Maiorescu, Irina; Gabudeanu, Larisa; Vîlcea, Alexandru-Lucian; Sabou, Gabriel-Cristian; Dârdală, Marian

Article

Intrusiveness and data protection in iot solutions for smart homes. amfiteatru

Amfiteatru Economic Journal

Provided in Cooperation with:
The Bucharest University of Economic Studies

Suggested Citation: Maiorescu, Irina; Gabudeanu, Larisa; Vîlcea, Alexandru-Lucian; Sabou, Gabriel-Cristian; Dârdală, Marian (2021) : Intrusiveness and data protection in iot solutions for smart homes. amfiteatru, Amfiteatru Economic Journal, ISSN 2247-9104, The Bucharest University of Economic Studies, Bucharest, Vol. 23, Iss. 57, pp. 429-447, https://doi.org/10.24818/EA/2021/57/429

This Version is available at:
https://hdl.handle.net/10419/281580

INTRUSIVENESS AND DATA PROTECTION IN IoT SOLUTIONS FOR SMART HOMES

Irina Maiorescu[1*], Larisa Gabudeanu[2], Alexandru - Lucian Vîlcea[3], Gabriel - Cristian Sabou[4] and Marian Dârdală[5]
[1)3)4)5)] *Bucharest University of Economic Studies, Romania*
[2)] *Babeş-Bolyai University, Cluj-Napoca, Romania.*

Please cite this article as:
Maiorescu, I., Gabudeanu, L., Vilcea, A.L, Sabou, G.C. and Dardala, M., 2021. Intrusiveness and Data Protection in Iot Solutions for Smart Homes. *Amfiteatru Economic*, 23(57), pp.429-447.

DOI: 10.24818/EA/2021/57/429

Article History
Received: 30 December 2020
Revised: 3 February 2021
Accepted: 17 March 2021

Abstract
The use of Internet of Things devices (IoT) by individuals in their homes has led to new opportunities for companies, to adapt their products, services and offers, based on the user profile. At the same time, these new services involve the reinterpretation of existing requirements regarding data protection, especially in terms of the ethics of using data and the security of personal data. The paper analyses in the scientific literature the intrusiveness generated by aggregations of personal data, the responsibility for data protection and user's perception of these issues. It presents further the results of a quantitative research on 183 respondents of all genders and working in different sectors of activity, with the aim of assessing the perception of intrusiveness and data protection in the use of their smart devices, with potential for IoT home interconnection. The results provide a new perspective on how smart device users relate to key issues from European data protection legislation. The study shows that there are differences explained by gender, age and parental status in the perception of intrusiveness and responsibilities for ensuring the security of aggregated data through IoT solutions. The results also show that accessing certain types of data is perceived as being more intrusive than others, and that respondents rely on other users' reviews to learn how data protection is provided through the IoT device.

Keywords: Internet of Things (IoT); GDPR; smart homes; smart devices; intrusiveness; data protection; data security;

JEL Classification: L86, M31, N44

* Corresponding author, **Irina Maiorescu** – e-mail: irina.maiorescu@com.ase.ro

Authors' ORCID:
Irina Maiorescu: orcid.org/0000-0003-1472-5136
Larisa Gabudeanu: orcid.org/0000-0002-2562-5344
Alexandru - Lucian Vîlcea: /orcid.org/0000-0002-0870-5668
Gabriel – Cristian Sabou: orcid.org/0000-0001-6428-2930
Marian Dârdală: orcid.org/0000-0003-2087-8817

Introduction

IoT solutions can be used in various areas, from industrial ones (e.g. factories, agriculture, producing and distributing energy), to those in the public interest (e.g. smart cities, smart and interconnected vehicles) and individual ones, such as smart homes (Maayan, 2020). In the last years, the use of smart devices with the potential of interconnection within IoT networks has increased (Statista, 2021**).** This rise has been noticed both for businesses, approximatively 34% of them using IoT solutions in 2019 (Vodafone, 2019), and for individuals (Maple, 2017).

People use various types of IoT solutions for their personal comfort and within their homes, such as smart TV, smart personal assistants, utility devices (e.g. light sources, outlets), smart surveillance cameras, smart electronic devices such as refrigerator, vacuum cleaner, air conditioning (Zheng et al., 2018), often in connection with a smart phone, smart watch or computer. There are debates in the scientific literature whether the smartphone can be included in the category of IoT objects (Futurelearn, 2020). However, the capabilities of this device to collect and transmit user data, such as location, pulse, temperature, applications used etc., turn it into IoT object (El Khaddar and Boulmalf, 2017; Norton, 2020). Furthermore, the European Union considers the term Internet of Things (IoT) as making reference to "the general concept of objects (electronic devices and daily used objects) that can be read, recognized, accessed, tracked and/or controlled remotely through the internet" (JO, 2010). An IoT device is "smart" through its hardware part, but also through its software part that can communicate and interact with the external environment, with other IoT devices or with the general management of the IoT device network (Dorsenmaine et al., 2015).

The interaction of these objects with the external environment and with other devices/IT systems involves the collection, storing and transfer of significant amounts of data, including personal data of their users or of those individuals found in their proximity. Such aggregated data are very valuable for companies, because they lead to understanding behavioural patterns, to creating user profiles (EDPS, 2016) – and, implicitly, exploiting these for own commercial purposes. At the same time, these smart devices can be the target of specific cybernetic attacks with the purpose of intercepting the data they transmit and obtaining gains for such data.

Data collected by the IoT devices – most often personal data, are usually stored also in other locations than in the IoT device used at home (such as cloud, various servers). For this reason, their protection, which is a legal requirement (EU Regulation 679/2016) is essential. The manner in which data has to be protected (including ensuring their security against improper processing and against unauthorized access) and used is stated by existing European legislation which includes the GDPR (EU Regulation 679/2016), liability for products and services and consumer protection. The proportionality of data processing (as mentioned under article 5 of the GDPR) implies the management of personal data in a manner expected by the user and not in manners which have an unjustified effect over the individual (ICO, 2018). Breaching the proportionality of data processing is closely linked to the intrusiveness concept described in the GDPR. At the same time, certain types of personal data need to be processed in order to ensure the security of IoT solution and for the improvement of existing systems.

