Economics, Market and Consumption Department
ul. 1 Maja 50, 40-287 Katowice, Poland
beata.kolny@ue.katowice.pl ● ORCID 0000-0002-9162-1704

DOI: 10.2478/minib-2021-0013

ABSTRACT

The popularity of smart devices that collect and share data on user behaviour grows every year, and the number of such devices in households is forecast to rise steadily. Therefore, the purpose of this paper is to present the attitudes of young consumers regarding the security of their data collected by smart devices, interconnected via the existing Internet infrastructure or other network technologies within the Internet of Things (IoT) systems. The paper was written based on both secondary and primary sources of information. Secondary sources were used to define the discussed issues related to the Internet of Things and the security of data collected by smart devices. Primary sources, on the other hand, offered direct evidence of the attitudes of young consumers on the security of such data. Direct research was carried out using an online survey carried out in 2021 on a sample of 588 consumers aged 18–34 living in Poland. The results show that more than half of the respondents pay great attention to where the data collected by the devices used in their households is kept and whether such data is safe. In spite of such declarations, more than half of those surveyed have no knowledge about the level of the security of such data. The respondents agreed with the statement that consumers accepted the uncertainty related to the loss of control over their personal data collected by smart devices more quickly than the risk involved in becoming disconnected from them.

Key words: Internet of Things, smart devices, data security, consumers

ABSTRAKT

Inteligentne urządzenia, które w trakcie funkcjonowania gromadzą i udostępniają dane o zachowaniach użytkowników, z roku na rok zyskują coraz większą popularność. Prognozuje się, że ich liczba w gospodarstwach domowych będzie stale wzrastać. W związku z tym celem artykułu jest zaprezentowanie stosunku młodych konsumentów do bezpieczeństwa swoich danych pobieranych przez inteligentne urządzenia, połączone istniejącą infrastrukturą internetową lub innymi technologiami sieciowymi w ramach Internetu rzeczy. Artykuł napisano na podstawie wtórnych i pierwotnych źródeł informacji. Informacje wtórne pozwoliły na zdefiniowanie omawianych zagadnień związanych z Internetem rzeczy oraz bezpieczeństwem danych pobieranych przez inteligentne urządzenia, informacje pierwotne natomiast pokazały stosunek młodych konsumentów do bezpieczeństwa tych danych. Badania bezpośrednie przeprowadzono metodą ankiety internetowej w 2021 roku na próbie 588 konsumentów w wieku 18–34 mieszkających w Polsce. Uzyskane wyniki wskazują, że ponad połowa respondentów zwraca dużą uwagę na to, gdzie są gromadzone dane pobierane przez urządzenia wykorzystywane w ich gospodarstwach domowych i czy te dane są bezpieczne. Mimo tych deklaracji ponad połowa respondentów nie ma wiedzy na temat stopnia zabezpieczania takich danych. Badani zgodzili się ze stwierdzeniem, że konsumenci szybciej akceptują niepewność związaną z utratą kontroli nad swoimi danymi osobowymi pobieranymi przez inteligentne urządzenia niż ryzyko rozłączenia się z nimi.

Słowa kluczowe: Internet rzeczy, inteligentne urządzenia, bezpieczeństwo danych, konsumenci

JEL: D12, D19, O33, L86

Introduction

The Internet can be perceived, on the one hand, as a static archive of information, and on the other as a rapidly growing interactive system, in which objects can identify one another and are endowed with "intelligence" through the ability to communicate information about themselves and access data collected by other objects. As the number of devices connected to the Internet continues to grow, so do the possibilities offered by the use of technology to forge connections not only between people but also between objects and between objects and people. The Internet of Things (IoT) has evolved from a network of interconnected computers (as well as

smartphones and tablets) to a network of interconnected objects. These include home electronics (e.g. smart TVs and streaming servers), household appliances (e.g. smart ovens, washing machines and refrigerators) and smart home automation devices (e.g. alarm systems, thermostats and smoke detectors), as well as smart medical equipment, cars, airplanes, houses, towns, cities and even countries. It is safe to assume that the Internet of Things comprises all interconnected things that can be monitored and controlled, and remain connected to the Internet at all times, which allows them to communicate and exchange information. However, the Internet of Things means that objects are not only interconnected but also capable of working autonomously with little need for human intervention. In this way, the Internet of Things facilitates the active participation of things/objects in the human environment, for example by sharing information with other network users or members using wireless technology. In the Internet of Things, objects can autonomously identify events and changes in their surroundings and act and react appropriately without human intervention (Malucha, 2019, p. 57).

