IoT Devices and the Need to Inform Utility Users of Collecting, Controlling and Processing of Personal Data

G. Vojković, Ph.D. * and M. Milenković, LL.M*
* University of Zagreb, Faculty of Transport and Traffic Sciences/Chair of Transport Law and Economics, Zagreb, Croatia
gvojkovic@fpz.hr
mmilenkovic@fpz.hr

Abstract - **The introduction of smart devices into households presents new challenges in terms of privacy and protection of personal data, given the wide set of data they collect. Replacing various meters that measure electrical energy, water or natural gas consumption, and with smart meters bring many benefits, such as the ability to read data automatically, an approach to managing energy distribution based on real-time energy consumption, although on the other hand it presents a new security risk. For example, by introducing a smart meter for electricity or water which can be monitored to even obtain information on how many household members are present in the household, and when the household is empty, and what are their life habits. Under the current consumer protection framework in the EU, service providers are under no obligation to notify customers that new consumer connected devices capture a significantly larger set of data about them and pose a potential privacy risk. In this paper, we consider the basic dangers to privacy and personal information brought by using IoT devices, and outline proposals to change the legal framework to inform consumers about the capabilities of these utilities to control devices bi-directional communication, coordination and the very need to monitor the data collected.**

Keywords – IoT, privacy, EU, regulation, data

I. INTRODUCTION

In last several years various measuring and other devices are being replaced by smart devices, as part of the IoT model. Electricity meters, water consumption meters and other different meters are becoming smart meters - allowing remote reading, alerting (e.g. at unusually high-power consumption) and with the addition of new functionality, e.g. measuring consumption at a certain point in time.

What is IoT? There are many definitions currently in use. In one of our previous papers, we chose one because of its practicality: "The Internet of Things, commonly abbreviated as IoT, refers to the connection of devices (other than typical fare such as computers and smartphones) to the Internet." The business media following the development of IoT often references different products and services such as interconnected cars, smart home appliances and even kitchen appliances and medical devices such as heart monitors. [1]

So far, there have been a few relevant market research efforts to estimate the size and importance of the IoT market. One of them has estimated that the number of internet-connected devices will outnumber humans interfacing the internet to the ratio of 4-to-1 by year 2020. Naturally, many of these devices will belong to IoT paradigm. [2] Another research we referenced in earlier papers referenced the fact that the average smart home in the United States now employs the services of eleven smart devices. [3]

This and other research have interesting ramifications and we can safely assume that IoT products and services have already transcended the development phase and the use by early technology adopters and enthusiasts and has entered a widespread everyday use.

In our everyday lives, the basic television sets have been replaced by increasingly connected and interactive Smart TV variety, households increasingly adopt products like smart speakers – virtual assistant and in some areas the general population is not even aware that utility companies, such as their water, gas or electricity supplier, has replaced their traditional meters to new devices employing IoT. [4]

Like all devices connected to the Internet, IoT devices are prone to malware attacks. These attacks have traditionally increased in number and severity. According to research conducted by infosec companies such as F-Secure, in the first half of 2019, their global honeypot network detected a threefold increase of information security incidents bringing a total to over 2.9 billion events. The same research underlines that most of the attacks were conducted by means of malicious software such as internet worms targeting TCP ports responsible for, among other things, IoT communication. [5]

The current IoT paradigm employs the use of a large number of devices produced by various manufacturers developed for hundreds of different uses even if they sometimes share the basic hardware platform and

communication hardware. The heterogeneous nature of these devices, most of which battery-powered and interconnected via wireless network interfaces, makes discovery and treatment of information security incidents a very demanding effort. The modern IoT technology can even create its own communication network without the help of dedicated infrastructure by utilizing its embedded wireless communication. [6]

Some IoT devices are not protected by sufficient access control. [7] However, the IoT cannot purely focus on network security. An application layer must be included. [8]

Replacing common metering devices used in households with smart devices is a reality in a larger part of the world today. The introduction of smart meters with the ability to read data remotely has become routine instead of the current "dummy" devices which needed to be physically accessed and periodically read.