The issue at hand is to find an equilibrium between intrusiveness and the obligation of IoT solutions providers to ensure security of the IoT devices; in addition, a balance is needed also between proportional processing of data and improvement of products/services, by understanding the needs of their customers – users of IoT solutions. There are studies in the scientific literature that analyse the behaviour of smart device users in terms of data protection and confidentiality (Abdi, Ramokapane and Such, 2019; Zheng et al., 2018; Tabassum, Kosinki and Lipford, 2019). This paper contributes to this area by investigating the manner in which essential European legislation aspects concerning data protection are perceived by users of IoT devices.

The paper is structured in four parts. Thus, the first part presents a literature review of (1) aspects concerning the intrusiveness of data provided by the IoT devices (1.1), responsibility for data protection (1.2), transparency and informing in data protection (1.3), data protection in the context of data aggregation for commercial purposes (1.4), as well as perception of personal data protection by IoT solution users (1.5). The second part of the paper describes the objectives, hypotheses and the methodology of the quantitative research, which aims to identify the perception of intrusiveness and data protection by users of IoT solutions (2). The third part presents the results and discusses them in relation to the established objectives and hypotheses (3). Finally, the fourth part presents the conclusions of the paper, emphasizing its theoretical and managerial implications, as well as future research directions.

1. Literature review

In the last years, researchers and public or private entities have been focused on data protection following its two main dimensions: collection, distribution and processing of data, respectively, ensuring security of data (Torre et al., 2016; Duan et al., 2019). Intrusiveness, as a consequence of insufficient data protection, brings different damages to users (CNIL, 2018). As per European legislation, there are multiple principles to be taken into account for ensuring data protection, such as predictability of data processing, transparency of data protection mechanisms, reduction of aggregation to the minimum required and accountability for data protection (EU Regulation 679/2016). However, this is a topic that is not evaluated in a uniform manner, given the cultural differences, personal opinion, evaluation criteria and the actual subjective nature of this concept (Solove and Citron, 2017).

The user, whose personal data is being collected and processed, is the only one that can evaluate the degree of feeling used and the damages incurred in this respect. The European legislation provides the framework through which the user of smart devices benefits from data protection, but whether he/she is informed and uses his/her rights is debatable (Haney, Furman and Acar, 2020).

1.1. Intrusiveness of data provided through IoT devices

The breach of the GDPR principles by entities involved in the provision of IoT solutions generates intrusiveness in the personal life of individuals whose data is collected and used without their consent. The principle of predictability of processing, in order to be properly implemented, requires a clear description of the reasons for which the data processing is needed. For example, the automated security solutions, for providing efficient services,

have to access and analyse data that are not necessarily needed for the functioning of smart devices (for example, IP address of the source/destination of the communication, patterns of the traffic data, information concerning the network to which the device is connected etc.) (Von Maltzan, 2019).

In addition, in order to avoid intrusiveness, the principle of data minimization has to be implemented, which entails that only the data necessary for providing the service should be collected and processed (Wright and Raab, 2014), taking into account the purpose of processing, disclosing or processing the data (Comas and Ferrer, 2015). If the data have already been collected and stored, the processing or disclosure to third parties has to respect this principle as well (Bolognini et al., 2019). An example in this respect is the decision of the European Court of Justice (ECJ, 2014) in terms of the metadata collected about an individual. This decision found the collection of data for providing voice messaging or call location, such as the telephone number or IP address of the device as being excessive, since these can provide a detailed profile of the user (Barbaro, Zeller and Hansell, 2006). There is research in this direction that has concentrated on the amount of data collected that is considered by users as justified in exchange for benefiting from a specific service provided by the IoT device (Naeini et al., 2017; de Boer, van Deursen and Van Rompay, 2019), but finding a common ground for the proper data quantity that should be collected and processed is difficult.

Unauthorized access to data is channelled through the vulnerabilities of the security protocols. These cybernetic attacks target different level of the IoT networks and, consequently, require a wide range of incident identification and prevention measures in order to ensure protection. Initially, such measures targeted identification of known attack types and static measures (Andrea, Chrysostomou and Hadjichristofi, 2015; Amanullah, et al., 2020; Yoon, 2020). Nevertheless, in the last years, given the development rate of new attack types, the idea of dynamic solutions has been adopted by using machine learning (Badsha, Vakilinia and Sengupta, 2019; Chesney, Roy and Khorsandroo, 2020), for identification of incidents in early stages (e.g. before exploitation). Currently, the security solutions focus on confidentiality, integrity and availability, but they are beginning also to analyse matters related to monitoring of data protection (Leloglu, 2017).

From a business perspective, preventing intrusiveness is closely linked to the principles mentioned by the consumer protection legislation, and as such, influencing the way IoT solutions are designed and implemented. Finding the balance between data confidentiality and data processing in a non-intrusive manner ensures the stability for selling products and services, given that users show a higher level of trust in such cases (Feng and Xie, 2019). Thus, although European legislation aims to minimize the intrusiveness felt by the user, it is important to find out how the user perceives this intrusiveness in relation to his/her personal data that is taken and processed.

1.2. The responsibility for protecting data accessed through IoT devices

The accountability principle, according to the GDPR, refers to the responsibility for implementing all appropriate mechanisms, procedures and controls (Wolters, 2017), to ensure that all legal requirements concerning personal data are implemented and can be proven (Working Party Article 29/2010). The clear explanation of the role and responsibility of each stakeholder for personal data processing leads to increasing the trust of the consumer and, implicitly, to positive effects on the long term.

From the perspective of data protection, according to the legislation, the responsibility for data processing pertains in general to the data controller. Further, the data controller generally remains liable for the actions of its data processors, with the exception of specific situations in which the data processor acts deliberately against the instructions of the data controller (EU Regulation 679/2016). In terms of data transfer, the entity that discloses the data is liable for the compliance with legal requirements, including for information of individuals about such disclosure of data (Fisk et al., 2015).

When referring to IoT solutions for smart homes, the following stakeholders can hold this position: IoT device hardware manufacturer, IoT device software manufacturer, storing service provider, IoT device management platform provider (Lee, Cha and Kim, 2019). In general, these stakeholders act as independent data controllers and are individually liable for their actions. Regardless, if they were to act together for processing data, they would be held jointly liable. Given the stakeholders involved and responsible for data protection (in collecting and processing activities, but also in data securing activities), we advance the question about the level of responsibility that users associate with the various entities involved in the protection of their data.

