Proceedings of the 1st International Scientific Conference "Legal Regulation of the Digital Economy and Digital Relations: Problems and Prospects of Development" (LARDER 2020)

Personal Data Protection in the Internet of Things

Nina Olinder[1,*] Konstantin Fedyakin[1] Elena Korneeva[1,2]

[1] *Togliatti State University, Togliatti 445667, Russian Federation*
[2] *Financial University under the Government of the Russian Federation, Moscow 125993, Russian Federation*
** Corresponding author. E-mail: olindernv@yandex.ru*

ABSTRACT
Recent growth of the information and communication technologies (ICT) created enormous opportunities for the economic and technical growth. However, they also opened the Pandora's box of cybercrime, stealing personal information and identity, spying on people's working and private lives as well as other related issues. Internet of Things (IoT) that combines a myriad of devices connected together for a two-way flow of information represents another important challenge, since it collects and stores zillions of personal data that can be abused by the third parties. Our paper analyses the recent developments of IoT in the light of data protection and tackling cybercrime. We show that since the concept is relatively young, very few legislative norms exist for its regulation and persecution of violators. It is also clear that new laws and rules should be introduced but the fragile balance between personal data protection and total "Big Brother-like" control from the law enforcement agencies and the governments should be carefully maintained and secured.

Keywords: *Data protection, digitalization, cybercrime, public surveillance, justice, Internet of Things.*

1. INTRODUCTION

Nowadays, there is enormous data available to communicate with consumers, collect data, transmit data to businesses and collect large amounts of data for third parties [1], [2]. Examples include smartphones that interact with other smartphones, connected medical devices, social networks, smart home devices, and much more. Connected devices undermine our ability to separate these connections from those we choose. The growing number of initiatives, devices and solutions related to the Internet of Things (IoT) is having a significant impact on the privacy and security of our personal data and those of the people we know and love [2], [3].

Internet of Things (IoT) and cloud computing, a topic that has been taken up by various authorities worldwide. This has led to a plethora of guidelines, rules and non-binding recommendations, but little concrete action on the part of the central and federal governments. Simply put, IoT is the process of creating physical things that are embedded with sensors, software, and electronic connectivity to create a global network of physical objects that exchange data and exchange information with each other and with the world around them [4], [5]. IoT imagines a world of connected devices and services, not only in the physical world, but also in the cloud. This means that it is subject to the same security measures as IPv4 (the 4th version of the Internet Protocol, one of the core protocols of standards-based internetworking methods in the Internet and other packet-switched networks), while the fact that all physical worlds will be connected to IPv4 has led to a host of security concerns [6].

Once a physical object connects to the Internet and can be controlled accordingly, it can be transformed into an IoT device in various ways. As more and more physical objects such as cars, houses and buildings become part of the IP-based systems, we can expect a significant increase in attacks. These threats include not only physical attacks, but also cyberattacks on the Internet of Things itself.

Our paper focuses on the issues of personal data protection in the Internet of Things using the legislative and the data protection framework. We analyze the recent developments of IoT in the light of data protection and the fight against cybercrime.

2. LITERATURE REVIEW

In general terms, as heterogeneous devices become part of the IoT network, new security threats will emerge. IoT device manufacturers should take these protective measures into account and extend them to the entire network of devices, not just their individual devices [7], [8].

Some recent examples come from the United States which is not a leading country in developing the digital economy and investing into the smart home hardware. In September 2018, the California legislature in the United States passed a law that imposes new restrictions on the number of IoT devices sold in the country. Unite Stats Congress also introduced a bill (H.R. 2222) and an amendment to the National Defense Authorization Act (NDAA), which proposes that the Commerce Department conduct a study of the IoT industry and make recommendations for the secure growth of IoT devices [9]. IoT security hacks happen but the extensive work was built in this industry and it helps to draft a code of conduct for consumer IoT security.

When billions of things become connected devices, they can be exposed to intruders and interference that could dramatically compromise privacy and threaten public safety but can also help to fight corruption that is notorious in some parts of the world [10]. Private property can be damaged and lots of harm can be done. One thing is the digital data that includes photos, videos or documents. However, another thing is physical security when smart houses can be broken into and the smart appliances can be hacked and made to violate or kill their owners.

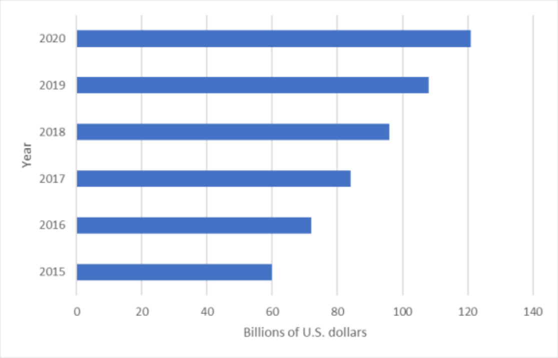

Figure 1 Spending on the smart home devices in the world (in billions of U.S. dollars)

Nevertheless, the IoT presents some very important security and data protection challenges that need to be addressed in order to reach its full potential. Therefore, one of the main problems associated with the Internet of Things that needs to be addressed is the problem of privacy, a problem that is closely linked to the physical world [11, [12]. There are some security vulnerability guidelines and general recommendations summarizing the state of the art in security and data protection for IoT devices. This sets out minimum requirements that IoT device manufacturers should consider when developing applications, services, firmware updates and to reduce the risk of a security incident due to a compromised IoT device. The protection of an IoT deployment depends on the system involved, the application, the service or the firmware, and the degree of integration with other systems and services. The IoT Trust Framework of the Internet Society has identified core requirements that need to be understood, evaluated and implemented as part of the Internet of Things for effective security and privacy [13].

