sciendo

IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law

Goran Vojković, Melita Milenković
University of Zagreb, Faculty of Transport and Traffic Sciences
Tihomir Katulić
University of Zagreb, Faculty of Law, Croatia

Abstract

Background: IoT and smart devices have become extremely popular in the last few years. With their capabilities to collect data, it is reasonable to have concerns about the protection of users' personal information and privacy in general. **Objectives:** Comparing existing regulations on data protection and information security rules with the new capabilities provided by IoT and smart devices. **Methods/approach:** This paper will analyse information on data collected by IoT and smart devices and the corresponding legal framework to explore whether the legal framework also covers these new devices and their functionalities. **Results:** Various IoT and smart devices pose a high risk to an individual's privacy. The General Data Protection Regulation, although a relatively recent law, may not adequately regulate all instances and uses of this technology. Also, due to inadequate technological protection, abuse of such devices by unauthorized persons is possible and even likely. **Conclusions:** The number of IoT and smart devices is rapidly increasing. The number of IoT and smart home device security incidents is on the rise. The regulatory framework to ensure data controller and processor compliance needs to be improved in order to create a safer environment for new innovative IoT services and products without jeopardizing the rights and freedoms of data subjects. Also, it is important to increase awareness of homeowners about potential security threats when using IoT and smart devices and services.

Keywords: IoT, smart homes, security, data protection, personal data protection
JEL classification: K22
Paper type: Research paper

Received: Dec 17, 2019
Accepted: Jul 16, 2020

Citation: Vojkovic, G., Milenkovic, M., Katulic, T., (2020), "IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law", Business Systems Research, Vol. 11, No. 3, pp. 167-185.
DOI: https://doi.org/10.2478/bsrj-2020-0033

Introduction

A current buzzword in the field of information technology – IoT (Internet of Things) -is expected to create a whole new sector of products and services. Recent Cisco

research estimates predicted a 43% year on year growth of IoT connections (Bhattacharjya et al., 2018). Unfortunately, it is also increasingly connected with the rise of information security incidents and potential personal data breaches with significant impact on the privacy of individuals around the world (Lin et al. 2016). Legal science, especially in the field of data protection has only recently started to acknowledge the scope of the problem (Bu-Pasha, 2020; Edwards, 2016; Yang et al., 2019).

Sometimes referred to as the internet of everything or industrial network, IoT is a broad term that encompasses various technologies. Most commonly it is understood as an adaptable technology allowing machines and devices to interact with each other over the Internet. It allows for remote control and access through existing network infrastructure, provide opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention (Balamurugan et al., 2018). It however creates an increasingly complex environment to ensure the recognized fundamental rights such as privacy and data protection (Geneiatakis et al., 2017). While there is a particular research into the effect smart home and smart city development has had on the protection of rights and freedoms of individuals, there are many issues and aspects that need to be visited and considered when considering the mechanisms applicable from the current legal framework. The current state of legal science explores unequivocally legal issues of transborder transfer of data (Sullivan, 2019), trustworthiness of personal digital assistants (Furey & Blue, 2019), efforts in establishment of user centric privacy (Skarmeta et al., 2019) to ideological resistance to smart home platforms as strongholds of digital capitalism (Goulden, 2019). Therefore, remarkably underlying the conflict between the struggling efforts of lawmakers and the indominable march of information technology development. With that in mind, the focus here is to analyse whether current provisions can be used to approach data protection and information security issues and serve as adequate compliance mechanisms.

The security threats posed by IoT devices have already been described in the literature (Jurcut et al., 2020). When we include more data collection capabilities enabled by smart meters (Iskraemeco, 2019) we come to a new situation that is not foreseen by the existing legal framework. Nor does the General Data Protection Regulation (GDPR, European Commission 2016a), as a new regulation, and consumer protection regulations, adequately regulate these new areas of possible violations of personal privacy. In this paper, using technical knowledge and comparing it with the legal framework, our intention to show to what extent the legal framework can be applied, and where amendments are needed. We will use the provisions, and recitals of regulations that speak about the purpose of regulations. This explanation is important because targeted interpretation. Targeted or teleological interpretation or interpretation from the status of only one of the many methods of interpretation or interpretation came to the most important, decisive method (Kačer & Ivančić-Kačer, 2019, p. 400).

IoT devices provide services to all kinds of applications through data gathering, identification, processing and communication capabilities. IoT connects infrastructure components and services for smart homes and offices, smart city infrastructure and is applicable in various fields of work – from general industry to real estate, healthcare, public safety. In principle, IoT generally allows for more interactive and efficient transportation and power utilities, etc. (Tzafestas, 2018). Developing IoT infrastructure can be expected to contain massive numbers of different sensors that collect, process and transfer data in addition to already widespread personal information processing

devices that are omnipresent in daily use such as personal computers, smartphones, television sets, game consoles and digital media reproduction devices.

Because of these characteristics, IoT is a technology of interest for modern hackers and cybercriminals. "While IoT deployments have been receiving much hype, their unique characteristics coupled with their interconnected nature indeed present new security challenges. Various technical difficulties, such as limited storage, power, and computational capabilities hinder addressing IoT security requirements, enabling a myriad of vulnerable IoT devices to reside in the Internet-space. Indeed, unnecessarily open ports, weak programming practices coupled with improper software update capabilities serve as entry points for attackers by allowing malicious re-programming of the devices, causing their malfunction and abuse" (Neshenko et al., 2020). Another point to consider is that the data that are generated around a single device may not be sensitive in itself. However, Iot networks usually consist of a large number of interconnected devices and when data is combined with data generated from other devices, it can reveal information such as the consumer habits, patterns of behaviour, and other data which may present significant risk for rights and freedoms of data subjects. New functionality brings new data security and privacy challenge, experts noticed that the weakest links of IoT can be driven by the low-cost devices with low security and cryptography technologies (Vongsingthong & Smanchat, 2015). Obviously, as IoT as a broad term encompasses many potential uses, it is not possible to cover all the issues and questions in the space available. In this paper we deal mostly with risks and challenges facing IoT smart home devices and not the IoT in industrial environment (smart containers and similar) in general, although it might not be possible to draw an exact line between such uses judging from the way these devices are incorporated into wide area networks. The General Data Protection Regulation has been in force only two years, from 25th May 2018. Meanwhile, the replacement of many measuring devices with smart meters has begun. Such smart meters that provide the utility provider with a significantly better insight into the life and habits of the user, require precise regulation. Users need to be aware of what kind of data is being collected on them. Furthermore, a large number of other smart and IoT devices do not have quality protection. Consumers need to be aware of this, which is not within the scope of the GDPR, but consumer protection regulations. In this paper, we would like to raise awareness of the need to apply and improve the legal framework.