The IoT trends have influenced electronic industry in Croatia and Slovenia as well. A local manufacturer has introduced IoT technology into metering devices, i.e. Iskraemeco AM550, an electricity meter that has been seen in use in the Republic of Croatia. This device provides two-way (''energy'') measurements, active energy and power, 4Q reactive energy & power, apparent energy & power, instantaneous value of voltage, current, power factor, frequency and power and an absolute measurement of active energy & power. [4] [9]

Additionally, this device has more possibilities of reading data. Optical port, RJ11 (for in-house display), wired and wireless M-bus, WAN/NAN Communication modules – PLC G2/G3, also point-to-point 2G/3G/4G. [9]

II. COLLECTION OF PERSONAL DATA BY SMART DEVICES

Unlike previous "dummy" devices, smart devices have two important differences:

a) they collect substantially more data,

b) the ability to read data remotely is a common feature.

As an example, we can take the aforementioned measurement of household electricity consumption (which is often the first device to be installed as a smart device). With a standard meter, we can read the consumption of the past time, if we stand in front of the device (that is, on a monthly reading, spending over the last month).

With smart meters, it is possible to read consumption at a specific time, which provides us with very sensitive personal and private information. Such a device monitors the power consumed at the exact time and it is possible to find out when tenants/users are usually in the household, or when they spend time outside the household. Such information may be valuable to the third malicious parties. In addition, with a little knowledge of the average consumption of the appliance, it is possible to reconstruct when tenants go to sleep, when they shower, whether they use the oven, what are their customs regarding the heating of the object etc.

Specifically, these are very sensitive private information. Collected information can also lead to the conclusion of how many tenants/users are currently in the household. Also, such information may be of interest to insurance companies, life insurance may be interesting to know if a person eats late or has other unhealthy lifestyle habits that can be indirectly detected.

Weaver wrote: "Residential utility customers have a legitimate expectation to preserve individual and behavioral privacy with regard to energy-related or water consumption data collected by the utility. (…) Furthermore, there is a deep concern that inadequate cyber security measures surrounding the digital transmission of smart meter data will expose such data to misuse by authorized and unauthorized users of the data." [10]

What a "smart" memory meter looks like was described back in 2010. [11]. Figure 1. shows power segments (appended with labels from activity logs) per day for one of the households.

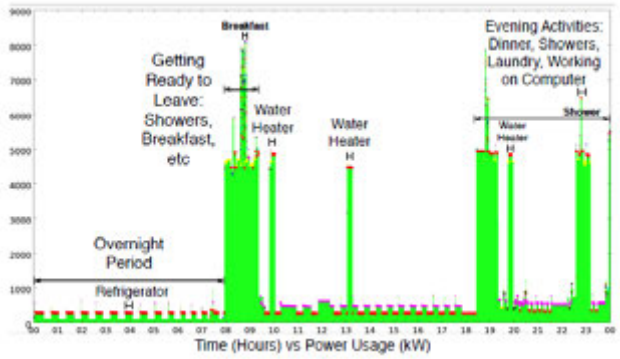

Figure 1. Example day-long second-level power trace [11]

Figure 2. reveals when users/consumers were in one of the households over the course of a month with weekends highlighted.

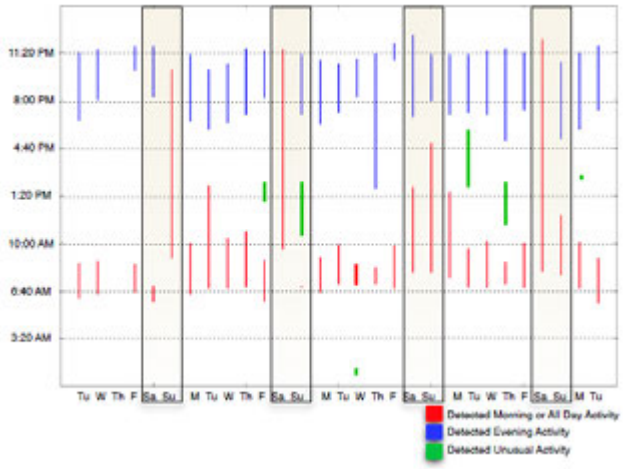

Figure 2. Identification of human presence with high [11]

Authors summarizing that analysis demonstrate how easy it is to identify private information from smart meters. [11]

Let's remind ourselves, when we talk about service providers, we are talking about companies that collect data from tens or hundreds of thousands of users! In addition, when it comes to malicious hacking, a malicious party can access a large number of measuring instruments in a very short period of time, because their security systems are similar and often defaulted (see infra).