1.3. Transparency and informing in data protection

The transparency principle, mentioned by the GDPR states that users are to be informed about what happens to their data and should consent for certain types of collection, processing and disclosure of their data. The information notices for users, about the processing of their personal data should be concise, clear, intelligible, easy to understand and easy to access. In case of using a two-layer approach (text and a link to the entire information notice), the text next to the link should contain sufficient information (data processing purposes, rights of individuals, name of data controller) from the information notice (EU Regulation 679/2016).

In the case of IoT solutions, information about the data processing should be adjusted in accordance with the type of activity performed by the IoT device (Melicher et al., 2016). Thus, if, traditionally, the information notice is provided when the device is installed or is included in the documentation pertaining to the device (in electronic or paper format), an approach that ensures the proper knowledge about the data processing entails push notifications/alerts before any change in data processing (Castelluccia et al., 2018). The same approach can be considered in order to obtain/re-obtain consent, if this is the legal processing basis (Lee, Cha and Kim, 2019). The transparency in involving third parties and adequate management of data processing can prove difficult and involve adequate internal procedures within the involved organizations. Moreover, the data retention period can be difficult to establish and to implement (Jin, 2017). If anonymization / pseudo-anonymization is required (according to the principle of data minimization), it must be implemented in a manner that does not have serious consequences for the individuals whose data is being collected or for the individuals on which the inferred results are applied (Khalteuner and Bietti, 2018). This has proven difficult to implement in practice, as, even anonymized data can contain information that can lead to negative or discriminatory consequences/ damages to individuals (Polonetsky, Tene and Finch, 2013). Further, the concept of protection of group personal data and their rights, according to the data protection legislation increases the complexity of this aspect (Wachter and Mittelstadt, 2019). The responsibility for data protection, therefore, involves informing users, but we

raise the question of how appropriate, in fact, the different methods of informing users about their data protection are.

1.4. Aspects concerning data protection in the context of data aggregation for commercial purposes

Data aggregation is essential for creating user profiles to improve services or products, for creating personalized offers (EDPS, 2016), as well as for providing targeted security functionalities that can identify a threat at the moment it enters the network or very soon after that moment (Working Party Article 29/2010). Big Data analysis on the aggregated data about previous attacks ensures a better learning mechanism for the machine learning algorithms used to identify and manage IoT network anomalies (Hussain et al., 2020). This represents a method of enhancing the security of the entire IoT home system and, consequently, of increasing users' trust in such devices, and accordingly the number of IoT devices in their homes (Thierer, 2015).

In case of complex systems, such as smart homes are, aggregation of data can be performed by multiple entities: IoT device manufacturer, providers of IoT management software, providers of the security solution installed etc. The aggregation can be local or general, including all devices managed by the respective providers in the world; further, the providers can transfer data between themselves with the aim of understanding better the different user profiles (Datta, Tschantz and Datta, 2015).

Aggregation of users' personal data brings various benefits to companies, such as: reducing costs and resources needed to create the traditional customer profile, hence increased time and budget for research and innovation, appropriate delivery of services to customers etc. Consumers also benefit from useful services provided at the right time, at a lower price, without straining to find the most suitable offers (Elvy, 2017). On the other hand, data aggregation and distribution can jeopardize transparency in the relationship with consumers and involve great responsibilities (Tene and Polonetsky, 2013). From a user's perspective, collecting a large quantity of personal data or transferring it to third parties can be seen as intrusive, except in cases when it is necessary for the functioning of the devices and the negative consequences on him/her are mitigated (Kleek et al., 2018). This raises the question of whether users perceive the intrusiveness differently, depending on the purpose for which the data is aggregated (i.e. commercial purposes vs. data security).

1.5. Perception on data protection by users of smart home IoT devices

The studies concerning the perception of data confidentiality and security by IoT home devices users indicate, in general, that they do not fully understand what data protection entails and what happens to their data. The research performed by Abdi, Ramokapane and Such (2019), which analyses the perception of users on Intelligent Personal Assistants (IPA), shows that users did not understand or had an incomplete image about where their personal data is stored, processed and disclosed. Another aspect of this research showed that, although users are aware that IPAs have the capacity to learn, they are reluctant to allow these devices to learn everything about them and about their behaviour. Even if users are sceptical about the policies that IoT manufacturers have about how personal data is processed, their confidentiality behaviour is not strongly influenced by these (Tabassum, Kosinki and Lipford, 2019).

Another study, carried out in order to understand smart devices holders' perception about the confidentiality of data managed by these, highlighted that the responsibility for ensuring the protection of personal data is believed to lie largely with the manufacturers of smart devices. It also revealed that users' attitude and behaviour towards data protection are influenced by the ease of using services and interconnecting IoT devices (Zheng et al., 2018).

Regarding the influence of demographic variables upon consumer perception concerning smart home security and confidentiality aspects, the research performed by Haney, Furman and Acar (2020) has shown that, although users are aware about the risks to which they are exposed, they fail to take measures to reduce such risks. The justification that stems from the study is considered to be the lack of users' technical knowledge. Also, according to Kim and Yoon (2019) it is indicated that the concern about data security and privacy seems to depend on the marital status of respondents. Hence it results that, to some extent, demographic variables influence users' attitude and perception of personal data protection. The question we raise in this respect, is whether other demographic variables, such as gender, age, parental status, influence the opinions and attitudes of IoT smart home users.

2. Objectives and research methodology

Starting from the questions that occurred while studying the scientific literature, we set accordingly the objectives for our research:

- **O_1** – Assessing the particularities of IoT devices use in homes.
- **O_2** – Identifying users' attitude about the protection of personal data collected by IoT devices in their homes.
- **O_3** – Determining the perception of intrusive data processing in general, and particularly for: a) commercial purposes; b) ensuring data security of the IoT device
- **O_4** – The evaluation of users' opinions on the entities that are responsible for data protection (data processing and assuring the data security).

To answer these questions, we set the research hypotheses, as following:

H1 – There is no difference related to the use of the IoT smart home devices associated with: a) gender; b) age; c) parental status; corresponding to O_1.

H2 – The perception of negative consequences generated by the improper processing of personal data is the same, regardless of: a) gender; b) age; c) parental status; corresponding to O_2.

H3 – The perception of personal data exposure through different types of unauthorized access (cybernetic attacks) to IoT networks is the same, regardless of: a) gender; b) age; c) parental status; corresponding to O_2.