Therefore, we prove why IoT devices represent a higher risk for personal data than previous monitoring technologies. After all, we put into perspective that technology and GDPR, including recitals, show us the purpose of Regulation. Since the GDPR includes information security requirements, and security is also important for devices that are not directly connected to service providers, we analyse the IoT and information security regulation with typical cases of IoT security breaches. As many metering devices do not collect user names directly (e.g. a three-tenant apartment), we analyse whether the data of such devices is still personal data. . Finally, concluding that the GDPR does not provide all the answers related to the safety, we also analyse the legal framework for consumer protection and make proposals for new regulations.

IoT personal data processing as a source of risk

While obviously far more efficient than previous monitoring devices, the IoT based devices equipped with sensors that can obtain personal data present a potentially considerable risk for personal data breaches and consequently rights and freedoms of data subjects. For example, electricity suppliers change the existing electricity consumption meters in households to the new digital meters which, as they are

connected to the Internet and allow various levels of internet access, represent a significant fraction of total IoT devices currently in use.

In a corridor of a residential building, on a standard electricity meter, the consumption in the accounting period, and day/night consumption are stored locally. The data on consumption is available only to a person physically in front of the meter, and that person can usually see the actual current consumption per rotation speed. On the other hand, a question whether a person is currently present in the household and is using an electrical appliance can usually only be ascertained by directly observing the meter, in the SE Europe the meter is usually positioned in the corridor of the building. These appliances are now being replaced by smart meters running as IoT devices.

As a local example, let us consider the function of a typical meter such as the "Iskraemeco AM550" electricity meter which is extensively being installed with users in the Republic of Croatia (further: Croatia). The device offers several ways of communication that exclude a need for manual readings such as Full DLMS-COSEM and IEC 1107 compliance; four independent communication interfaces: Optical port, RJ11, for in-house display, M-bus, wired and wireless, WAN/NAN Communication modules – PLC G2/G3, and point-to-point 2G/3G/4G. The manufacturer itself states that specific user applications for "Smart Grid" features are new levels of ability to customize the meter (Iskraemeco, 2019). The device is capable of measuring much more than electricity consumption itself, it also 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 (Iskraemeco, 2019).

This device has been singled out as an example due to the fact it has been installed in many households in Croatia and the region, however there are many similar devices that can be found in the market elsewhere. It is obvious that a device that has so far only measured the power consumption has been replaced by a much more capable one, one that now also measures several other values that can directly or indirectly be used to follow and profile the user behaviour through time, presenting a potential new risk for the data subjects.

Another example can a be smart water meter. One of these products readily available in the European market is "Apator smart +" class of water meter. For this example, we can use S SMART+ - VANE-WHEEL SINGLE-JET DRY WATER METERS (DN15-20). It is described thus: " For measuring the flow and volume of water with a temperature up to 30 °C or 50 °C, or warm water with a temperature up to 90 °C in the closed-circuit system with the full flow of the flux, and on the maximum working pressure up to 16 bar (PN16)." Features of device include: " Pre equipped for installation of radio module for communication in the Wireless M-Bus, impulse module and M-Bus module" (APATOR, 2019).

If that module is installed reading the collected data is quite simple: "Wireless M-bus is a complete solution for wireless reading of various scales. Communication takes place at 868 MHz according to the wireless M-bus protocol (standard EN 13757-4: 2005). The ''Walk-By-Read mode'' uses a handheld reader or a laptop equipped with a Bluetooth converter. In most cases, we perform the drive-by reading, meaning that our smart car equipped with antennas and a Bluetooth converter can come in front of the building and all internal water meters are read automatically and when we enter the shaft to read the main water meter, we immediately know if there is any difference in the reading " (Vodoservis Mate, 2019).

Communication standard is widespread and documented: BS EN 13757-4:2005 Communication systems for meters and remote reading of meters. Wireless meter readout (radio meter reading for operation in the 868-870 MHz SRD band). Water meter does not collect an extensive data set like electricity meter, but one who has access and collects data daily or every few days can collect sensitive data, for example when households is empty. Experts agree that using Internet of Things technologies leave many of the safety concerns ultimately with and in the hands of the consumer. (Tzafestas, 2018).

Should an unauthorized and potentially malicious user obtain access to the data of the electricity meter, there could be unintended but potentially very serious consequences for the data subject. For example, if data on power consumption could be established, with knowledge of the energy and consumption of individual devices, the malicious users could easily obtain real time and historical data about data subjects habits and behaviour such as when the resident comes home from work or other functions, which is the optimal room temperature preferred or even when energy intensive appliances such as ovens or vacuum cleaners are being used indicating activity or habits. Additionally, it could be ascertained when the occupant/data subject is showering, whether there is more than one person in the apartment, when and how long they watch television or spend time in various places in the household. What once was a simple record of electricity consumption now is representing a detailed record of personal life and habits.

Speaking from the legal perspective, the current situation with the lack of security of connected products has been somewhat helped by the fact that manufacturers have not been held responsible with respect minimum information security levels of their product. Since the consumer awareness is still low, there have not yet been enough cases to establish the clear frame of their liability. Since there is no regulatory nor economic incentive, the market fails to provide appropriate measures. (Opinion Consumers and IoT security, 2019). This makes the devices extremely vulnerable, when there is no obligation to install updates or apply similar measures, even middle skilled hacker can jeopardize device.