Even before the "smart devices" era, in 2012, British Information Commissioner's Office has already warned how data from different measurement devices represent personal information: "Data concerning the water consumption for a particular address will be tenants' personal data due to the fact that data determines how much that individual will be charged off." [12] This can be applied to smart devices.

Information Commissioner's Office states another important fact regarding the collection of various consumer spending data: "Also, if necessary, the water utility company is likely to be able to easily obtain the name of, if not the occupier, then at least the registered owner of the property." Utilities are usually connected and closely related to the local government, often linked to management and ownership. Therefore, it is very easy to link and misuse different consumption metrics with personal and proprietary data.

General Data Protection Regulation (further: GDPR) does not specifically mention IoT devices, but according to material scope in the Art. 2. of the GDPR includes IoT devices: "This Regulation applies to the processing of personal data wholly or partly by automated (…). [13]

GDPR in Recital 6 acknowledges: "Rapid technological developments and globalization have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities." [13]

For data collected by different meters it is important Recital 39 of the GDPR: ""Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing." [13]

Regarding the ability to read IoT devices remotely, the service provider must apply appropriate safeguards in accordance with rectal 83 of the GDPR: "In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected." [13]

An IoT device, such as a power or water meter, is a substantially different device from a "dummy" meter. It enables the collection of a whole range of very sensitive information about the service user. Recital 60 of the GDPR states: "The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed." [13]

Do service providers inform the user of a substantially different, wider, and more accurate range of data collected by IoT meters and other devices in comparison to "dummy" devices? For example, in Croatian business practice, a service user who receives an electricity meter only signs the record that the meter has been replaced.

IoT devices can easily be used for "profiling". By the GDPR definition, profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person. In such case, according Recital 60 and the Art. 13. the data subject should be informed of the existence of profiling and the consequences of such profiling. [13]

Also, the question about the devices for measuring energy consumption should be looked beyond the GDPR itself, taking into account the overall capabilities of these devices, not just the set of functions used by the service provider.

Relationship between users/consumers of utilities and similar services and providers of these services cannot be viewed only through the view of the GDPR, but also through regulations governing consumer protection. Users should therefore be aware of the possibilities provided to the service provider by the IoT measuring device, in order to get acquainted to what they give their consent when using such devices. Also, they should be aware that such devices are potentially vulnerable by the third parties.

Appropriate and quality data protection on the servers of the service providers does not necessary mean much if an unauthorized person can easily read the device located in front of the household of any potential service user.

III. INFORMING USERS ON THE IMPACT OF IOT DEVICES ON THEIR PRIVACY

The basic relationships between the various utility providers and consumers are governed by consumer protection regulations. The basic consumer protection regulation in the European Union is Directive on consumer rights. [14]

Scope of Directive on consumer rights is noted in the Art. 3 "This Directive shall apply, under the conditions and to the extent set out in its provisions, to any contract concluded between a trader and a consumer. It shall also apply to contracts for the supply of water, gas, electricity or district heating, including by public providers, to the extent that these commodities are provided on a contractual basis." [14]

Directive on consumer rights regulates in detail consumer information rights. According the Art. 1, "The purpose of this Directive is, through the achievement of a high level of consumer protection, to contribute to the proper functioning of the internal market by approximating certain aspects of the laws, regulations and administrative provisions of the Member States concerning contracts

concluded between consumers and traders." When 'consumer' means any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession; and 'trader' means any natural person or any legal person, irrespective of whether privately or publicly owned, who is acting, including through any other person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession in relation to contracts covered by this Directive. [14]

In the Art. 5. "Information requirements for contracts other than distance or off-premises contracts" (distance or off-premises contracts have additional rules which are not important for this paper) Directive on consumer rights quote that before the consumer is bound by a contract other than a distance or an off-premises contract, or any corresponding offer, the trader shall provide the consumer with the information in a clear and comprehensible manner, the main characteristics of the goods or services, to the extent appropriate to the medium and to the goods or services. Such obligation shall also apply to contracts for the supply of water, gas, or electricity, where they are not put up for sale in a limited volume or set quantity.