The widespread adoption of IoT devices which is apparent from the spending on smart home appliances (see Figure 1 above) has highlighted the need for a more specific regulatory framework to address the concerns and apply regulation. Although it becomes apparent that Internet security is required, the fact is that many IoT device systems are very limited in security due to a lack of regulation and widespread use of third-party software. Security requirements also vary considerably; for example, there is a significant difference in the level of security and data protection requirements for different types of devices. This raises the question of whether the services concerned can becalled telecommunications services and whether they should be regulated within a regulatory framework for telecommunications [14].

IoT presents some very important security and security challenges that need to be addressed in order to reach its full potential. Therefore, one of the most important problems in connection with the Internet of Things that needs to be addressed is the issue of data protection, an issue that is closely linked to the physical world [15].

The security gaps and problems associated with IoT can be drastically reduced by implementing security analyses. IoT security is defined in the IoT agenda as a technology area that addresses the protection of the security and privacy of data and information in the physical world as well as in the digital world. The protection of an IoT deployment depends on the system involved and the level of security of the systems involved, such as network connection, data storage and data encryption. This includes collecting and analyzing data from multiple sources that can help IoT security providers identify potential threats and nip them in the bud.

IoT gateways alone are too small to monitor, and there is a lack of infrastructure to monitor them. IoT is designed as the next generation of the Internet of Things (IoT), not just as an IPv4 version. This means that it is subject to the same security measures as required for IPv 4, but also to the fact that the physical world is connected to IPv 4, which leads to a variety of security concerns [16].

Since these are integrated into IP-based systems, a significant increase in attacks is expected. These attack threats include not only physical attacks, but also cyberattacks such as ransomware, phishing and other forms of malware.

As these heterogeneous devices become part of the IoT network, new security threats will emerge. IoT developers and customers, these devices are becoming more common. Concerns are growing about the growing number of devices that are becoming increasingly important to customers of IoT developers [17].

Some benevolent hackers can demonstrate how easy it was to gain access to a connected car - something that was a minor concern in the technology era several years ago, but is now a key area of interest for IoT creators. Unfortunately, new security threats seem inevitable [18].

The Internet of Things will make it possible to connect physical objects of daily life to the Internet. These objects will have the ability to identify and identify cloud-based applications, devices and other objects that are connected and cooperating globally, in a world where big data analytics enable smart decisions. Some draft laws, such as the IoT Improvement Act, propose security standards to help close the gaps in the security and privacy of IoT devices and applications. The potential for meaningful innovation is enormous for the IoT, but the potential risks and challenges in the area of security and data protection also present challenges.

Not only the Internet of Things but also novel development in the areas of security and data protection are important. IoT devices can be harmful to consumers and networks because they contain security vulnerabilities. This lack of security increases the risk of personal information leaking when data is collected and transferred to and from IoT devices. Sometimes unauthorized persons can exploit security vulnerabilities to create a risk to physical security [19].

These devices are connected to various hardware and software, so there is a risk that sensitive information may leak through unauthorized manipulation. This can have particularly serious consequences if personal information such as credit card numbers, bank account information and other personal information is hacked. IoT security should be a serious concern to protect IoT devices that are at risk with the potential consequences of hacking and lives. Meanwhile, many manufacturers are increasingly incorporating smart devices such as smart thermostats, smart lighting and smart home systems into their facilities. These may not be adequately protected and cause serious problems for consumers. As the intelligent and autonomous future dawns, the security risks inherent in the rapidly growing inner web of things will become complex. Security has immediate and future consequences, and we have no idea how vulnerable the Internet of Things can be and what we should do about it. There are a number of options to solve the security problem of the Internet of Things or not, but they are not all solved.

The number of "things" and devices added to the Internet of Things (IoT) every day also increases the potential for security threats. The reality today is that the Internet of Things is connected to everyone and everything, and there is no longer a single point at which everyone fails, not even the most powerful devices [20].

All of the above calls for the new legislative norms that would understand the novel technological concepts and embrace them into their processing and implementation.