IoT devices can also be misuse for DDoS attacks. "Consumer products that fall in the IoT category are connected products. Their connectivity will typically be to a service accessible over wide-range (e.g. Internet) protocols and optionally to a smartphone application accessible over short-range protocols (e.g. Bluetooth, WLAN, etc.). In scenarios where IoT products are compromised and used in a distributed Denial-of-Service (DDoS) attack, it is the former type of connection that is exploited by malicious actors" (Opinion Consumers and IoT security, 2019).

IoT and General Data Protection Regulation

While the new European general framework of data protection, the General Data Protection Regulation (GDPR), does not specifically mention IoT devices, nor do the national application laws such as the Croatian General Data Protection Regulation Application Act, it does feature a number of recitals and provisions applicable to data collection through smart home devices and IoT.

In preamble, the Regulation in Recital 6 of the GDPR acknowledges that: "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. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and

social life and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organizations, while ensuring a high level of protection of personal data" (European Commission, 2016b).

The legislative response to these developments from the perspective of data protection, apart from the General Data Protection Regulation and associated Directives and Regulations such as the Directive 2016/680 and the Directive 2016/680 and the Regulation 2018/1725, has been mostly through the national implementations acts dealing with the position and competences of independent national supervisory bodies and regulating the issues left by the GDPR to the national legal systems, as well as updating national laws to comply with data protection principles set forth by the Regulation.

According to a study by the Global Privacy Enforcement Network in 2016, most of the connected devices fail to adequately explain to customers how their personal data is processed which is now a direct violations of the transparency principle and applicable provisions of the General Data Protection Regulation. Failure to inform data subjects on the details of processing is perhaps not surprising given the extent to which IoT services involve significantly more parties than traditional services, for example, sensor manufacturers, hardware manufacturers, IoT operating systems vendors, IoT software vendors, mobile operators, device manufacturers, third party app developers, however it does represent a significant breach of data subjects rights.(Borelli et al., 2015).

Naturally, IoT products and services allow for collecting large amounts of data, some of which may be of potentially of sensitive nature. As far as the idea of a device that communicates with people or generally exchanges information with the environment in order to facilitate certain tasks, e.g., a washing machine that automatically orders detergents is a concern. It is obvious that certain safeguards need to be undertaken as not to jeopardize the privacy of the users. The Regulation mandates that the service provider ensures the safety and security of processing.

The Regulation takes this further in Recital 39 elaborating on the principles of data protection, especially the principles of purpose limitation, storage limitation and data minimization: "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. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review."

The volume of data that IoT products and services collect can contain personal and sensitive data interesting to a wide array of third parties ranging from financial institutions such as banks and insurance companies, to communications and entertainment service providers as well as market researchers etc.

The integration of home and IoT brings new forms of risks, and residents' perception on these new risks is quite important for the development of smart home technologies. IoT devices use wide array of sensors that collect and process staggering amounts of data. A number of authors have recognized several key points regarding the application of the GDPR to IoT processing, mostly focusing on issues regarding identifying appropriate legal basis (such as the prevalent and often inappropriate use

of consent which is unsuited to many IoT situations), struggle of IoT service operators with data protection principles enshrined by the Regulation such as principles of transparent, fair and legal processing, data minimisation and data security – confidentiality and integrity (Bastos et al., 2018).

These authors correctly suggest that data breach reporting provisions may present, at least at this point in development, a challenging requisite for IoT service and product providers as both identifying risk and determining consequences of a data breach in IoT environment that may number thousands or hundreds of thousands of distinct devices that may work largely independently or predominantly collaborate in a network which is a potentially daunting exercise with no clear cut forensic protocols or assessment schemes.

Another interesting point these authors raise, on which we agree is the requirement of data protection by design and by default as stipulated by the Article 25 of the GDPR. Taking into account the conditions set forth by the GDPR may not be an easy task in development of new innovative IoT devices and services. Cost of implementation of appropriate measures may be prohibitively high considering the relatively simple nature of sensors and monitoring devices that limit the ability of manufacturers to effectively implement efficient technical and organisational measures to help comply with GDPR requirements.

Similar observations were made previously by other authors, notably Wachter who conducted a systematic analysis of available literature in 2018 and identified a number of key issues, some going back to papers published years before GDPR which was adopted in 2016, especially including security and consent. To previously outlined GDPR requirements, Wachter also adds provisions regarding certain data subjects' rights, general security requirements for data controllers and data protection impact assessment provisions (Wachter 2018a).

Most IoT devices have a physical aspect that demands ensuring the physical safety regarding the device as well as the user and the environment that the device is deployed in. This integration between cyber-security and physical safety raises the need for a new approach to these problems and development of sufficient security controls (Columbus, 2018). Smart household appliances such as electricity meters, toasters, TVs, refrigerators, and other smart household appliances can also cause some major issues as they gather a wealth of data and life habits of natural persons living in these households (e.g. the exchange of data between home appliances).

On average, current research shows that the regular smart home ecosystem is one comprised of about 20 smart devices, including the household gateway or router (Pascu, 2018).

Also, this may represent potential threat in the event of exploitation of such data, given that these are personal data of natural persons through which third parties can monitor and use their habits.

In 2014, the European Commission issued a recommendation regarding the preparations for the roll-out of smart metering strategies (European Commission (2014)). In this Recommendation, data protection and security considerations are outlined. It's also quite ironic that mobile phones act as a tracking device so hackers can use their location information to steal data, hurt or at least find out natural persons daily routines and behaviour patterns.

With respect to IoT in context of smart homes, data protection laws demand several considerations mandated by the General Data Protection Regulation and potentially expanded on by national application laws such as *privacy by design and by default*, adequate analysis and treatment of risks to rights and freedoms of data subjects, processing in compliance with the principles of processing and on established and

properly evaluated legal basis (especially concerning potential for widespread unlawful secondary use of collected data).

Users who enthusiastically accept IoT or those that are compelled to do so, i.e. through obligatory replacement of electricity meters are usually not aware of the extent of the processing – the type, nature and volume of personal data collected, let alone their potential (mis)use. The Regulation now mandates that data controllers inform data subjects on the purpose, volume and scope of their processing.

The data controllers, and by extension their data processors offering Internet of things devices and services are required, starting with the Article 5 of the GDPR, to behave in an accountable way towards personal data, processing the data in accordance with the principles and compliance mechanisms put forth by the Regulation.