H4 – Respondents consider that the request to access different types of data, through their IoT devices, is similarly intrusive; corresponding to O_3.

H5 – There are no differences between perceived intrusiveness for commercial purposes (either for personalized or for general offers), and the perceived intrusiveness for developing data security services; corresponding to O_3.

H6 – The perception of intrusiveness with the purpose of providing data security services is not influenced by a) gender; b) age; c) parental status; corresponding to O_3.

H7 – The perceived responsibility for processing data retrieved through IoT home devices is not influenced by: a) gender; b) age; corresponding to O_4.

H8 – The perceived liability for ensuring the security of respondents' data, when using IoT home devices, is not influenced by: a) gender; b) age; corresponding to O_4.

Consequently, we conducted a quantitative research aimed at assessing the intrusiveness and protection of personal data, as perceived by users of IoT smart home solutions. Studies indicate that using online questionnaires is increasingly popular, both in academia and in business, because it has notable advantages (Aaker et al., 2013). Hence, the quantitative research was based on an online questionnaire, designed on the Question Pro platform, which contained 19 questions. It was initially tested in terms of clarity of wording on a mini sample of 8 people. Following the feedback received, the questionnaire was revised for a better understanding of the questions meaning. It was online distributed in October 2020 to 277 people, aged between 19 and 65, professionally active, living in different regions of the country, through several accounts of LinkedIn social network which belong to people working in the legal, teaching, business environment (sales and marketing), IT and constructions – engineering. Respondents who stated at the beginning of the questionnaire that they do not have a smart device were asked to stop completing the questionnaire. The sampling was non-probabilistic, with a total of 183 complete and valid questionnaire responses.

The data taken from the online reporting platform of the questionnaire were first processed with Microsoft Excel and then analysed with the statistical software Minitab 16. The internal consistency of the results for the intrusion perception was verified, the Cronbach Alfa coefficient being 0.773. Similarly, for the responsibility for data protection, the Cronbach Alpha coefficient is 0.719, which provides the premises for their validity.

3. Results and discussions

Starting from the first objective (O_1), we wanted to know what smart devices are used by respondents in their own homes. As such, they were asked to select all the smart devices that they use. From the analysis of their responses, it resulted that the most popular devices are the smart phones, followed by smart TVs (see Table no.1). Other devices, like smart watches or smart baby monitors were indicated by less than 3% of respondents.

Table no. 1: The use of different smart devices in the respondents' homes

Smart TV	Smart personal assistants (i.e. Google Home)	Smart utility devices (i.e. lighting, outlets)	Smart surveillance devices	Smart phones	Smart household appliances (i.e. refrigerator, vacuum cleaner, A/C units)	Others
70.5%	14.2%	27.9%	19.1%	89.6%	55.2%	2.7%

If the high percentage of the owners of smart phones or TVs does not surprise, it's remarkable that more than half of the respondents own at least one smart household appliance device. Still, this may be explained by the fact that, due to the coronavirus

pandemic in 2020, when the population spent a significant amount of time in their homes, the investments focused on keeping a clean and comfortable environment, the consumers being interested especially in robotic cleaning devices (Neagu, 2021).

We also tested the validity of **H1** hypothesis, corresponding also to O_1. The Pearson Chi Square test indicates a correlation between the use of IoT devices and the age of the respondents, the resulting Pearson Chi Square coefficient being 13.624 for 3 degrees of freedom, and an associated p-value of 0.003 – lower than the set cut-off level at 0.05. The analysis of the responses distribution indicates that users younger than 35 years are using these devices more than the other age categories. The distribution based on gender is: 111 females (60.7%) and 72 males (39.3%). We identified a correlation between the gender of the respondent and the use of smart personal assistants (e.g. Google Home), the Pearson Chi Square coefficient being 4.275 for 1 degree of freedom, the associated p-value being 0.039, the male respondents using more than expected this kind of device. At the limit, the Pearson Chi Square coefficient of 3.596 for 1 degree of freedom and an associated p-value of 0.058 indicates an association between the owners of surveillance systems and the parental status, the results indicating that the respondents who are parents use these more than respondents with no children. This contradicts up to some extent the results of Kim and Yoon (2019), where it is claimed that single persons or freshly married couples tend to be more interested in the security aspects of their homes, while families with children don't seem to pay a special interest to these aspects, but rather to the main advantages that smart homes offer, namely easing the household activities and providing more free time. Between the use of other devices and the age, gender and, respectively, parental status, we could not find any other associations. *Still, the identified differences invalidate **H1** hypothesis.*

Related to the second objective (O_2), we wanted to know what is the attitude of the respondents regarding how they obtain information about processing and protection of their personal data, before purchasing a smart device that is able to connect to the IoT network of their homes. They were asked to indicate up to what extent a certain attitude is describing them, on a scale from 1 to 5 (1 – describes me very little, 5 – describes me very much). The distribution of data looks quite symmetrical for each of these variables (the skewness coefficients vary from 0.05 and 0.56). As such, in order to find what attitude characterizes most of the respondents when they search for information regarding personal data protection, we applied the One Sample Wilcoxon Signed Rank test, comparing the median of each variable with the value of 3, the middle value of our scale (Rey and Neuhauser, 2011; Voraprateep, 2013; Rotenstein, 2020). The results are shown in Table no.2. As we can notice, most of the respondents rely much and very much on other users' recommendations, when it comes to getting informed about personal data protection, the other attitudes not describing the majority of respondents.

Table no. 2: The One Sample Wilcoxon Signed Rank test for evaluating respondents' attitude about obtaining information about the processing of their personal data

Respondent' s attitude	Null hypothesis (H_0) vs. alternative hypothesis (H_a) – statistic context	P-value*	Decision	Estimated median
I read the terms, conditions and policies regarding data protection related to the device	median = 3.0 vs. median >3.0	0.386	Accept H_0	3.0
I rely on friends' recommendations		0.204	Accept H_0	3.0
I rely on other users' reviews		0.002	Reject H_0	3.5
I take into account the utility of the device without analysing how personal information is processed		0.991	Accept H_0	3.0

* significance level <0.05

Next, respondents were asked to rate on a scale of 1-5 the usefulness of the different manners of obtaining their consent when being informed about data processing policies (see table no. 3). Due to the skewness to the left of the analysed data sets (the skewness coefficients being -1.61, respectively -0.94, -1.69 and -1.81) we tested the median against the value of 4, on a scale from 1-5, using the Sign Test (Rotenstein, 2020).