The traditional Internet differs from the Internet of Things in that the former involves such objects as computers, smartphones and tablets that are interconnected chiefly for the purpose of being used by humans. People use such devices to connect to the Internet, search for information, send emails, watch films, listen to music and so on. In the Internet of Things, in turn, data is additionally collected and exchanged by devices in what is referred to as machine-to-machine communication, or M2M (Miller, 2015). Since the collection of data within the Internet of Things is indispensable, it is crucial to ensure that such data can be managed and communicated in a secure manner that protects user privacy. Therefore, protecting consumer data to prevent unauthorized access and maintain their integrity is crucially important for their IoT transmission (Krawiec, 2020, p. 74).

Kwiatkowska (2014, p. 69) argues that as the Internet of Things evolves, it is necessary to build trust in such systems and guarantee to users that the data generated in the network is protected from unauthorized access. Without trust, it is not possible to exploit the full potential of the IoT. Most users realize that, for example, Google mobile apps track their location, but

this is done to provide them with additional benefits. However, there are situations in which users may not be aware of what data is collected and when. For example, this happens when applications are running in the background, the devices on which they are installed remain inactive or users forget to turn them off. It will not be possible to fully tap into the potential of IoT devices unless people are confident that these objects pose no major threats to their privacy.

Given that network-connected devices have become commonplace to such an extent in today's households, the purpose of this paper is to examine the attitudes of young consumers — who inevitably have or will have contact with smart devices interconnected via the existing Internet infrastructure or other network technologies within the framework of IoT systems — regarding the security of their data collected by those devices.

Material and Methodology

The study utilized both secondary and primary sources of information. Secondary sources were used to characterize issues related to the Internet of Things and the security of data collected by IoT devices. Information from secondary sources was supplemented by information from primary sources gathered by the author through direct research using an online survey taken between 1 March 2021 and 18 May 2021. The study questionnaire was made available through the SurveyMonkey platform, and the link was sent to potential respondents by email. The sample of 588 individuals was selected to consist exclusively of young consumers aged 18–34, with 50% of the sample being women, the other 50% men. Among those surveyed, 20.7% lived in rural areas, 27.6% in cities of up to 99,000 inhabitants, 24.0% in cities of 100,000–199,000 inhabitants and 27.7% in cities of more than 200,000 inhabitants. Most respondents rated the financial situation of their households as "good" (63.8%) and stated that they were able to afford certain luxury goods. Among those surveyed, 26.0% rated the financial situation of their households as "sufficient" (i.e. they were forced to budget for all major purchases), compared with 9.7% who declared that their financial situation was "very good" and only 0.5% who rated the condition of their finance as "bad". For the purposes of this

paper, it appeared useful to examine the competence of the respondents in the use of objects and tools necessary to operate smart devices. "Very good" skills at using smartphones were declared by 70,1% of the respondents, at using tablets by 49.8% of the respondents and at using various Internet applications by 61.9% of the respondents. When the declarations of "good" and "very good" skills were aggregated, the percentage shares in almost all cases rose to well over 90% (except for tablets, where "good" and "very good" skills at using those devices were declared by a total of 75.8% of the respondents).

Defining the Internet of Things

The Internet of Things is generally seen as being comprised of four different elements: devices that allow the active collection and transmission of measuring data that represents how they function; a communication network that connects devices (i.e. the Internet); IT systems capable of collecting incoming data; analytical solutions that process the data and allow conclusions to be drawn and additional business value to be created (Rozmus, 2019, pp. 65–66). As a result of difficulties in defining the concept, the Internet of Things may also be understood as including the following: the use of radio frequency identification (RFID) technology to determine the location (markings) of objects in order to monitor their position; communication between machines, or communication between devices aimed at optimizing their performance; the use of a network of sensors to transmit data and information from these objects to the network (Mazurek, 2018). In addition, the Internet of Things can be understood as all smart objects capable of reacting to their surroundings, as well as processing and remembering digital information and transmitting it to other objects (and users) via Internet protocols. In considering the use of the word "smart" to describe such objects, we can assume that objects can be called smart if they can be managed and controlled remotely (for example by setting a timer to preheat an oven or turning on a dishwasher or a washing machine) via smartphone or tablet applications (Miller, 2015), share data about themselves and provide access to the information collected by other things.