Through registration process and information channels offered to their users, data subjects using such devices and services should be notified about the nature, volume and scope of personal data processing.

The controllers should adopt proper technical and organizational protection measures, assert the level of risk to the rights and freedoms of their data subjects and regulate their relations with data processors as regulated by the Article 28 of the Regulation.

Needless to say, controllers should carefully examine the processing operations conducted by their devices and services, establish proper and applicable basis for personal data processing and rely on contractual and consent basis according to standards regulated by the new legal framework as well as existing practice as put forth by the Article 29 Working Party and the European Data Protection Board guidance documents, national supervisory body guidance and opinions and established legal practice.

Data controllers responsible for IoT infrastructure will need to develop ways to let users exercise their data protection rights. Some of those rights, such as the right of data portability are there to prevent unwanted user lock-ins often observable in different IT industry fields. There is also a question of user control over collection and processing of data. As before, principles of personal data processing and now firmly recognized and established rights of data subjects and their firm enforcement should help mitigate the feeling of the loss of user control and foster a safer environment for further development of these technologies.

The level of control that data subjects enjoy over their data is largely dependent on how well the manufacturers of IoT based equipment and products manage to inform their customers about the nature and purpose of data their devices collect. This includes both what the data collected is used for and what the likely consequences for the users are (Open Rights Group, 2019). This is the reason why it is necessary to make amendments to the Regulation at Member States level, according to which manufacturers must inform consumers with the installation of new IoT devices in their households on which data can be collected by the particular device.

IoT and information security regulations

As the structure and organization of the Internet does not take into account the borders between nations and other established parameters of competence, the problems concerning the availability and regular service of Internet service providers may have an obstructive effect on one of the Member States or the EU as a whole. Safety and security of network and information systems and the personal data processing that underlines so much of the current Internet economy is the key for development of the internal digital single market as well as increasingly for public

safety as more and more communal infrastructure services rely on networked technology for more efficient and smarter function.

As the EU lawmakers adopted the Network and Information Security Directive, its main objective was to raise the level of Member State cooperation in establishing and maintaining a high level of network and information security throughout the EU (European Commission, 2016b).

Establishing cooperation bodies, defining responsibilities and designating contact institutions in Member States, and adopting national information and network security strategies was a required formal step in this effort, however the regulation of information security obligations for providers in Member States was required by transposing the Directive into national legal systems by 2018. In reality, this process took a while longer but was finally completed in early 2020 with 13 Member States adopting a single national law as the transposition measure and 15 Member States adopting or updating two or more national laws which most of the Member States achieved through one or more national transposition measures.

In the case of Croatia, the transposition of the NIS Directive was carried out through provisions of the Act on Cyber Security of Essential Service Operators and the Digital Services Providers – The Cyber Security Act of key service providers and digital service providers (Hrvatski Sabor, 2018a). It contains the relevant definitions of key terms and concepts (Article 5), applicable criteria for appointing essential service operators and digital service providers (Articles 6-13, Annex I&II), as well as establishing obligations for these service providers in order to maintain adequate level of cybersecurity (Articles 14 through 24).

While the essential service providers are recognized and designated directly by the Act on the basis of NIS Directive Criteria and the comparative practice and experiences of other Member States, the recognition and designation of digital services providers is subject to a procedure. This procedure includes, alongside of criteria as regulated by the Cyber Security Act, designation by the competent body, in this case the Ministry of Economy, Entrepreneurship and Crafts (Hrvatski Sabor, 2018a, Articles 1-3).

Foreseeable use of IoT in offering certain essential services such as power and water distribution, as well as proliferation of smart home devices will trigger recognition and designation of controllers of these services as essential or digital service providers. These controllers are now obliged to implement technical and organizational measures to effectively manage risks as well as measures to prevent and mitigate effects of information security incidents on the security and safety of information systems (Hrvatski Sabor, 2018a, Article 14).

In particular, essential services operators need to implement such technical and organizational measures to effectively ascertain the incident risk, prevent, discover and solve information security incidents and mitigate incident effect to the lowest possible impact level (Hrvatski Sabor, 2018a, Article 15).

In turn, digital services providers when implementing required technical and organizational measures need to ensure safety of systems and installations, incident discovery and solving, maintain service continuity, adequately monitor, audit and test implemented measures and follow recognized information security standards in information security (Hrvatski Sabor, 2018a, Article 16).

The provisions of the Cyber Security Act of 2018 were operationalized in the provisions of the national Regulation on Cyber Security of Essential Service Operators and Digital Service Providers which was also enacted in 2018 (Hrvatski Sabor, 2018c). As there is no case law to examine following the start of application of the new regulations, at this moment speculation about their applicability is purely theoretical.

While the measures contained in these provisions represent an organisational and financial burden for the service providers, they do *prima facie* lead to higher degree of security and the Regulation demands that essential service operators create and manage an information security policy that needs to define goals and guidelines how to preserve the continuity of function of key systems, assess and manage risks, describe the system of information security management including the auditing of implementation of cybersecurity measures, provide key operational security procedures and include organisation and implementation of educational and awareness raising efforts. The Regulation further regulates the obligation of identified essential service providers to ensure physical security of the key systems, to ensure the availability of equipment required for continuing function and maintenance of essential systems etc. The essential service providers are required to manage contractual relations with external service providers that may affect the key systems, including assessing risks before contracting outsourced services and products.

Essential service providers are also mandated to control access to essential system premises, log and note access to essential systems, implement antimalware and anti-denial-of-service (anti-DOS) controls as well as manage development, research and continuity of operation of essential services. The operators are required by the Regulation to conduct vulnerability assessments, and in cases of serious security incidents to notify competent authorities designated by the Cyber Security Act.