Table no. 3: The sign test regarding the proper manners of giving informed consent for the processing of personal data

Manner to get informed and give consent	Null hypothesis (H_0) vs. alternative hypothesis (H_a) – statistic context	P-value*	Decision	Median
During the installation process	median = 4.0 versus median >4.0	0.0000	*Reject H_0*	5.0
On the website of IoT device manufacturer		0.0046	*Reject H_0*	5.0
On email		0.0000	*Reject H_0*	5.0
In the software application for the management of the IoT device		0.0000	*Reject H_0*	5.0

* 0.05 significance level

As the test results show in table no.3, most of the respondents think that all the means of getting information are useful (the median of each variable is 5, on a scale from 1 to 5). The results confirm the other research in the scientific literature that emphasize the importance of displaying the policies of processing the personal data in multiple ways and multiple places (Castelluccia et al., 2018), this giving the users the sense of control over the personal data that they share (Wright and Rabb, 2014). Further on, we wanted to know what is the period of time over which the data should be stored to provide proper security to their IoT devices. The responses are presented in Table no.4.

Table no. 4: The opinion of the respondents related to the optimal period of time for storing personal data for providing proper security to IoT devices

<1 month	1-3 months	3-6 months	6 months – 1 year	> 1 year	The period set by the security solution provider
15.3%	10.4%	13.7%	8.2%	4.4%	48.1%

It is interesting that almost half of the respondents are willing to let the security solution provider decide the optimal period for storing their personal data in order to ensure adequate security services for their IoT devices. Only a small percentage (15.3%) considers that the stored information should be deleted after no more than one month from the moment it was recorded.

Regarding the **H2** research hypothesis we aimed to see if there are statistically significant differences explained by gender, age or parental status in perceiving the consequences of improper personal data processing. Thus, respondents were asked to rate on a scale of 1 to 5 (1 – very mild, 5 – very severe) the severity of the following consequences of improper data processing: disclosure of personal data to unauthorized persons, use of data for personalized marketing offers, use of data to create general user profiles, transfer of data to other entities (institutions / companies / authorities) without their consent. In all cases, the Sign Test places the median at 5, which indicates that all these consequences are seen as very serious by most respondents. We applied Kruskal Wallis test on each of these consequences cross checked against demographic variables, but no statistically significant differences were found. *Thus hypothesis **H2** is validated.*

Regarding **H3**, respondents were asked to rate on a scale of 1 to 5, the extent to which they consider that unauthorized access (cybernetic attacks) to various components of an IoT network, exposes their personal data to attackers. For all these possible scenarios of a cybernetic attack, the sign test points to a median of 5, indicating the fact that most of the respondents consider that the unauthorized access to data, no matter where it takes place (network, management software solution, cloud or the device itself), is exposing in a very high extent their personal data. However, analysing these results in correlation with demographic variables using Kruskal Wallis test, we found significant statistical differences. They are presented in Table no.5.

Table no. 5: The results of Kruskal Wallis test for hypothesis H3

Research hypothesis	Null hypothesis (H_0) – statistic context	Tested variable	Cross variable	Decision	*P*-value*
H3	The distribution of the tested variable is the same in all the categories of the cross variable	Unauthorized access of the IoT device itself	Age	*Reject* H_0	0.003
		Unauthorized access of the mobile/desktop management software solution of the IoT device		*Reject* H_0	0.035

*0.05 significance level

The percentage of respondents under the age of 25 which consider "unauthorized access of and IoT device itself" and "unauthorized access of the mobile/desktop management software solution of the IoT device" as being situations that expose in a very high extent personal data, is lower than that of the other age groups. These differences lead to *the invalidation of **H3.***

Table no. 6: The sign test regarding the willingness of the respondents to grant access to different types of personal data through IoT devices

Willingness to grant access to personal data as:	Null hypothesis (H_0) vs. Alternative hypothesis (H_a) – statistic context	P-value*	Decision	Median
Video/audio	H_0 median = 3.0 vs. H_a median < 3.0	0.000	*Reject H_0*	2.0
About health and physical condition		0.000	*Reject H_0*	2.0
Identification data (i.e. name, date of birth)		0.001	*Reject H_0*	2.0
About habits of using IoT devices		0.004	*Reject H_0*	3.0

*0.05 significance level

Next, we analysed the perception of intrusiveness in various circumstances (O_3), hence we evaluated first the willingness of respondents to grant access to various types of personal data. As it can be observed in Table no. 6, even if the medians of the different types of data are located under 3 (on a scale from 1 – very low willingness, to 5 – very high willingness), their testing was needed to see if between them there are significant static differences.

Table no. 7. The result of Mann Whitney test for testing the H4 research hypothesis

Tested variables	N	Median	Results
Willingness to grant access to video/audio personal data	183	2.0000	W = 30787.0 Test ETA1 = ETA2 vs ETA1 not = ETA2 is significant for p value 0.0058
Willingness to grant access to data about habits of using the IoT device	183	3.0000	
Willingness to grant access to data about health and physical condition	183	2.0000	W = 30229.5 Test ETA1 = ETA2 vs ETA1 not = ETA2 is significant for p value 0.0009
Willingness to grant access data about using habits of IoT devices	183	3.0000	

*0.05 significance level

The Mann Whitney test applied to the independent variables "video/audio personal data" and "data about the usage habits of IoT devices" indicates a difference between the medians (see Table no.7), with the majority of respondents considering more intrusive the access to audio/video personal data than the access to data about the habits of using their IoT devices (a lower willingness to grant access to data indicates a higher perception of intrusiveness). Similarly, the users seem more reticent to grant access to data about health and physical condition, than to data about usage habits. *Thus, hypothesis **H4** is rejected.*

Further, the respondents were asked up to what extent they perceive as intrusive collecting and using their data for different purposes (personalized offers, general offers and security solutions). The One Sample Wilcoxon Signed Rank was applied, under data symmetry conditions. This indicates the fact that the majority of respondents perceive, irrespective of the purpose, the use of personal data as highly and very highly intrusive, with the median in all three cases being greater than 3 – the middle on a scale from 1 to 5 (see Table no.8).

