Vojković, Goran; Milenković, Melita; Katulić, Tihomir

Conference Paper

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

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

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

Abstract

IoT technology required to build smart homes, regarding automation and control processes, represents a significant information security and personal data protection challenge. Smart homes demand a new level of security requirements as they contain relevant, vulnerable and private information. Since IoT technology offers opportunities and imposes risks, an IoT based smart home is susceptible to the IoT security vulnerabilities and attacks via Internet. Personal data covering household habits could easily become available to the third parties without data subject consent. The business model created by the smart home technology industry based on sharing the house owners' data with third parties is now facing significant obstacles with regard to data protection regulation and practice being developed in European Union. This paper indicates potential threats and points out current regulatory provisions regarding preserving data privacy and information security in the IoT smart home environment.

Keywords: IoT, smart homes, security, data protection, personal data protection
JEL classification: K22

Introduction

Internet of Things (IoT) is proving to be one of the most prevalent buzzwords in recent years in information technology industry, one expected to create a whole new sector of products and services, but also one increasingly connected to the rise of information security incidents and potential personal data breaches with significant impact on the privacy of individuals around the world.

As a mix of developing and existing technologies applied to a new context, even finding a proper definition of the term is not an easy task. As this technology spreads, its effects are being felt in areas usually reserved for big, centralized, often critical infrastructure such as energy and water transportation and distribution infrastructure, communications, transport but its potential is also to enable citizens using national administrative and legal services (European Commission, N/A).

Market research companies such as Gartner estimate that by 2020 internet-connected devices will outnumber humans interfacing the internet to the ratio of 4-to-1, many of which will belong to IoT paradigm and will create new dynamics for marketing, sales and customer service (Hung, 2017).

While the search history of the term IoT reveals that it was first used in 1999 in an industry presentation dealing with RFID and Internet business integration (Ashton, 2019) probably the first use of the term in context of published scientific research goes back to 2002 and a paper presented by several Finnish researchers with a topic concerning tracking and tracing parcels through a system hosted on a distributed computing infrastructure (Främling, 2002). A relatively recent, by standards of regulation and legal research (but certainly outdated by standards of information technology development) white paper by CISCO defines IoT as Internet of Objects, a next (chapter in) evolution of the Internet, "…*a huge leap in its ability to gather, analyse, and distribute data that we can turn into information*…" (Evans, 2011).

One of the more practical definitions of IoT was provided by global business media: "*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. Cars, kitchen appliances, and even heart monitors can all be connected through the IoT. And as the Internet of Things grows in the next few years, more devices will join that list.*" (Meola, 2018). Similar, another industry leader defines IoT: "*The Internet of Things combines data, cloud, connectivity, analytics and technology to create a 'smart' environment, one in which everyday objects are embedded with network connectivity in order to improve functionality and interaction.*" (Ning, 2013).

A recent fact sheet published by the European Commission (N/A) uses a definition provided by FP7 project CASAGRAS (Coordination and Support Action for Global RFID-related Activities and Standardization):"…*a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and involving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability.*" (European Commission, 2019). It is obvious that omnipresence of IoT devices and services, as well as their interconnection will give rise risks that may endanger individuals and nations alike.

It can be surmised that the general purpose of IoT is to expand the functions of the Internet by increasing the ability to connect numerous objects providing important information to be processed and acted upon in an intelligent way.

By using the IoT model, users can share both the information provided by user behaviour and the information collected by the connected things in the physical world. 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.

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.

IoT, especially in the context of developing smart home infrastructural network is often described as pervasive, local, collecting massive amount of data, by definition largely autonomous and connecting widely heterogenous devices (Vongsingthong et al., 2015).

Value of this technology and the scope of its use is increasing, and so are the budgets allocated for its development and application.

From the perspective of information security, no smart device is insignificant, as each represents a potential attack avenue of attack hackers can manipulate to get inside a home network and take control over devices linked to it.

According to available industry research, the average smart home in the United States houses 11 smart devices, including accessories, at a common rate of 2 devices per home. The most common smart devices in US homes are smartphones (91%), smart TVs (73%) and tablets (72%) (KPMG, 2017).

Smart TVs with 24/7 hours access and connection to the Internet have also become standard; similarly, virtual assistants like Amazon Echo are sold in millions of copies, and as we are often told by innovators and industry experts surely tomorrow there will be a flood of washing machines that automatically order detergents, and refrigerators which order food online hitting the market.

Almost every smart home device can be connected to the Internet. "*Any stand-alone internet-connected device that can be monitored and/or controlled from a remote location is considered an IoT device… almost all products can be an Internet of Things devices.*" (Meola, 2018).