The person who claims to have coined the term "Internet of Things" is Kevin Ashton, who first used the words as the title of a presentation at Procter & Gamble in 1999, explaining that "[l]inking the new idea of RFID in P&G's supply chain to the then-red-hot topic of the Internet was more than just a good way to get executive attention" (Ashton, 2009). He argued that computers and the Internet depended on people for information because almost all the data available on the Internet had been posted there by people. He observed that humans nonetheless had "limited time, attention and accuracy" to capture and create data, but no such limitations applied to RFID and sensor technology, which was why the Internet of Things could transform the world, perhaps even more profoundly than the Internet did (Ashton 2009). A transformed world will become possible thanks to communication not only between humans and smart objects but also between smart objects themselves, and such communication will be enabled anytime, anywhere and on any medium (Kwiatkowska, 2014, p. 60). In the position paper on standardization for Internet of Things technologies issued in January 2015 by the European Research Cluster on the Internet of Things (IERC), the Internet of Things is defined as a "dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network" (Guillemin et al., 2015, p. 13, quoted after Vermesan et al., 2011, p. 10). Another definition emphasizes that the Internet of Things is "[a]n open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment" (Madakam et al., 2015, p. 165). According to another source, the term "Internet of Things" was coined "to reflect the growing number of smart, connected products and highlight the new opportunities they can represent" (Porter & Heppelmann, 2014). One of the simplest definition of the Internet of Things is as "a system of physical objects that can be discovered, monitored, controlled, and interacted with by electronic devices that communicate over various networking interfaces and can be

connected to the wider internet" (Guinard & Trifa, 2016, p. 3). The devices that can be connected within the IoT may vary greatly, including in terms of size. Importantly, the "things" in the Internet of Things do not actually have to have a physical form. They may include points or sets of data, for example information about a person's location or the temperature in a room collected by a dedicated device such as a thermostat or a smartphone (Miller, 2015). In addition, the word "things" may comprise both living things (such as human beings, animals, and plants), as well as inanimate ones (Madakam et al., 2015, p. 165). Consequently, the Internet of Things is formed by all objects equipped for example with sensors/detectors. However, this does not mean that a specific object must be directly connected to the Internet. But to connect to the IoT, objects must be able to communicate, which means sending and receiving data (e.g. Auto-ID, short-range radio transmission such as Bluetooth, ZigBee and NFC, as well as Wi-Fi networks; Guinard & Trifa, 2016). Such communication means that devices must be on the one hand fitted with sensors (such as temperature, vibration, humidity and movement sensors, as well as GPS) to collect information from their surroundings and pass it on and on the other hand capable of receiving a transmitted signal, processing it and triggering a specific reaction (such devices include smartphones, tablets, computers or other objects that will automatically perform a specific action; Kokot & Kolenda, 2016).

The research and advisory company Gartner forecasted that there would be 8.4 billion connected things in use worldwide in 2017. Most of these (5.2 billion, or 63% of all applications in use) would be used by consumers and their households (Gartner, 2017). According to data published on Statista, the total installed base of IoT-connected devices is expected to reach 30.9 billion units worldwide by 2025, compared with 13.8 billion units projected in 2021. In turn, the total base of non-IoT devices (such as smartphones, laptops and computers) is expected to reach just over 10 billion units by 2025, three times less than the IoT units (Statista, 2021). Moreover, statistics from 2019 show that one in four Poles would like to have IoT devices in their homes, chiefly to improve their quality of life (for the purpose of monitoring utilities as well as home and health monitoring; Statista, 2019). Apart from offering unquestioned