Example cases of IoT security breaches

Practical use of IoT is already riddled with numerous incidents and disclosed or discovered vulnerabilities that may reveal the incident threat level and risk for users' rights and freedoms. Some of them were reported on by mainstream news or technology magazine, such as the case of SAM Seamless Network in 2019 (Narendra, 2019)

Smart home appliances offer new venues for attack. An attacker can hack into the smart home system and unlock the front door, open windows or turn on appliances causing damage to the home of the victim. These new type of smart home attacks result in new forms of risks for the residents (Denning et al., 2013). Cameras (security cameras of baby monitor) can be hacked and used for illegal access or join into a zombie network with the purpose to commit a distributed denial of service attack (Wallace, 2018). Garage doors collect data on when you usually arrive home from work, giving tech-savvy thieves information they need to plan a break in. There are many similar examples, and new devices and uses are connected into smart home platforms practically on everyday basis.

The fast growth and proliferation of devices and associated risks would benefit from a systematic overview and classification. One such classification groups risks into the five categories (Apiumhub, 2018):

1. Risk to personal data and privacy: The Internet of Things presents a higher risk to personal data processing.
2. Technical vulnerabilities in authentication: As IoT devices are connected through the network, they usually employ some sort of cloud interface. Its vulnerability may lead to compromise of data subject security.
3. Human factor: As IoT is a relatively new technology, the staff at companies offering these services and products are relatively uninformed which hightens the risks to information systems and data subject personal data
4. Inadequate data encryption: IoT networks usually lack sufficient data encryption capabilities.

Risks of having an increasingly complex information system: the more devices, people, interactions and interfaces, the more the risk for data security also increases. It means that there is more variety and diversity in the system, so the challenge of managing all points in the network to maximize security also increases. Some of the worst case scenarios of IoT attacks that have so far been noted by security researchers include content streaming platform attacks, massive malware distribution attempts, hacking of increasingly connected smart vehicles as well as medical devices:

1. In October 2016, the largest DDoS attack ever occurred on service provider Dyn using an IoT botnet, followed by the crash and unavailability of large sections of the Internet, including Twitter, Guardian, Netflix, Reddit and CNN. This IoT botnet was enabled by malicious software called Mirai. Once infected with Mirai, computers constantly searched the Internet for vulnerable IoT devices, and then used known default usernames and login passwords, contaminating them with malware. Among the devices that were attacked were digital cameras and DVR players.
2. In 2017, the US Food and Drug Administration (FDA) confirmed that certain medical devices had vulnerabilities that could allow hackers to access the devices such as pacemakers and defibrillators used to monitor and control patients' heart functions and prevent heart attacks. Because of the vulnerability of the transmitter, hackers could control the shocks, manage the incorrect pacing, and drain the battery.

a) 3. An IBM affiliated security research website reported a possibility of an attack targeting an Internet connected vehicle. A team of researchers was able to take total control of a Jeep SUV using the vehicle's CAN bus (Dunlap, 2017). The Jeep computer needed a firmware update, and it used the Sprint mobile network, and a team of experts realized they could make the car behave the way they wanted: make it run off the road, slow down and speed up potentially endangering the occupants of the vehicle or bystanders. We can conclude that IoT affects personal data and generally information about people's' habits and their movement, in two (2) ways:

   a) As smart devices are technologically supported by IoT, they collect much more data than "dummy" devices,
   b) IoT devices, on the contrary, are much more vulnerable to hacking or other forms of abuse than classical devices.

These mentioned issues make security issues far more complicated, both legal and technological. Huawei forecasts 100 billion IoT connections by 2025, and McKinsey Global Institute suggests that the financial impact of IoT on the global economy may be as much as $3.9 to $11.1 trillion by 2025 (James, 2015).

Smart devices obviously have benefits for both consumers and businesses. In 2017 alone, the market for these devices brought in $ 84 billion, almost 16% more than in 2016, according to a report by Ablondi (2018). By 2023, 274M homes worldwide, or 14% of all households, will have at least one type of smart system installed (Strategy Analytics, 2018).

While there are various ways to protect consumers from the IoT security threats – education about information security basics as an integral part of digital literacy, changing default privacy and security settings and managing personal access codes etc. - some age long accepted practices still apply in the digital domain. When buying an IoT device or home appliance it is important to know that buying a reliable device from a reputable supplier means greater chance of the supplier satisfying EU data protection and information security regulations such as naming representatives or having accountable subsidiaries in the EU. Such suppliers will have conducted data

protection impact assessments and other compliance activities for their products and the companies themselves, have invested into information security standard certification and have a history of understanding the modern regulatory framework in contrast to cheap products from mostly unknown suppliers available only through wholesale Internet commerce sites.

Safety wise smart home device suppliers and platforms operators should create vulnerability management program. Such program should identify and fix device weaknesses that can emerge over time – a common reason would be the use of outdated operating systems or antivirus software for personal use. "Users' right to data protection and right to privacy must be balanced in the design and governance of identification technologies in the IoT" (Wachter, 2018b).

Therefore, the appropriate measures must be taken to make smart homes safer and more suitable for life. It is also necessary to carry out a careful assessment of safety risks, which must be preceded by security implementation to ensure that all underlying problems are detected immediately and that timely protection measures have been taken.

Discussion

Is IoT Data necessarily a Personal Data?

IoT devices obviously create interesting new legal and policy challenges that lawmakers have not encountered before. At the same time, IoT technologies add to many issues that already exist and manifest in data protection practice (Rose et al., 2015). Utility companies and other similar service providers may claim that the data they collect on IoT devices is not personal data, that is, they do not fall within the scope of GDPR. It is also clear why - the theses we cite in this article state that sensitive personal data may be involved, and the storage and processing of such data must be conducted in accordance with the rules imposed by Regulation. It is not only a matter of formally defining information as personal, but also a matter of security. Art. 32 of the Regulation has the following on the issue of data controller obligations concerning Security of processing: " Taking into account the state -of -the -art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including *inter alia* as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."

Based on the evaluation of the established ECJ and national supervisory body practice and applicable WP29 and EDPB guidelines, data collected by IoT may indeed represent personal data if it relates to an identified or identifiable natural person, and in some cases it may even reveal sensitive data such as data relating to health, biometric data and data related to aspects of data subject behaviour..

The easiest way to avoid the extra cost coming from obligations to ensure safe and secure processing of such data is to deny that data in question are personal information. Therefore, we consider it important to establish here that personal

information is what is indeed at stake. Such an issue is important not only for IoT meters but also for other IoT devices which collect data on the activities of natural persons.