The markets and the consumers have welcomed commercial application of IoT as market research shows that: "…*combined markets of the Internet of Things (IoT) will grow to about $520B in 2021, more than double the $235B spent in 2017. Data center and analytics will be the fastest growing IoT segment, reaching a 50% Compound Annual Growth Rate (CAGR) from 2017 to 2021. System integration, data center and analytics, network, consumer devices, connectors (or things) and legacy embedded systems are the six-core technology and solution areas of the IoT market*." (Columbus, 2018).

We can conclude that IoT has mostly transitioned from the development phase where such smart devices are used by tech enthusiasts, who are usually the originators of new technologies (from radios to PCs), to a widespread everyday use. Smart TVs have become common, smart speakers – virtual assistants (like mentioned Amazon Echo) are also in everyday use, and in some areas the general population does not know that their utility provider, e.g. electricity supplier, has switched to IoT. Such development brings numerous benefits and numerous savings, however on the other hand numerous risks in the area of personal data protection, electronic commerce and infrastructure security.

How does the IoT sees our personal data better than previous devices

While obviously far more efficient than previous monitoring devices, the IoT based sensors present a tangible 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 the corridor of a residential building, on the 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).

Naturally, this 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 behavior through time, presenting a potential new risk for the data subjects.

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 behavior such as when the resident comes home from work or other functions, which is the optimal room temperature he or she prefers or even when energy intensive appliances such as ovens or vacuum cleaners are being used indicating his 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 was once a simple record of electricity consumption now representing a detailed record of personal life and habits.

IoT and GDPR

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 Law on Application of the General Data Protection Regulation, 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 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 the protection of personal data". (European Commission, 2016a).

Naturally, IoT products and services allow for collecting large volume of data, some of which may be of potentially very 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 automatically orders detergents) is concerned, 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. Most IoT devices have a physical aspect, which requires us to consider physical safety regarding the device as well as the user and the environment that is deployed in. This integration between cyber-security and physical safety raises the need for new thinking and 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, the regular smart home ecosystem is comprised of 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 2017, the European Commission produced a recommendation for 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 cell phone 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 the 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.

IoT and information security regulation

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 is 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, 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 – *Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga* (Official Gazette of Republic of Croatia, 2018).

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 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 (Official Gazette of Republic of Croatia, 2018, 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 (Official Gazette of Republic of Croatia, 2018, 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 (Official Gazette of Republic of Croatia, 2018, 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 (Official Gazette of Republic of Croatia, 2018, Article 16).

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.

According to telemetry collected from Bitdefender BOX units, 50% of printers have the weakest passwords in a smart home, but only 5% of IP cameras were found with weak passwords. NAS (Network attached storage) devices have better, more complex passwords, as only 0.2% were found vulnerable due to poor passwords. The weakest passwords were overall detected in phones (44.78%), printers (16.60%), and computers (10.32%), while stronger passwords were found securing prototyping platforms (7.97%), routers (1.79%), cameras (1.05%), NAS (0.83%), tablets (0.29%) and IoT devices (0.16%) (Främling, 2002).

Smart home appliances offer new venues for attack. An attacker can hack into the smart home system and unlock the door or turn on appliances such as fireplaces which then may lead to burglary or fire at the home of a victim. These new type of 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:

1. Risk to personal data and privacy: The Internet of Things represents taking the data collection, storage and analysis mechanisms to a greater scale. There are more and more devices connected to the Internet and there are also more elements that require protection: the device itself, the network, the application or the platform that it uses.
2. Technical vulnerabilities in authentication: The IoT works with devices of different nature that will be connected to the Internet and collect user data in the cloud through the tool itself. One task to do is to work in depth on the authentication mechanisms to ensure the privacy of the user.
3. Human factor: IoT is a relatively new technological advance. Ignorance of IoT security, both by companies and individual users, also increases the risks of cybersecurity due to lack of experience and the human factor.
4. Inadequate data encryption: the transmission of data by non-encrypted means presents a major security problem. Consider also the importance of network security, since the IoT is generally focused on mobile devices of various types and predominantly wireless networks.
5. 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 (Apiumhub, 2018).

We can conclude that IoT affects personal data and generally information about peoples' 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 makes security issues far more complicated, both legal and technological.

According to Bitdefender study, the top ten (10) most vulnerable devices in 2017 were: routers (59,45%), computers (9,48%), smart TVs (1,65%), cameras (2,92%), printers (8,70%) NAS (9,32%) etc. (Främling, 2002).