benefits, smart devices and houses also raise certain concerns. A survey commissioned by Dynatrace and taken on a sample of 10,002 respondents in eight countries of the world (the UK, the US, France, Germany, Australia, Brazil, Singapore and China) found that 73% of the respondents feared being locked in or out of a smart home. Those surveyed were also concerned that they would not be able to control the temperature or lights in a smart home (68% and 64% respectively; Dynatrace, 2018). When it comes to consumer trust in the IoT, Cisco's report *The IoT Value/Trust Paradox* from 2017 describes the findings a survey of 3,000 consumers. According to the report, consumers noticed the growing value of IoT services, but they were very concerned about the security of their data and how it was used. Only 9% of the respondents believed that their data was secure, and only 14% believed that companies did a good job of informing them what data they collected and how they used such information. Despite expressing mistrust, however, consumers would not want to disconnect from the IoT devices: 42% said that such devices were too integrated into their daily lives for them to disconnect, regardless of the perceived risks. The same survey also found that the share of consumers who correctly identified personal IoT devices such as wearables and home security systems was more than twice as large that the share of the respondents who recognized public IoT devices such as streetlights, energy meters and traffic systems (63% versus 27%, respectively). Such results show that consumers are less aware of public IoT implementations (Cisco, 2017). According to the antivirus software company Bitdefender, typical IT devices such as computers, tablets, laptops, routers, smartphones and consoles account for slightly under two thirds of all devices in a home network, while IoT devices (such as robot vacuums, smart light bulbs, etc.) account for the remaining one third. It is expected that the number of IoT devices will continue to grow, which will greatly increase the risk that the data of their owners will be intercepted (Krakowiak, 2020). When consumers and their households decide to purchase smart devices, they must therefore pay attention to the manufacturer's policy on releasing updates and bug fixes and keep their information secure on an ongoing basis.

Data Security in the Internet of Things

Data security in the Internet of Things is understood as the security of information collected by devices connected to the network. Guaranteeing data security involves meeting the requirements of data availability, confidentiality and integrity. Availability means that the data must be available exactly when it is needed. Confidentiality requires data owners or administrators to decide on who can access data, and data integrity requires data accuracy, authenticity, timeliness, and completeness. However, the existing infrastructure appears insufficient to manage Internet of Things systems (Karimi & Atkinson, 2013, p. 14). Similarly, in the opinion of Sikorski & Roman (2020, p. 46), data security is the most immature aspect of the IoT despite the fact that every business must implement numerous security measures to guarantee product quality from both technological and organizational perspectives. It is important to have clear information about the data being collected and processed, the assigned role of the data controller and the international standards, as well as norms and certifications that have been implemented. Polish provisions regulating the use of the Internet of Things can be divided into four basic groups: legal regulations relating to cyber-security, regulations on protecting personal data and privacy, provisions of civil law dealing with accountability for harm caused by unsafe products, and provisions dealing with intellectual property rights (Konarski, 2000).

Security aspects should be considered and addressed from the very beginning of the IoT design process. Security by design is a popular concept that aims to encourage businesses to plan security features from the outset, as opposed to additional, hasty implementations made at the end of the design process or after the launch of product sales (Wytrębowicz et al., 2020, p. 69).

In the implementation of security features in the development of the IoT, the recommendations of the International Telecommunication Union (ITU) may be used as a point of reference. The recommendations list the functional requirements for IoT devices in the area of the processing, storage, transmission and aggregation of data from IoT elements (Krawiec, 2020, p. 74). One of the key elements ensuring cyber security is a gateway.

This is an IoT unit that connects devices to the communication network and translates communications between network protocols and device protocols. In order to ensure the security of applications, the ITU recommends that gateways control access to devices and to themselves, protect data security and confidentiality for themselves and devices, and support self-management and remote maintenance. In order to meet the requirement of security and confidentiality, gateways must support identification access to IoT devices, mutual authentication with applications, the security of data transmission and storage, and confidentiality protection mechanisms, among other things. As for the requirement of self-management and remote maintenance, gateways must support self-diagnosis, self-repair, remote maintenance, software updates and automatic configuration or configuration by applications (International Telecommunication Union, 2017, p. 2, 9).