Table no. 8. The One Sample Wilcoxon Signed Rank test for estimating the median of intrusiveness of aggregated personal data for different purposes

Intrusiveness of personal data aggregation for:	Null hypothesis (H_0) vs. Alternative hypothesis (H_a) –statistical context	P-value*	Decision	Estimated median
Personalized commercial offers	H_0 median = 3.0 vs. H_a median > 3.0	0.005	*Reject H_0*	3.5
General commercial offers aimed at all users		0.000	*Reject H_0*	3.5
Security solutions for IoT devices		0.000	*Reject H_0*	3.5

* significance level <0.05

As data in groups don't have a normal distribution (the Kolmogorov-Smirnov test for normality was performed), we used Mann Whitney Test to compare intrusiveness for creating commercial personalized offers versus intrusiveness for creating commercial offers to all users. The result of comparing ETA1 = ETA2 vs ETA1 < ETA2 is significant at 0.0360, W = 31759.0. It shows that the percentage of high and very high perception of intrusiveness for personalized commercial offers is lower than that of intrusiveness for general offers. There were found no significant differences between intrusiveness perceived

for commercial purposes (neither for personalized offers, nor for offers dedicated to all users) and the intrusion in personal data for developing security solutions, the associated p-values being 0.63, respectively 0.15). *It is confirmed thus the set hypothesis **H5**.*

To verify **H6**, whether the perception of the intrusiveness of data aggregation for developing security solutions is influenced by the variables: gender, age or parental status, we applied the Kruskal Wallis test. The test resulted in a statistically significant association between intrusion and parental status. It appears that respondents, who are also parents, consider in higher percentage than respondents without children (p-value = 0.049 <0.05, the significance threshold) that access to their personal data and that of their family is highly intrusive. No statistically significant differences in respondents' perceptions by gender or age were observed. *This invalidates **H6**.*

In order to identify possible differences regarding the entities responsible for data protection (O_4), depending on gender and age, we performed an analysis, both in terms of appropriate, ethical collection and processing of data retrieved through IoT devices **(H7),** as well as from the point of view of data security **(H8**).The respondents over 35 years consider in a higher percentage than the other age categories that the responsibility for processing the personal data belongs to the cloud storing solution provider (p value - 0.04). The male respondents consider in a higher extent than female respondents, that the responsibility for the collecting and processing of personal data by IoT devices belongs to the user and to the manufacturer of the IoT device (p value 0.034, respectively 0.036). Therefore, ***H7** is invalidated.* Testing H**8**, we remarked that respondents over 45 years, consider in a higher proportion than other age categories that the cloud storing solution administrator (p value - 0.001) and the provider of the security solution installed on the IoT devices (p-value 0.052) are entities responsible in a very high degree for ensuring the security of the data. Again, the male respondents consider in a higher percentage that the responsibility for ensuring the security of data pertains to the user in a high degree (p-value 0.004). ***H8** is invalidated.*

Table no. 9. Median of responsibilities for data protection (collecting – processing and ensuring security) of various entities, on a scale from 1 to 5

Responsibility	IoT device producer	Mobile/desktop IoT management software provider	Security solutions installed by user	Cloud storage administrator	User
Collecting and processing data	4.0	5.0	4.0	5.0	4.0
Ensuring the security of data	4.0	5.0	4.0	5.0	4.0

It is interesting to notice that, even though the questions related to the responsibility of different entities on processing personal data and ensuring data security were not consecutive in the survey, the median is identical (see table no.9). Confirming previous research, the majority of users consider that the IoT device producers are responsible in a high extent for data security (Zheng et al., 2018). However, from our analysis, that included the other entities involved in data protection, the provider of the management software solution and the cloud database administrators also share a high responsibility in processing and securing personal data from IoT smart home solutions.

Conclusions

As the intelligence of IoT devices increases, they collect and process increasing amounts of data. There is a need for a clear delimitation between the aggregation of personal data to improve the functionality and security of IoT solutions and the intrusion into the lives of individuals for the benefit of other entities. European data protection legislation, although strict in this regard, does not limit or standardize the amount of data that can be downloaded from users of IoT smart devices. Taking into account the main requirements of the legislation, as well research in the field, we developed a quantitative research that had as objectives the assessment of using IoT home devices particularities, the identification of users' attitudes towards data protection practices, determining the perception of data processing intrusion in general, and in particular for the commercial purposes and data security, as well as assessing respondents' views on entities responsible for data protection of IoT home devices (data processing and data security).

The research showed that before purchasing a smart device, respondents rely on the reviews of other users for information, rather than reading the terms, processing and protection policies provided by the supplier. The ways of informing and giving consent to these, such as email, the manufacturer's website, the IoT device installation program, the IoT device administration application are considered useful and very useful by most respondents. These results can contribute to the understanding and implementation of the principle of transparency by IoT solution providers.

In terms of intrusion, the respondents perceive the processing of video/audio data and of health/physical condition data as being more intrusive than data about interaction habits with the IoT device, for example. Intrusiveness, regardless of the purpose for which the data are collected and used, is similarly perceived by the respondents. Although using personal data for developing security solutions is generally perceived as being intrusive, almost half of the respondents state that the provider of the security solution can store their personal data as much as it considers necessary. In terms of responsibility, there are certain differences in perception, depending on gender and age. It is interesting that the male respondents consider in high percentage than the female respondents that the user is the one most responsible for ensuring the security of the IoT device. In general, the responsibility for both ethical data collection and processing, as well as for ensuring data security, is associated more with the entities that create smart device management applications and data cloud solution administrators. This research emphasizes also, that the attitude of IoT solutions users about data protection and the perceived intrusiveness, when their data are accessed and used by third parties, depend on demographic variables such as age, gender, parental status. It is interesting to notice that, although users do not inform themselves, by reading data processing and protection policies when purchasing an IoT device (even though these policies could mention that personal data may be accessed and processed by third parties), they feel that unauthorized access and improper processing of personal data is very serious.

The results of the research, even if *limited in terms of the sampling method used*, contribute to the theory in the field and to a better understanding of how users of IoT devices perceive intrusiveness, due to the aggregation of their data. Also of what is their attitude towards key points related to personal data protection. The results provide an interesting perspective to companies involved in developing IoT solutions, as well as for the standardization organizations and for regulators. Nevertheless, these results have to be complemented by detailed research into those elements that predominantly contribute to the formation of the intrusiveness' perception. A future direction of research would be investigating the reasons

for which privacy policies are not read, in order to identify aspects that have to be improved to ensure wider awareness and understanding of personal data processing consequences.