Directive on consumer rights does not regulate smart devices and utilities connected with IoT. We believe that consumers should have the right to be informed about smart devices that will be implemented in their households in the future, which measure services such as water, gas, or electricity. This problem is not fully covered by the GDPR. "To summarize its material scope, the GDPR applies to any processing of personal data. The Regulation will become relevant for companies as soon as any data processing takes place. The (material) scope is interpreted in a very broad manner in order to ensure a high level of protection." [15]

Here, we shall mention the previous acquaintance of the user with the possibilities of the device, specifically the acquaintance with the criteria. In our opinion, the consumer should give his consent to any new IoT "smart" device that the utility provider would like to implement in its property for the purpose of simplifying service metering. The trader must inform the consumer about the functionality and the relevant interoperability of device, especially meter.

The capabilities of IoT devices are as we already mentioned, substantially wider than the actual range of data that provider is processing at some point! Security of IoT devices is generally not satisfactory, 2019 reports mention increasing attacks on IoT systems. "Internet of Things (IoT) has become a primary target for cybercriminals. The repeated security incidents on IoT devices represent a rising trend for IoT attacks. The proliferation of connected devices in consumer, enterprise, and healthcare organizations, and their internal vulnerabilities, have created a security blind spot where cybercriminals can launch a Zero-day attack to compromise devices like webcams, smart TV, routers, printers, and even a smart home." [16]

As an example. Portals for IT-experts noted in 2019. about malware called Silex. "Silex works by trashing an IoT device's storage, dropping firewall rules, removing the network configuration, and then halting the device. It's as destructive as it can get without actually frying the IoT device's circuits." [17]

There is interesting example from Russia, where government has recently mandated that all electricity meters be replaced by online smart meters. It open new "black market", Russian criminals started modifying and selling customized firmware for such devices. These modified smart meters are marketed on black market as a means to save on monthly residential bills for electricity, water, and gas."[18] Authors of same document predict that in the future, hacking smart meters may become lucrative for criminals.

Let us ask ourselves a question: is today already possible to order vendor cheating software to show a lower consumption of benchmarks, and/or could the same software be used to "increase" the bill to a non-sympathetic neighbor? Or to gather information about when someone is in the household? Obviously, it is possible. If a device can be hacked, it can be misused, regardless of which set of data is collected by the provider. A hacker or a user of such services (who commissioned the hacking service on the black market) may use the device and data for completely different purposes than those collected by the service provider. Therefore, we believe that the installation of these devices should be governed by consumer protection regulations, not by the GDRP!

And let us also take into consideration another fact, Moore in his book "Crossing the Chasm" shows model which describes the market penetration of any new technology product in terms of a progression within the types of consumers it attracts throughout its useful life:

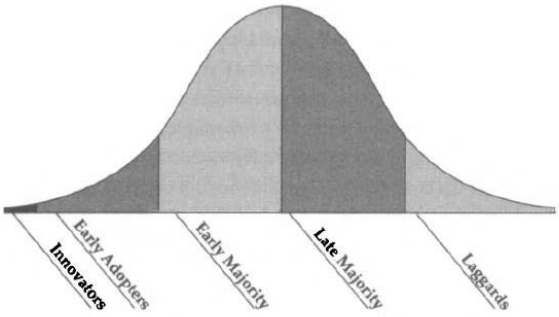

Figure 3 Technology adoption life cycle by Geoffrey A. Moore [19]

The chart above clearly illustrates why IoT devices are vulnerable. Although it cannot be directly applied to metering devices (their introduction depends on the provider), it can be applied to all the other IoT devices. Initially used by enthusiasts and advanced users who are usually familiar with technology, security systems, and hacking devices. And then later, as the device becomes standard, it is increasingly bought by users who lack specialized knowledge and skills, further increasing the vulnerability of these devices.

In order to gain its full affirmation, it is necessary to ensure the highest possible degree of security and privacy

in the use of IoT devices and the proper operational implementation of IoT.

There are several potential threats:

- Security threats: refers to the prevention of financial harm that can be experienced by users and IoT service providers, as well as the loss of reputation and payment of provider penalties
- Privacy abuse: unethical usage of users' data and users' habits
- Operational threats: data loss, contract breach and inaccurate data.