Given that IoT devices can be so attractive to consumers, they must be informed about the risks associated with the use of such devices and the security measures they should adopt (Royal Society, 2017). Using IoT devices may pose a problem related to ownership. Obviously, consumers become owners of the physical devices they purchase, but they may not have full ownership of the data being collected within IoT systems. Issues that should be resolved are related to the question of who owns such data, restrictions in data processing and transfer to third parties, free updates and access to data for consumers. In addition, consumers should be made aware of any threats that may be posed, for example by the collection of data by voice-control devices. If the manufacturer of devices is able to remotely decide about what functions are available, this may be seen as a disadvantage of IoT systems (Maj, 2015, p. 54).

Another issue related to the security of IoT systems is the protection of the privacy of both the users of such systems and any third parties whose data is simultaneously collected. Privacy threats typically result from a careless approach to the security of these systems. Threats can be mitigated by the proper design of security policies, which provide the basis for such implementations as authentication, encryption and access rights (Wytrębowicz et al., 2020, p. 69). Businesses implementing IoT systems must remember that they need users' consent to share detailed data on how

those users interact with IoT devices. Consumers must be offered true and reliable solutions that will balance their privacy concerns related to how the data that accurately profile their daily behaviours might be used in the future, as well as to who will be using such data and how. This will allow them to make informed decisions about providing data about their behaviour to obtain significant benefits. A survey conducted on 6–31 May 2015 on a sample of 1,121 individuals by IAB Polska and GoldenSubmarine found that 47% of the respondents feared leaks of their data and the data of their loved ones, 43% were concerned about privacy loss, and 34% feared loss of control over devices. However, it is worth mentioning the main benefits associated with the use of IoT devices and the hopes expressed by consumers. Among the respondents, as many as 38% expected a greater sense of personal security, 28% expected the security of their loved ones to improve, and 20% hoped for better security in the context of their health (Kolenda, 2016, p 30). IoT users expected above all a greater sense of security in the broad sense, control over their devices and appliances, as well as comfort and the possibility to save money. In the eyes of the respondents, such benefits could most easily be provided by technologies allowing the smart management of devices, appliances and energy in their homes (Krejtz, 2016, pp. 26–27). Ensuring the privacy of users remains important in this context.

Survey Results and Discussion

A survey of opinions on IoT data security conducted by the present author found that one in two respondents pay great attention to where data collected by devices used in their households is kept and whether such data is secure. Such declarations were more likely to be made by men (57.7%) than by women (46.2%). One in three respondents answered that they had not thought about such issues, and the share of women who declared this was significantly greater than the share of men (41% compared with 24.4%). Nearly 12% of respondents declared that they did not pay any attention to where their data was kept and whether it was secure (Table 1). Other responses included, in particular, statements that respondents had

no control over where data is kept. Some of the respondents answered that although they tried to pay attention to such issues, and would rather keep data sharing to a minimum, they had no control over this process and were forced to accept it if they wanted to use such devices. Other respondents, in turn, were aware that their data was being collected, but did not pay much attention to this fact. In addition, they paid attention to where the data was kept depending on what types of devices wanted to access their data and whether data collection was needed to continue to use such devices. The respondents also replied that they sometimes paid attention to where the data collected by such devices was kept, but they did not always do so, and that they found data security important and believed that the manufacturer's assurances in this respect were sufficient. Where possible, they also tried to minimize the amount of data they shared, and were careful not to provide any sensitive data.

Table 1. Attitudes Towards Data Collection by Smart Devices, by Gender (in %)

Specification	Total sample	Respondents by gender	
		Women	Men
I pay great attention to where the data collected by the devices used in my household is kept and whether such data is secure.	52.0	46.2	57.7
I have not thought about where the data collected by the devices used in my household is kept and whether such data is secure	32.7	41.0	24.4
I pay no attention to where the data collected by the devices used in my household is kept and whether such data is secure.	12.0	11.4	12.7
Other	3.3	1.4	5.2

When the respondents were asked about their opinion about the security of consumer and consumer behaviour data collected by smart devices, more than one in two (54.4%) had no knowledge about the level

of the protection of such data. Such an answer was more likely to be indicated by women (62.6%) than by men (46.2%). More than 28% of respondents felt that data collected by smart devices was not well protected. This answer was indicated by more women than men (36.1% and 20.7%, respectively) Only 17.2% of respondents believed that data collected by smart devices were well protected. The opinion was more likely to be expressed by men than by women (17.7% compared with 16.1%) (Table 2).