References

Aaker, D.A., Kumar, V., Leone, R.P. and Day, G.S., 2013. *Marketing Research*. 11th ed. Danvers: John Wiley & Sons.

Abdi, N., Ramokapane, K.M. and Such, J.M., 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In USENIX Association, *Fifteenth Symposium on Usable Privacy and Security*, Santa Clara, CA, USA, 12-13 August 2019. Santa Clara: The USENIX Association.

Amanullah, M.A., Habeeb, R.A.A., Nasaruddin, F.H., Gani, A., Ahmed, E., Nainar, A.S.M. and Imran, M., 2020. Deep Learning and Big Data Technologies for IoT Security. *Computer Communications*, 151, pp. 495-517.

Andrea I., Chrysostomou C. and Hadjichristofi G., 2015. Internet of Things: Security Vulnerabilities and Challenges. In IEEE, *IEEE Symposium on Computers and Communication (ISCC IEEE 2015)*, Larnaca, Cyprus, 6-9 July 2015. Larnaca: IEEE.

Badsha, S., Vakilinia, I. and Sengupta, S., 2019. Privacy Preserving Cyber Threat Information Sharing and Learning for Cyber Defense. In IEEE, *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 7-9 January 2019. Las Vegas: IEEE.

Barbaro, M., Zeller, T. and Hansell, S., 2006. A Face is Exposed for AOL Searcher no. 4417749. *New York Times*. *9* Aug, p.8.

Bolognini, L. and Balboni, P., 2019. IoT and Cloud Computing: Specific Security and Data Protection Issues. *Internet of Things Security and Data Protection – Internet of Things*, pp. 71-70.

Castelluccia, C., Cunche, M., Le Metayer, D. and Morel, V., 2018. Enhancing Transparency and Consent in The IoT. In IEEE, *2018 IEEE European Symposium On Security and Privacy Workshops (Euros&Pw)*, London, 23-27 April. London: IEEE.

Chesney, S., Roy, K. and Khorsandroo, S., 2020. Machine learning algorithms for preventing IoT cybersecurity attacks. In Arai K., Kapoor S., Bhatia R. (eds), *Proceedings of SAI Intelligent Systems Conference*, London, 3-4 September. London: Springer, Cham.

CNIL, 2018. *Privacy Impact Assessment Guidance*. *French Data Protection Authority* [online]. Available at: <https://www.cnil.fr/en/privacy-impact-assessment-pia> [Accessed 6 December 2020].

Comas, J.S. and Ferrer, J.D., 2015. Big Data Privacy: Challenges to Privacy Principles and Models. *Data Science and Engineering*, 1, pp. 21-28.

Datta, A., Tschantz, M.C. and Datta, A., 2015. Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice and Discrimination. *Proceedings on Privacy Enhancing Technologies*, 2015(1), pp. 92-112.

De Boer, P.S., van Deursen, A.J. and Van Rompay, T.J., 2019. Accepting the Internet-of-Things in our homes: The role of user skills. *Telematics and Informatics*, *36*, pp. 147-156.

Dorsemaine, B., Gaulier, J.P., Wary, J.P., Kheir, N. and Urien, P., 2015. Internet of Things: a definition & taxonomy. In Khalid Al-Begain and Nidal AlBeiruti, *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, Cambridge, UK, 9-11 September. Cambridge: IEEE.

Duan, Y, Sun, X., Che, H., Cao, Z.L. and Yang, X., 2019. Modeling Data, Information and Knowledge for Security Protection of Hybrid IoT and Edge Resources. *IEEE Access*, 7, pp. 99161-99176.

ECJ, 2014. *Cases C293/12 and C594/12. Digital Rights Ireland*, [online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293& from =EN> [Accessed 6 December 2020].

EDPS, 2016. *Opinion 8/2016 Opinion on coherent enforcement of fundamental rights in the age of big data* [online]. Available at: <https://edps.europa.eu/data-protection/our-work/publications/opinions/big-data_en> [Accessed 6 December 2020].

El Khaddar, M.A. and Boulmalf, M., 2017. Smartphone: the ultimate IoT and IoE device. In: N. Mohamudally, ed. 2017. *Smartphones from an applied research perspective*, Rijeka: Intech. pp.137-184.

Elvy, S.A., 2017. Paying for privacy and the personal data economy. *Columbia Law Review*, 117(6). [online]. Available at: <https://columbialawreview.org/content/paying-for-privacy-and-the-personal-data-economy/> [Accessed 6 December 2020].

Feng, Y. and Xie, Q., 2019. Privacy Concerns, Perceived Intrusiveness and Privacy Controls: An Analysis of Virtual Try-On Apps. *Journal of Interactive Advertising*, 19(1), pp. 43-57.

Fisk, G., Ardi, C., Pickett, N., Heidemann, J., Fisk, M. and Papadopoulos, C., 2015. Privacy Principles for Sharing Cyber Security Data. In IEEE, *Proceedings of the IEEE International Workshop on Privacy Engineering*, San Jose, 21-22 May. San Jose: IEEE.

Future Learn, 2021. *Is a smart phone an Internet of Things device?* [online] Available at: <https://www.futurelearn.com/info/courses/internet-of-things/0/steps/8432> [Accessed 28 February 2021].

Haney, J.M., Furman, S.M. and Acar, Y., 2020. Smart Home Security and Privacy Mitigations: Consumer Perceptions, Practices and Challenges. In A. Moallem (ed.), *International Conference on Human-Computer Interaction*, Copenhagen, Danemark, 19-24 July 2020. Copenhagen: Springer, Cham.

Haney, J.M., Furman, S.M. and Acar, Y., 2020. Research Report: User Perceptions of Smart Home Privacy and Security. *NISTIR 8330*, p.11.

Hussain, F., Hussain, R., Hassan, S.A. and Hossain, E., 2020. Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Communications Surveys & Tutorials*, 22(3), pp. 1686-1721.

ICO (Information Commisioner's Office), 2017. *Big data, artificial intelligence, machine learning and data protection.* [online] Available at: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf [Accessed 6 December 2020].

ICO (Information Commisioner's Office), 2018. *Guide to the General Data Protection Regulation*. [online] Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/#fairness> [Accessed 6 December 2020].