To make building and using IoT platforms safe to use, the American non-profit organization OWASP (Open Web Application Security Project) analyzed IoT technology and listed 10 IoT vulnerabilities in its 2018 report**:**

1. weak, Guessable, or Hardcoded Passwords,
2. insecure Network Services,
3. insecure Ecosystem Interfaces,
4. lack of Secure Update Mechanism,
5. use of Insecure or Outdated Components,
6. insufficient Privacy Protection,
7. insecure Data Transfer and Storage,
8. lack of Device Management,
9. insecure Default Settings,
10. lack of Physical Hardening. [20]

In short, IoT meters are sensitive to a whole range of potential threats. They are also vulnerable outside the scope of the GDPR, as they can be abused by the third parties, especially if they are not adequately protected or properly maintained by the utility provider, or the devices are not maintained properly. Problems can also occur outside of the service provider itself - for example, cessation of upgrades by the manufacturer.

Therefore, we believe that the user should be aware of such potential threats and should give prior consent to the use of IoT devices.

IV. PROPOSAL FOR NEW EU-REGULATION

We believe that Directive on consumer rights should be supplemented. Possibilities and threats of IoT devices should be listed in the recital. Furthermore, in the Art. 5. of the Directive (Information requirements for contracts other than distance or off-premises contracts), it states that consumer information should be supplemented by a new point which should read:

"The utility provider is obliged to explain to the recipient of the service when placing an IoT device (measuring device) into the household, including:

- what are the purposes of measuring of such a device,
- where can it be used and,
- what capabilities of this type of reading the device has."

Also, with each implementation of the new device comes an instruction on the device, which previously stated what are the main technical capabilities of the device that is being implemented into the household.

In Britain, Guy Herbert of NO2ID says: "Smart meters are presented as an environmental and power-saving initiative. But it's a highly surveillant model. It can tell how many showers you have had, when Evidence of the race to monetize the data from smart meters is already emerging." [21]

Moreover, what we would like to point out is the reasonable fear that once the data is released, it can ''fall into the wrong hands'' and in that field the big data market will open very quickly, which will potentially be very dangerous for citizens and another possible attack on their personal and private information. What can be even worse if a third party who is not even a utility operator reaches this large amount of data and knows the devices at the technical level because the devices themselves are not protected from intrusion by third parties and they can simply resell such data or compromise the privacy of the individuals who have been hacked.

V. CONCLUSION

Due to the reasons outlined above, it is clear that utility data collection methods for electricity, and also gas or water usage of data for home users using smart meters could represent an unnecessary and unreasonable invasion of privacy. IoT devices, and especially here we emphasize measuring devices, pose a serious privacy and security risk, and users of such devices should most certainly be informed of what kind of data could such devices read. Although at first glance this obligation appears to be covered by the provisions of the GDPR, however, the issue of notifying end-users is much broader.

According to the GDPR, 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. [13] About that controller has obligation to inform a natural person.

Therewith, IoT ecosystem often has insufficient protection, and they are often left with default passwords, and it is also to be expected that many consumers won't even have many years of technical support and regular security upgrades. In such cases, potential for abuse is much broader than the data set collected by the operator and the obligation to notify the user. Therefore, the authors believe that European consumer protection regulations should cover both IoT and metering devices in such a way to impose an obligation of informing users of the capabilities of such devices, privacy threats, and measures to be taken by the users for their own safety; primarily changing initial device codes. Nevertheless, when introducing smart meters, the users should be explicitly aware of the capabilities and purpose of these devices.

As Tan noticed: "IoT ecosystem involves multiple parties in multiple jurisdictions in multiple countries." [22] Thus, the system only becomes more complicated and

prone to attacks by the third malicious parties and exploitation of all user information collected by the system through smart meters.

Recognizing the fact that IoT devices are increasingly being used by users who are not experts, and utilities do not even ask users if they would like to install such devices in their households, therefore we propose the aforementioned amendments to the Directive on consumer rights which would oblige utilities introducing smart devices, and even sellers of smart devices, to inform consumers of all the functionalities of these devices, the ability to collect data, the ability to read data from these devices, and the purpose for which data will be used, given that the most of the read data is actually unnecessary for the utility provider when issuing the invoice. The obligation to provide detailed information on device capabilities and their potential impact on privacy should be explicitly defined for metering IoT devices - which are installed without the option to refer the users to the capabilities of the device, and sometimes without even referring to the fact that the usual scale has been replaced by IoT device.