Table 2. Opinions on the Security of Data Collected by Smart Devices, by Gender (in %)

Specification	Total sample	Respondents by gender	
		Women	Men
I have no knowledge about the level of the protection of my data collected by smart devices	54.4	62.6	46.2
Data collected by smart devices is not well protected	28.4	20.7	36.1
Data collected by smart devices is well protected	17.2	16.7	17.7

The respondents were also asked to rate selected aspects of data security on a scale of one to seven, where one represented "strongly disagree" and seven "strongly agree." The survey found that most respondents agreed with the statement that before purchasing smart devices consumers wanted to know who would have access to their personal data collected by such devices, and whether such data would be secure (a mean rating of 4.68). Women were found to agree with this statement more than men (mean ratings of 4.77 versus 4.59). A slightly lower mean rating (4.56) was given to the statement that before purchasing smart devices consumers wanted to know where the data collected about them by these devices would be stored. Women were again found to agree with this statement more than men (mean ratings of 4.70 versus 4.43). Very similar mean ratings, confirming that respondents agreed with the statements in question, were given to the statements that consumers accepted the

uncertainty related to the loss of control over their personal data collected by smart devices more quickly than the risk of becoming disconnected (4.21) and that consumers were more concerned about disconnection from smart devices than the risk of losing control over them (4.15; see Table 3). Importantly, the results of the present study are consistent with the results presented in the Cisco report (Cisco, 2017). Despite not having sufficient knowledge about data security, respondents would not like to be disconnected from smart devices because they accepted the loss of control over smart devices more quickly than becoming disconnected.

Table 3. Attitudes Towards Selected Aspects of Data Security, by Gender (Mean Ratings*)

Specification	Total sample	Respondents by gender	
		Women	Men
Before purchasing smart devices, consumers want to know who will have access to their personal data collected by such devices and whether such data is secure	4.68	4.77	4.59
Before purchasing smart devices, consumers want to know where the data collected about them by such devices will be stored	4.56	4.70	4.43
Consumers accept the uncertainty involved in losing control over their personal data collected by such devices more quickly than they accept the risk of becoming disconnected from them	4.21	4.22	4.19
Consumers fear becoming disconnected from smart devices more than the risk of losing control of them	4.15	4.12	4.17

*On a scale from one to seven, where one represented "strongly disagree" and seven "strongly agree."

Summary

Ever-more rapid technological advances have created an extremely interesting world for consumers, offering countless possibilities of communication between humans, between objects and humans and

between these objects themselves — all this with little or no human intervention. Such technologies are aimed at helping humans perform daily tasks faster and more easily. But despite offering unquestioned benefits, the use of smart devices also poses dangers related to the collection of user data by such devices. As the popularity of IoT systems grows every year, devices that are connected or have access to the network have become commonplace in homes. A survey of consumer attitudes to the security of data collected by smart devices (connected to the existing Internet infrastructure or using another network technology) found that more than half of the respondents declared that they pay great attention to where the data collected by devices used in their household was kept, and whether such data was secure — and so we may assume that they treat their interactions with IoT devices very consciously and responsibly. But on the other hand, we note that at the same time, more than half of them declared that they had no knowledge about the level of the protection of the data that smart devices collected about them. This observed discrepancy in responses may indicate that the respondents wanted to present themselves as being more responsible and competent than they actually are, or that such responses were given by those who declared that they did not pay attention to where their data is kept and do not think about the issue. Only just over 17% of respondents believed that the data collected by smart devices was well protected, which points to the importance of detailed information in this regard and educational efforts towards rasing consumers' awareness about the security of their data gathered under the framework of the IoT. In addition, respondents agreed with the statement that consumers accepted the uncertainty involved in losing of control over their personal data collected by smart devices more quickly than they accepted the risk of becoming disconnected, and the statement that they were more concerned about becoming disconnected from smart devices than about the risk of losing control over them. These findings suggest that the possibility of using such devices is more important to consumers than the security of their data. Finally, it is worth noting the limitations of the presented findings — these include the non-representative nature of the sample and reliance on the declarations of respondents pertaining to general aspects of data security, without detailed investigation of the specific functions of individual devices and their security.