Jin, G.Z., 2017. Artificial Intelligence and Consumer Privacy. *NBER Working Papers*, 24253, National Bureau of Economic Research Inc.

JO (Jurnalul Oficial al Uniunii Europene), 2009. *Rezoluția Parlamentului European din 15 iunie 2010 referitoare la internetul obiectelor (2009/2224(INI))*, [online] Available at: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:236E:0024:0032:RO:PDF> [Accessed 6 December 2020].

Kaltheuner, F. and Bietti, E., 2018. Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR. *Journal of Information Rights*, Policy and Practice, 2(2), p.None.

Kim, S. and Yoon, J., 2016. An exploratory study on consumer's needs on smart home in Korea. In Marcus A. (eds), *International Conference of Design, User Experience and Usability*, Toronto, Canada, 17-22 July 2016. Toronto: Springer, Cham.

Kleek, M.V., Liccardi, I., Binns, R., Zhao, J., Weitzner, D.J. and Shadbolt, N., 2017. Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps. In Association for Computing Machinery, *Proceedings of The 2017 Chi Conference On Human Factors in Computing Systems*, Denver, 2 May. New York: Association for Computing Machinery, pp.5208-5220.

Lee, G.Y., Cha, K.J. and Kim, H.J., 2019, Designing the GDPR Compliant Consent Procedure for Personal Information Collection in the IoT Environment. In: IEEE, *Internet of Things (ICIOT) 2019 IEEE International Congress,* Milan, 8-13 July. Milan: IEEE.

Lee, S., 2019. Internalizing the Harm of Privacy Breaches: Do Firms Have an Incentive to Improve Data Protection? An Event Study. *TPRC47: The 47th Research Conference on Communication, Information and Internet Policy*.

Leloglu, E., 2017. A review of Security Concerns in Internet of Things. *Journal of Computer and Communications,* 5, pp. 121-136.

Maayan, G.D., 2020. *The IoT Rundown for 2020: Stats, Risks and Solutions.* [online] Available at: <https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for-2020.aspx> [Accessed 28 February 2021].

Maple, C., 2017. Security and privacy in the internet of things. *Journal of Cyber Policy*, 2(2), pp. 155-184.

Melicher, W., Sharif, M., Tan, J., Bauer, L., Christodorescu, M. and Leon, G.P., 2016. (Do Not) Track Me Sometimes: Users' Contextual Preferences for Web Tracking. *Proceedings on Privacy Enhancing Technologies*, 2, pp. 135-154.

Naeini, P.E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L. and Cranor, L.F., 2017. Privacy expectations and preferences in an IoT world. *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pp. 399-412.

Neagu, L., 2021. *Cum a schimbat pandemia piața de roboți casnici.* [online] Available at: <https://www.economica.net/cum-a-schimbat-pandemia-piata-de-roboti-casnici_196906.html> [Accessed 28 February 2021].

Norton, 2021. *What is The Internet of Things (IoT)?* [online] Available at: < https://us.norton.com/internetsecurity-iot.html> [Accessed 28 February 2021].

Polonetsky, J., Tene, O. and Finch, K., 2016. Shades of gray: seeing the full spectrum of practical data de-identification. *Santa Clara Law Review*, 56(3), pp. 594-618.

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 2016. [online] Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [Accessed 2 December 2020].

Rey D., Neuhäuser M., 2011. Wilcoxon-Signed-Rank Test. In: *M. Lovric (ed) International Encyclopedia of Statistical Science. Berlin, Heidelberg: Springer.*

Rotenstein, E., 2020. Statistica matematica. *Teste neparametrice.* [online via internal VLE] Ioan Cuza University. Available at: <https://www.math.uaic.ro/ ~eduard/ Capitolul%207.%20Teste%20neparametrice.pdf> [Accessed 28 February 2021].

Solove, D.J. and Citron, D.K., 2017. Risk and anxiety: A theory of data-breach harms. *Texas Law Review*, *96*, p.737.

Statista, 2021. *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025*. [online]. Available at: < https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/> [Accessed 28 February 2021].

Tabassum, M., Kosinski, T. and Lipford, H.R., 2019. "I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. In USENIX Association *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, Santa Clara, USA, 12-13 August 2019. Santa Clara: The USENIX Association.

Tene, O. and Polonetsky, J., 2013. Judged by the Tin Man: Individual Rights in the Age of Big Data. *Journal of Telecommunications and High Technology Law*, 11, pp.351-368.

Thierer, A., 2015. The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation. *RICH. J.L. & TECH.*, 21(2), article4.

Torre, I., Koceva, F., Sanchez, O.R. and Adorni, G., 2016. A framework for personal data protection in the IoT. In *Infonomics Society, 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, Barcelona, Spain, 5-7 December 2016. Denver: IEEE.

Vodafone, 2019. *Vodafone IoT Barometer 2019.* [online]. Available at: <https://www.vodafone.com/business/news-and-insights/white-paper/vodafone-iot-barometer-2019#> [Accessed 2 December 2020].

Von Maltzan, S., 2019. No Contradiction Between Cyber-Security and Data Protection? Designing a Data Protecton Compliant Incident Response System. *European Journal of Law and Technology*, 10(1), p.None.

Voraprateep, J., 2013. *Robustness of Wilcoxon Signed-Rank Test Against the Assumption Of Symmetry. Master of Research, The University of Birmingham*, [online] Available at: < https://core.ac.uk/download/pdf/18614332.pdf> [Accessed 28 February 2021].

Wachter, S. and Mittelstadt, B., 2019. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, 2019(2), pp. 494-620.

Wolters, P.T.J., 2017. The security of personal data under the GDPR: a harmonized duty or a shared responsibility?. *International Data Privacy Law*, 7(3), pp.165-178.

Working Party Article 29/2010 on Opinion 3/2010 on the principle of accountability. [online]. Available at: <https://www.dataprotection.ro/servlet/ViewDocument?id=654> [Accessed 17 November 2020].

Wright, D. and Raab, C., 2014. Privacy principles, risks and harms. *International Review of Law, Computers & Technology*, 28(3), pp.277-298.

Yoon, J., 2020. Deep-learning approach to attack handling of IoT devices using IoT-enabled network services. *Internet of Things*, 11, p.100241.

Zheng, S., Apthorpe, N., Chetty, M. and Feamster, N., 2018. User perceptions of smart home IoT privacy. arXiv e-prints, pp.arXiv-1802.