GDPR Art. 4. defines: "'personal data' meaning any information relating to an identified or identifiable natural person; 'data subject'; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Following the coming into force of the Lisbon Treaty and the Charter of Fundamental Rights protection of personal data in the EU has been defined as a fundamental right separate from the right to privacy. GDPR, Preamble 1 also states that "The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her." Also, Preamble 39 quotes: "Any processing of personal data should be lawful and fair."

The question of what belongs to personal data has already been extensively analysed in legal literature and the judicature of ECJ (i.e. regarding the dynamic ip addresses in the Case C-582/14: Patrick Breyer v Bundesrepublik Deutschland). One of the earliest examples is the one published by the UK's Information Commissioner's Office (ICO), analysing the provisions of the UK Data Protection Act 1998 (DPA). ICO's document "Determining what is Personal Data" states: "It is important to remember that it is not always necessary to consider 'biographical significance' to determine whether data is personal data."

This document also cites an example of a case of collecting water measurement data: "A utility company may not record the name of the occupier of the house to which it provides water, but may simply note the address of the property and address all bills to 'the occupier'. Data concerning the water consumption for a particular address will be personal data about the occupier where this data determines what that individual will be charged for. In this last example, even without a name associated with the water consumption data, this data will be personal data in that it determines what the occupier will be charged and the occupier is identified, even without a name, as the person living at the property in question and is therefore distinguished from other individuals. Also, if necessary, the water 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" (Determining what is personal data, 2012).

In countries where utility bills typically come labelled with a user's name, this data represents personal data. Further let's consider that the scope of personal data in practical, if not legal sense, is wider today than it was twenty years ago and on the basis of which these examples are cited. Recent literature supports this view: "It should be noted that personal data can relate to more than one person. For example, the location of a person at any particular time may also constitute the personal data of other known individuals in the same location. Joint property ownership can amount to the personal data of two persons. The content of an email sent by a tenant living in an apartment block complaining about his neighbour may contain information relating to both the complainer and the person about whom the complaint was made. A page of text recording a discussion between two individuals, perhaps including a detailed exchange of views or a disagreement, may be the personal data of both" (Carey, 2018, pp. 14).

Utility providers, telecoms, and other companies can relatively easily collect information about individuals residing in a residential facility, e.g. apartments or houses; consumption bills are tied to the name of the natural person; telecoms additionally offer various benefits of "family packages" to gain an accurate family image), and therefore we can conclude that the data that can be traced on the habits of householders and guests using IoT devices, whether metric or otherwise are undoubtedly personal information, even when they are not individualized, e.g., data on the electricity consumption of an apartment where two people reside.

Comparison of different categories of such data may pose a particular privacy risk, e.g. a utility company in a local government unit may collect data from different measuring devices as well as from other sources, e.g., local video surveillance of parking lots. A negligent or malicious operator comparing such information could get a very accurate and sensitive image of one's movements and habits, and deeply invade a person's privacy.

IoT and customer protection rules

The European Consumer Protection Framework does not regulate IoT and smart devices in terms of informing IoT device users of the ability to collect data by such devices. This is understandable because the legal framework is outdated (Council Directive 93/13/EEC of 5 April 1993, Directive 98/6/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council and Directive 2011/83/EU of the European Parliament and of the Council). National regulations, such as the Croatan Customer Protection Act provides only a brief reference in the need to comply with data protection regulations (Hrvatski Sabor, 2018b).

The new proposed legal framework partly addresses the issue of data collection through the introduction of new digital services (EU to modernize Act on Consumer Protection). Thus, it is proposed that: "In respect of personal data of the consumer, the trader shall comply with the obligations applicable under Regulation (EU) 2016/679." Also interesting is the following provision regarding the provision regarding the use of personal data by the trader, considering the obligations of the trader in the event of termination(Council of the European Union, 2019).

However, there is no obligation on the trader to explicitly inform the user about the ability to collect data from an individual smart device, e.g., electricity meter. This is in stark contrast with the provisions of the GDPR, from the basic principles of processing to the right of data subjects to be informed and to access their data. Here, we mention the Croatian practice - the dummy meter is being replaced by a smart device, where the user only signs a record of the change of the meter, but is not familiar with the new possibilities of collecting data on the changed device, except in the case of self-information.

Conclusion

The focus of this paper was to present the applicable data protection and information security regulative context to the rise of Internet-of-Things data processing paradigm, also to outline the activities that data controllers and processors should undertake to mitigate possible data breaches. Even though personal data protection has been recognized as a fundamental right of individuals in the EU for almost two decades, and after almost the same development period, now there is an established information security regulatory framework with obligations for essential service operators and digital service providers. There is still much effort required to increase awareness of both service providers and the homeowners about potential security

threats that may be possible when using these devices and services. IoT rapidly occupies the global market which brings unprecedented benefits mostly from improved efficiency, accuracy and economic benefits. It changed the world of wi-fi connected devices; thus, they are becoming more interconnected in a smart grid and can easily reduce human intervention which was the idea from the beginning of development.

Our research has confirmed that users should be protected and acquainted with the smart devices implemented into their households according to the GDPR, bearing in mind that utility service install smart devices into their households priorly without letting users know what type of device is being installed, and without their proper consent. Future research should analyse developing comparative law and discuss best practices, especially on the level of EU Member States. The new laws and regulations transposing the NIS Directive and accompanying the GDPR present an opportunity to improve regulatory framework to ensure data controller and processor compliance and create a safer environment for new innovative IoT services and products without jeopardizing the rights and freedoms of data subjects.

The paper predicts and gives examples of practical implications showing that this can sometimes be detrimental to utility users because they are not aware of their rights, and thus do not even recognize potential security threats that cannot be ruled out. In the end, however, the complexity of smart home infrastructure may very well prove impossible to apply standard information security solutions to smart devices such as smart TVs, connected home appliances or connected energy sensors and water distribution services. Therefore, integrated security approach, risk identification, risk management and ultimately accountable behaviour of data controllers and other service providers is of foremost importance.