References

1. Ashton, K. (2009, 22 June). *That 'Internet of Things' Thing: In the real world, things matter more than ideas*. RFID Journal. Retrieved May 4, 2021, from http://www.rfidjournal.com/articles/pdf?4986
2. Cisco. (2017, December 12). *Cisco Survey Reveals Divide Between IoT Value and Trust* [Press release]. The Newsroom: Cisco's Technology News Site. Retrieved June 23, 2021, from https://newsroom.cisco.com/press-release-content?articleId=1900060
3. Dynatrace. (2018). *IoT Consumer Confidence Report: Challenges for Enterprise Cloud Monitoring on the Horizon*. Retrieved June 14, 2021, from https://assets.dynatrace.com/en/docs/report/2824-iot-consumer-confidence-report-dynatrace.pdf
4. Gartner. (2017, February 7). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016* [Press release]. Retrieved June 17, 2021, from https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016
5. Guillemin, P., Berens, F., Vermesan, O., Friess, P., Carugi, M., & Percivall, G. (Eds.). (2015, January). *Internet of Things: Position Paper on Standardization for IoT Technologies*. European Research Cluster on the Internet of Things (IERC). Retrieved June 22, 2021, from http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Standardization_Final.pdf
6. Guinard, D. D., & Trifa, V. M. (2016). *Building the Web of Things: With examples in Node.js and Raspberry Pi*. Manning Publications.
7. International Telecommunication Union (2017, October 29). *Recommendation ITU-T Y.4101/Y.2067. Common requirements and capabilities of a gateway for Internet of things applications*. http://handle.itu.int/11.1002/1000/13384
8. Karimi, K., & Atkinson, G. (2013, June). *What the Internet of Things (IoT) Needs to Become a Reality* [White paper]. Freescale Semiconductor & Arm. https://www.mouser.com/pdfdocs/INTOTHNGSWP.PDF
9. Kokot, W., & Kolenda, P. (2016). *Czym jest Internet rzeczy* [What Is the Internet of Things]. In P. Kolenda (Ed.), Internet rzeczy w Polsce. Raport. IAB Polska [Report] (pp. 8–11). ICAN. https://www.iab.org.pl/wp-content/uploads/2016/05/Raport-Internet-Rzeczy-w-Polsce.pdf
10. Kolenda, P. (2016). *Pierwsze badanie Internetu rzeczy w Polsce* [The first survey of the Internet of Things in Poland]. In P. Kolenda (Ed.), Internet rzeczy w Polsce. Raport, IAB Polska [Report] (pp. 28-30). https://www.iab.org.pl/wp-content/uploads/2016/05/Raport-Internet-Rzeczy-w-Polsce.pdf
11. Konarski, X. (2020, 17 June). *Internet Rzeczy — najważniejsze regulacje prawne w Polsce* [Internet of Things — the most important legal regulations in Poland]. Traple Konarski Podlecki. Retrieved on July 28, 2021, from https://www.traple.pl/2020/06/17/internet-rzeczy-najwazniejsze-regulacje-prawne-w-polsce/
12. Krakowiak, L. (2020, November 30). *Potężny wzrost ataków ma urządzenia IoT* [A surge in attacks on IoT devices]. Computerworld. Retrieved June 20, 2021, from https://www.computerworld.pl/news/Potezny-wzrost-atakow-na-urzadzenia-IoT,424095.html