VI. REFERENCE

[1] A. Meola, "What is the Internet of Things (IoT)? Meaning & Definition", 2018, Available: https://www.businessinsider.com/internet-of-things-definition [Accessed 17 2 2020]

[2] M. Hung, "Leading to IoT" Available: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf [Accessed 17 2 2020]

[3] "Risk or Reward:What lurks within your IoT?", 2017 Available: https://assets.kpmg/content/dam/kpmg/pl/pdf/2018/02/pl-Raport-KPMG-Risk-or-reward-What-lurks-within-your-IoT.PDF [Accessed 17 2 2020]

[4] G. Vojković, M. Milenković and T. Katulić, "IoT and Smart Home Data Breach Risks from the Perspective of Croatian Data Protection and Information Security Law", in *Proceedings of theENTRENOVA -ENTerprise REsearch InNOVAtion Conference*, Rovinj, Croatia, 2019

[5] F-Secure, "Attack Landscape H1 2019", 2019 Available: https://blog-assets.f-secure.com/wp-content/uploads/2019/09/12093807/2019_attack_landscape_report.pdf [Accessed 25 2 2000]

[6] H. Peterson, E. Baccelli, M. Wählisch and J. H. Schiller, "The Role of the Internet of Things in Network Resilience", in *Internet of Things. IoT Infrastructures. First International Summit, IoT360*, Rome, Italy, 2014

[7] R. Sagy, "Internet of things security: new connections, new threats", IBM, Las Vegas, 2016

[8] H. Suo, J Wan, C. Zou and J. Liu, "Security in the internet of things: a review", in *2012 4th International Conference on Computer and Automation Engineering (ICCAE 2012)*, Mumbai, India, 2012

[9] Manufacturer page, "Iskraemeco", 2019 Available: http://www.iskraemeco.com/files/5514/3982/5764/AM550.pdf [Acceseed: 18 2 2020]

[10] K. Weaver, "How Smart Meters Invade Individual Privacy," SkyVision Solutions, Available: https://smartgridawareness.org/privacy-and-data-security/how-smart-meters-invade-individual-privacy/ [Accessed 25 2 2020]

[11] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet and D. Irwin, "Private Memoirs of a Smart Meter", in *BuildSys 2010*, Zurich, Switzerland., November 2, 2010

[12] Information Commisioner Office, "Determining what is personal data, v1.1, 20121212" Available: https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf [Accesed: 19 2 2020]

[13] "Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),L 194/1 OJEU

[14] "Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council", L 304/64

[15] V. Paul and A. Von Dem Bussche, "The EU General Data Protection Regulation (GDPR)", Springer International Publishing, 2017

[16] R. Srinivas, "10 IoT Security Incidents That Make You Feel Less Secure" CISOMAG, 10 January 2020 Avaiable: https://www.cisomag.com/10-iot-security-incidents-that-make-you-feel-less-secure/ [Accessed 23 2 2020]

[17] C. Cimpanu, "New Silex malware is bricking IoT devices, has scary plans," ZDNet, 25 June 2019 Available: https://www.zdnet.com/article/new-silex-malware-is-bricking-iot-devices-has-scary-plans/ [Accessed 23 2 2020]

[18] S. Hilt, V. Kropotov, F. Mercês, M. Rosario and D. Sancho, "The Internet of Things in the Cybercrime Underground", Trend Micro Research, 2019

[19] G. A. Moore, "Crossing the Chasm, 3rd Edition: Marketing and Selling Disruptive Products to Mainstream Customers", HarperBusiness, 2014

[20] OWASP, "OWASP Internet of Things," 2018 Available: https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf [Accessed 25 2 2020]

[21] P. Collinson, "Is your smart meter spying on you?", The Guardian, 2017 Available: https://www.theguardian.com/money/2017/jun/24/smart-meters-spying-collecting-private-data-french-british [Acessed: 20 February 2020]

[22] S. Tan, " How safe is your personal data collected by your smart devices?", The Business Times, 2018 Available: https://www.businesstimes.com.sg/opinion/how-safe-is-your-personal-data-collected-by-your-smart-devices [Acessed 20 2 2020]