In this paper we explained how such devices bring numerous savings nevertheless on the other hand IoT brings unsuspected risks in the area of personal data protection and security of infrastructure. As number of IoT and smart home device security incidents continues to rise, it is going to be quite difficult to ensure safe and secure processing of user data without empowering users themselves through active decision-making about the security status of their own IoT home network.

References

1. "EU to modernise law on consumer protection, available at: https://www.consilium.europa.eu/en/press/press-releases/2019/03/29/eu-to-modernise-law-on-consumer-protection/ (15 December 2019)
2. Ablondi, W. (2018), 2018 Global Smart Home Forecast, Strategy Analytics, San Francisco.
3. APATOR. (2019), "JS SMART+ - Vane-wheel single-jet dry water meters (DN15-20), available at: http://www.apator.com/en/offer/water-and-heat-metering/water-meters/vane-wheel-water-meters-to-r100/js-smart-dn15-20 (8 December 2019)
4. Apiumhub (2018), "IoT security issues and risks", available at: https://apiumhub.com/tech-blog-barcelona/iot-security-issues/ (23 February 2019)
5. Balamurugan S., Ayyasamyio A., Suresh Joseph K., (2018), "A Review on Privacy and Security Challenges in the Internet of Things (IoT) to protect the Device and Communications Networks", International Journal of Computer Science and Information Security (IJCSIS),Vol. 16, No. 6, 58-62
6. Bastos, D., Giubilo, F., Shackleton, M., El-Moussa, F. (2018), "GDPR privacy implications for the Internet of Things", in 4th Annual IoT Security Foundation Conference, 4 December, IoT Security Foundation, London, pp. 1-8.
7. Bhattacharjya, A., Zhong, X., Wang, J., Li, X. (2018), "Secure IoT structural design for smart homes", in Rawat, D. B., Zrar, K., (Eds.), Smart Cities Cybersecurity and Privacy, Elsevier, Amsterdam, pp. 187-201.

8. Borelli, D., Xie, N., Neo, E. K. T., "The Internet of Things: Is it just about GDPR?", https://www.pwc.co.uk/issues/data-protection/insights/the-internet-of-things-is-it-just-about-gdpr.html (14 December 2019)
9. Bu-Pasha, S. (2020), "The controller's role in determining 'high risk' and data protection impact assessment (DPIA) in developing digital smart city", Information & Communications Technology Law, Vol. 29 No. 3, pp. 391-402.
10. Carey, P. (2018), Data Protection, Oxford University Press, Oxford.
11. Columbus, L. (2018), "IoT market predicted to double by 2021, reaching $520B", available at: https://www.forbes.com/sites/louiscolumbus/2018/08/16/iot-market-predicted-to-double-by-2021-reaching-520b/#5b35472d1f94 (22 February 2019).
12. Council of the European Union. (2019), "Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Council Directive 93/13/EEC of 5 April 1993, Directive 98/6/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council and Directive 2011/83/EU of the European Parliament and of the Council as regards better enforcement and modernisation of EU consumer protection rules", available at: https://www.consilium.europa.eu/media/38907/st08021-en19.pdf (15 December 2019)
13. Denning, T., Kohno, T., Levy, H. M., (2013), "Computer security and the modern home", Communications of the ACM, Vol. 56 No. 1, pp. 94-103.
14. Determining what is personal data (2012), v1.1, 12.12.2012, ico. Information Commissioner's Office, available at: https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf (15 December 2019)
15. Dunlap, T. (2017), "The 5 worst examples of IoT hacking and vulnerabilities in recorded history", available at: https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/ (25 May 2020)
16. Edwards, L. (2016), "Privacy, security and data protection in smart cities: A critical EU law perspective", European Data Protection Law Review, Vol. 2 No. 1, pp. 28-58.
17. ENISA Advisory Group. (2019), "Opinion consumers and IoT security", available at: https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group/ag-publications/final-opinion-enisa-ag-consumer-iot-perspective-09.2019 (30 September 2020)
18. European Commission (2016b), "Directive (EU) 2016/1148 of the European parliament and of the council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union", available at http://data.europa.eu/eli/dir/2016/1148/oj (27. September 2020)
19. European Commission. (2014), "Commission recommendation of 10 October 2014 on the data protection impact assessment template for smart grid and smart metering systems (2014/724/EU)", available at: http://data.europa.eu/eli/reco/2014/724/oj (27. September 2020)
20. European Commission. (2016a), "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)", available at: http://data.europa.eu/eli/reg/2016/679/oj 27. September 2020)
21. Furey, E., Blue, J. (2019), "Can i trust her? Intelligent personal assistants and GDPR," in 2019 International Symposium on Networks, Computers and Communications, , 18-20 June, IEEE, Istanbul pp. 1-6.
22. Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., Baldini, G. (2017), "Security and privacy issues for an IoT based smart home", in 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, 22-26 May, IEEE, Opatija, pp. 1292-1297.
23. Goulden, M. (2019), "'Delete the family': Platform families and the colonisation of the smart home", Information, Communication & Society. doi: 10.1080/1369118X.2019.1668454