13. Krawiec, J. (2020). *Internet Rzeczy (IoT). Problemy cyberbezpieczeństwa* [Internet of Things (IoT): Cyber security problems]. Oficyna Wydawnicza Politechniki Warszawskiej.
14. Krejtz, K. (2016). Prywatność w Internecie rzeczy [Privacy in the Internet of Things]. In P. Kolenda (Ed.), *Internet rzeczy w Polsce. Raport. IAB Polska* [Report] (pp. 26–27). ICAN. https://www.iab.org.pl/wp-content/uploads/2016/05/Raport-Internet-Rzeczy-w-Polsce.pdf
15. Kwiatkowska, E. M. (2014). Rozwój Internetu rzeczy — szanse i zagrożenia [The development of the Internet of Things — opportunities and threats]. *Internetowy Kwartalnik Antymonopolowy i Regulacyjny*, *8*(3), 60–70. https://ikar.wz.uw.edu.pl/images/numery/22/pdf/60.pdf
16. Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications, 3*(5), 164–173. https://doi.org/10.4236/jcc.2015.35021
17. Maj, I. (2015). Internet rzeczy i zagrożenia z nim związane [The Internet of Things and Related Threats]. *Bezpieczeństwo. Teoria i praktyka*, *3*, 51–57. Oficyna Wydawnicza AFM.
18. Malucha, M. (2018). Internet rzeczy — kontekst technologiczny i obszary zastosowań [Internet of Things — the technological context and areas of application]. *Studia i Prace WNEIZ US*, *54/2*, 51–69. https://doi.org/10.18276/sip.2018.54/2-04
19. Mazurek, G. (2018). Internet Rzeczy a cyfrowa transformacja — implikacje dla marketingu B2C [The Internet of Things and the digital transformation — implications for B2C marketing]. In Ł. Sułkowski & D. Kaczorowska-Spychalska (Eds.), *Internet of Things. Nowy paradygmat rynku* (pp. 33–57). Difin.
20. Miller, M. (2015). *The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities Are Changing the World*. Que Pub.
21. Porter, M. E., & Heppelmann, J. E. (2014). How Smart, Connected Products Are Transforming Competition. *Harvard Business Review*, *92*(11), 64–88. Retrieved from https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition
22. Royal Society. (2017, December). *The Internet of Things: Opportunities and threats. Conference report*. Retrieved June 22, 2021, from https://royalsociety.org/~/media/events/2017/10/tof-iot/iot-conference%20report-final.pdf
23. Rozmus, S. (2019). Gospodarstwo domowe w dobie Internetu Rzeczy [Households in the era of the Internet of Things]. *Rocznik Kolegium Analiz Ekonomicznych*, *54*, 61–73.
24. Sikorski, M. (Author), & Roman, A. (Ed.) (2020). *Internet Rzeczy* [Internet of Things]. Wydawnictwo Naukowe PWN.
25. Statista. (2019, December 16). *Share of consumers interested in Internet of Things improvements in Poland in 2019, by type of improvement*. Retrieved June 21, 2021, from https://www.statista.com/statistics/1083078/poland-interest-in-internet-of-things-improvements/
26. Statista. (2021, March 8). *Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025*. Retrieved June 21, 2021, from https://www.statista.com statistics/1101442/iot-number-of-connected-devices-worldwide/

27. Vermesan, O., Friess P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., Jubert, I. S., Mazura, M., Harrison, M., Eisenhauer, M., & Doody, P. (2011). Internet of Things Strategic Research Roadmap. In O. Vermesan & P. Friess (Eds.), *Internet of Things — Global Technological and Societal Trends* (pp 9–52). River Publishers.
28. Wytrębowicz, J., Radziszewski, P., & Cabaj, K. (2020). *Inżynieria systemów Internetu rzeczy. Zagadnienia bezpieczeństwa i komunikacji* [Engineering aspects of the Internet of Things systems: Issues of security and communication]. Oficyna Wydawnicza Politechniki Warszawskiej.

Beata Kolny, PhD, DSc, Associate Professor of the University of Economics in Katowice — holds the degree of *doctor habilitowany* (DSc) in economic sciences. She is an Associate Professor of the University of Economics in Katowice and head of the "Culture Manager" post-graduate studies program. She has implemented numerous research projects, both alone as well as in teams of market and consumption researchers and in interdisciplinary teams. She has been involved in the implementation of projects funded by six grants (from the State Committee for Scientific Research, the Polish Ministry of Science and Higher Education, and the National Science Centre). She specializes in market and consumption research, especially the behaviour of market participants. Her scientific interests centre around leisure time, especially the market of leisure services.