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, the one which will identify and fix device weaknesses that can emerge over time, perhaps through dated security software or operating systems for private homes. "*Users' right to data protection and right to privacy must be balanced in the design and governance of identification technologies in the IoT.*" (Wachter, 2018).

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.

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 and 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 there is now 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 home owners about potential security threats that may be possible when using these devices and services.

The complexity of smart home infrastructure may very well prove impossible to apply classical security solutions to smart devices such as smart TVs, connected home appliances, wearables, smart entertainment, or connected sensors of energy and water distribution services so integrated security approach, risk identification and treatment and accountable behaviour of data controllers and other service providers is of foremost importance.

As number of IoT and smart home device security incidents continues to rise, it is going to be 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. Apiumhub (2018), "IoT Security Issues and Risks", available at: https://apiumhub.com/tech-blog-barcelona/iot-security-issues/ (23 February 2019).
2. Ashton, K. (2019), "That internet of things thing", RFIDJournal, available at: https://www.rfidjournal.com/articles/view?4986 (25 June 2019).
3. 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).
4. 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.

5. 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).
6. 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) L 119/1.
7. 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 (NIS Directive), L 194/1 OJEU.
8. European Commission (N/A), "IoT Privacy, Data Protection, Information Security", available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753 (25 June 2019).
9. Evans, D. (2011), "The Internet of Things: How the next evolution of the internet is changing everything", White Paper, Cisco, available at:
10. Främling, K. (2002), "Tracking of material flow by an Internet-based product data management system", Tieke EDISTY magazine, No. 1, pp. 24-25.
11. Hung, M. (2017), "Leading to IoT", Gartner, available at: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf (25 February 2019). https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (25 June 2019).
12. Iskraemeco (2019), Manufacturer web page, available at: http://www.iskraemeco.com/files/5514/3982/5764/AM550.pdf (23 February 2019).
13. KPMG (2017), "Risk or Reward: What lurks within your IoT?", available at: https://assets.kpmg/content/dam/kpmg/pl/pdf/2018/02/pl-Raport-KPMG-Risk-or-reward-What-lurks-within-your-IoT.PDF (22 February 2019).
14. Meola, A. (2018), "What is the Internet of Things (IoT)? Meaning & Definition", available at: https://www.businessinsider.com/internet-of-things-definition (23 February 2019).
15. Ning, H. (2013), Unit and Ubiquitous Internet of Things, CRC Press, Boca Raton, FL, USA.
16. Official Gazette of Republic of Croatia (2018), Act on Cybersecurity of Essential Service Operators and Digital Service Providers – Zakon o kibernetičkoj sigurnosti operatera ključnih usluga i davatelja digitalnih usluga, Narodne novine (Official Gazette of Republic of Croatia) 64/2018.
17. 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).
18. Vongsingthong, S., Smanchat, S., A (2015), "Review of Data Management in Internet of Things", Asia-Pacific Journal of Science and Technology, Vol. 20, No. 2, pp. 215-240.
19. Wachter, S. (2018), "The GDPR and the Internet of Things: a three-step transparency model", Law, Innovation and Technology, Vol. 10, No. 2, pp. 266-294.
20. 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 (23 February 2019).

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 graduated from the Faculty of Law in 1996, and gained Master's degree in 2003, on the topic of Maritime Domain of the Republic of Croatia, while in 2006 he obtained his Ph.D. under the title of Legal Status of Inland Ports. Goran Vojković has more than twenty years of work experience in the civil service and privately owned companies, 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 today, for the second mandate, he is an external member of the Committee for Legislation of the Croatian Parliament. Also, he has a great experience working on the EU projects 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. He lives in Ivanić-Grad. The author can be contacted at **goran.vojkovic@gmail.com**.

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 writing her doctoral dissertation under the title: "Comparative Analysis of Concessions for Managing Airports – the Applicative Croatian Model". She has written few papers and articles in the field of Administrative Law, Transport 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. He is an Assistant Professor at the ICT Law Department of the Faculty of Law, University of Zagreb. Teaches undergraduate and graduate courses in Information Technology Law from Data Protection and Privacy in Electronic Communications, Internet Governance, Introduction to Information Security, to Electronic Media Law and Copyright in Information Society. Member of the Internet Society, Croatian Academy of Legal Science, Croatian Copyright Society, International Association of Privacy Professionals and Internet Governance Forum. Certified ISO 27001 and ISO 37000 lead auditor. From 2017 member of the Program Committee of the CARNet Users Conference. 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.**