24. Hrvatski Sabor. (2018a), "Zakon o kibernetičkoj sigurnosti operatera ključnih usluga i davatelja digitalnih usluga" (Act on Cybersecurity of Essential Service Operators and Digital Service Providers), Official Gazette of Repubic of Croatia, 64/18.
25. Hrvatski Sabor. (2018b), "Zakon o zaštiti potrošača" (Customer Protection Act), Official Gazette of Repubic of Croatia, No. 41/14, 110/15, 14/19.
26. Hrvatski Sabor. (2018c), "Uredba o kibernetičkoj sigurnosti operatera ključnih usluga i davatelja digitalnih usluga" (Regulation on Cybersecurity of Essential Service Operators and Digital Service Providers), Official Gazette of Repubic of Croatia, 68/18.
27. Iskraemeco. (2019), Manufacturer web page, available at: https://www.iskraemeco.hr/AM550.pdf (28 September 2020)
28. James M., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., Aharon, D. (2015), "The Internet of Things: Mapping the value beyond the hype", McKinsey Global Institute, available at: https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.ashx (26 May 2020)
29. Jurcut, A., Niculcea, T., Ranaweera, P., & LeKhac, A. (2020), "Security considerations for Internet of Things: A survey". SN Computer Science, Vol. 1, Article 193.
30. Kačer, H., Ivančić-Kačer, B. (2017), "O rješavanju antinomija i pravnih praznina (posebno) na primjeru odnosa Zakona o sportu i Zakona o obveznim odnosima" (Resolving antinomies and in particular legal gaps in the example of relations between sports act and obligatory relations act), Zbornik radova Pravnog fakulteta u Splitu, Vol. 54 No. 2, pp. 397- 414.
31. Lin, H., Bergmann, N. (2016), "IoT privacy and security challenges for smart home environments", Information Vol. 7 No. 3, pp. Article 44.
32. Narendra, M. (2019), "Research reveals the most vulnerable IoT devices", available at: https://gdpr.report/news/2019/06/12/research-reveals-the-most-vulnerable-iot-devices/ (11 May 2020)
33. Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., Ghani, N. (2019), "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations", IEEE Communications Surveys & Tutorials, Vol. 21 No. 3, pp. 2702-2733.
34. Open Rights Group. (2019), "Privacy policies for Internet of Things devices must comply with GDPR", available at: https://www.gdprtoday.org/privacy-policies-for-internet-of-things-devices-must-comply-with-gdpr/ (14 December 2019)
35. Pascu, L. (2018), "The IoT threat landscape and top smart home vulnerabilities in 2018", Bitdefender, available at: https://www.bitdefender.com/files/News/CaseStudies/study/229/Bitdefender-Whitepaper-The-IoT-Threat-Landscape-and-Top-Smart-Home-Vulnerabilities-in-2018.pdf (22 February 2019)
36. Rose, K., Elridge, S., Chapin, L. (2015), "The Internet of Things: An overview, understanding the issues and challenges of a more connected world", available at: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf (26 May 2020)
37. Skarmeta, A., Hernández-Ramos, J., Martinez, A. (2019), "User-centric privacy", in Ziegler, S. (Ed.), Internet of Things Security and Data Protection, Springer, Basel, pp. 191-210.
38. Sullivan, C. (2019), "EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era", Computer Law & Security Review, Vol. 35 No. 4, pp. 380-397.
39. Tzafestas, S. G. (2018), "The Internet of Things: A conceptual guided tour", European Journal of Advances in Engineering and Technology, Vol. 5 No. 10, pp. 745-767.
40. Vodoservis Mate. (2019), " Ugradnja vodomjera na daljinsko očitavanje" (Installing remote reading water meter), available at: http://www.vodoservis-mate.com/s/ugradnja-vodomjera-na-daljinsko-ocitavanje/7 (8 December 2019)

41. Vongsingthong S., Smanchat, S. (2015), "Review of data management in Internet of Things", Asia-Pacific Journal of Science and Technology, Vol. 20 No. 2, pp. 215-240.
42. Wachter, S. (2018b), "The GDPR and the Internet of Things: A three-step transparency model", Law, Innovation and Technology, Vol. 10 No. 2, pp. 266-294.
43. Wachter, S. (201a), "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR", Computer Law & Security Review Vol. 34 No. 3, pp. 436-449.
44. Wallace, B. (2018), "A look at the security risks of IoT Devices", available at: https://hackernoon.com/a-look-at-the-security-risks-of-iot-devices-f0d6ffe1441d (22 May 2020)
45. Yang, L., Noe, E., Eliot, N. (2019), "Privacy and Security aspects of e-government in smart cities", in Rawat, D. B., Ghafoor, K. Z. (Eds.), Smart Cities Cybersecurity and Privacy, Elsevier, Amsterdam, pp. 89-102.

About the authors

Goran Vojković, PhD, Associate Professor, Chair of Transport Law and Economics, University of Zagreb, Faculty of Transport and Traffic Sciences. He was born in Split in 1971. He has more than twenty years of work experience in the civil service and private sector, working on different types of jobs; from the Governmental Office Counsellor to the Head of Governing Council of the Port Authority of the port of Vukovar. For four years he was a member of Supervisory board of JANAF company, and, for two terms, he was an external member of the Committee for Legislation of the Croatian Parliament. Also, he has a great experience working on the EU projects both in Croatia and Bosnia and Herzegovina. Currently, he works as an Associate Professor at the Faculty of Traffic and Transport, University of Zagreb, and at the University North, and he co-operates with the other higher education institutions in Croatia. The author can be contacted at **goran.vojkovic@fpz.hr.**

Melita Milenković, LL.M., Research and Teaching Assistant, Chair of Transport Law and Economics. Faculty of Transport and Traffic Sciences, University of Zagreb. She was born in Slavonski Brod, Croatia, she graduated from the Faculty of Law, University of Osijek where she obtained her Master's degree in Law. Currently, she is employed as a Research and Teaching Assistant at the University of Zagreb, Faculty of Transport and Traffic Sciences, Chair for Transport Law and Economics. She is at the 3rd year of doctoral studies programme at the University of Ljubljana, Faculty of Law, presently in the final phase of drafting and submitting a thesis under the title: "Comparative Analysis of Concessions for Managing Airports – the Applicative Croatian Model". She has written papers and articles in the field of Administrative Law, Transport Law, ICT Law and Public Procurement Law. The author can be contacted at **melita.milenkovic@fpz.hr.**

Tihomir Katulić, PhD, Assistant Professor, ICT Law Department, Faculty of Law, University of Zagreb. Teaches undergraduate and graduate courses in Information Technology Law ranging from Personal Data Protection and Privacy in Electronic Communications, Internet Governance, Introduction to Information Security and Intellectual Property. Member of the Internet Society, Croatian Academy of Legal Sciences, Croatian Copyright Society, International Association of Privacy Professionals and Internet Governance Forum. Certified ISO 27001 and ISO 37000 lead auditor and an experienced data protection consultant. Occasionally writes opinions and columns for Croatian magazines Bug, Mreža, Banka, Infotrend, Novi Informator, Poslovni dnevnik, Privredni vjesnik and Sistemac on topics ranging from data protection, copyright, digital media, information security, computer crime to electronic commerce and internet governance. The author can be contacted at **tihomir.katulic@pravo.hr.**