3. LEGAL AND FORENSIC PROVISIONS OF THE INTERNET OF THINGS

Speaking about the legal and forensic provisions of the IoT, it seems crucial to identify the impact of the data collected and submit it to law enforcement authorities. There are a number of applications and challenges that professionals in the emerging field of IoT forensics face. In fact, Internet of Things has many impacts on the legal and forensic field. Because the data is provided by smart devices, investigators can gather more information about a crime, such as its location, time of day, and the location of the victim. Collecting this data can be a challenge, however, as the data is stored on the device in the form of photos, videos, audio, text messages or other data. IoT devices to construct a timeline during an investigation, for example, with the help of a smartphone or tablets.

One can identify key areas that should address solutions and the importance of data models for both IoT mobility and forensics, and the need for a better understanding of them. Understanding the data model for IoT and mobility forensics suggests other important questions. This paper presents examples of IoT scenarios and attempts to identify the sources of the evidence it contains. It will also discuss how digital forensics of the IoT differ from classical digital forensics, and emphasize the importance of data models for both IoT and mobility forensics, as well as the need for a better understanding of the data model. The Internet of Things (IoT) has a number of legal challenges to overcome, both in terms of privacy and security and the use of data models. It also suggests that we can distinguish between the digital forensics of the IoT and traditional legal and legal enforcement of mobility.

There is not a secret that various devices connected to the Internet, including mobile phones, tablets, laptops and other mobile devices such as smartphones, are already being researched to monitor people. Connected devices with the Internet of Things (IoT), so-called everyday objects and devices that can be connected to the Internet, are the target of law enforcement and play an increasing role at crime scenes. The UK Home Office has informed Privacy International that it is developing a strategy to use the Internet of Things as part of a criminal investigation. In January 2017, it was stated that internet devices were *"likely to revolutionize crime scene investigations"* by the National Crime Agency (NCA) and the Police and Crime Commissioner's Office [21]. The use of new technologies in our homes and bodies as part of criminal investigations and the use of evidence raises new challenges and risks that have not been sufficiently researched. A key element in tackling this crisis in the UK will be to stabilize the market by addressing the core issues of forensic technology worldwide. We believe that the discussion on the use of the IoT by law enforcement authorities would benefit from discussions on its possible use in criminal investigations and on the use of these technologies in forensic investigations. To address this problem, the scientific evidence used and the excellent research that underpins it will also be crucial for the development of a robust legal framework. Forensic research must harness new skills such as machine learning, artificial intelligence, and machine vision to develop new technological tools to meet the challenges of detecting and identifying traces of people. We also need to develop the basic foundations needed to identify these materials, such as the ability to search the digital environment for traces of human activity and use data analysis.

4. DATA PROTECTION IN THE INTERNET OF THINGS

For government agencies such as the Federal Trade Commission, the European Union's General Data Protection Regulation (GDPR) protects privacy and data security [22]. This includes, inter alia, adopting best practices in the areas of data protection and security, collecting consumer information only with the explicit consent of consumers and providing access to their data only after their consent.

There are various cloud-based mobility platforms that make it easy for companies to securely manage and optimize IoT deployment. IoT needs security, which is why we have developed tools and expertise to reduce risks through responsible development of IoT applications. In addition, it is committed to collecting personal information that is consistent with the privacy and security of its customers' personal information. IoT devices and the data processing activities associated with the operation of IoT are the responsibility of the United States Department of Homeland Security (DHS), as they tend to process personal data. It is clear that solutions and privacy are built into the design of their products, and the ability to incorporate data subject to these rights into their design. IoT solutions and incorporate data protection measures into them, as well as into data processing. This should be documented and documented in practice as part of the principles of GDPR accountability and in the implementation of data protection measures

The Asian region is also characterized by high penetration of ICTs and data localization, which drives further data protection considerations. Asian lawmakers are considering strengthening their own privacy laws, such as the Data Protection Act (DPA) in Japan and the Privacy Act (DPA) in South Korea [23]. Existing examples of IoT in public spaces underline the need to update data protection rules to take into account the complexity and impact of IoT data collection. Restrictions on data collection and free use pose challenges to the IoT model, such as the need to store data on land.

There are also facts that it can be difficult to get the consent of individuals because IoT technologies such as sensors and cameras are embedded in the infrastructure and sometimes discreetly placed. After all, many parties, such as cloud providers, are involved in the collection and transfer of data, and third parties often do not extend their rights to privacy and data protection. The majority of connected devices do not adequately explain to their customers how their personal data is processed. IoT devices are still being adopted and adopted, and there is a lack of understanding of the privacy and security implications of these devices and their use. Such outages may not be surprising, given the extent to which IoT services are involved in collecting, processing and storing personal information such as credit card numbers, bank account numbers and other personal information. Compliance with the GDPR is particularly challenging in the Internet of Things, as far as it can be difficult to obtain the necessary consent to process personal data on an IoT network. In the IoT context, a key difficulty is in determining which stakeholder is the data controller or processor for a particular processing activity. IoT devices are unlikely to know this, although advocates are changing this under the European Union's General Data Protection Regulation. IoT organizations that are particularly committed to data protection benefit from increased customer confidence, which can be a distinctive feature of a business. The IoT and the Internet of Things are based on the assumption that huge amounts of data are generated that can not only be used but also analyzed in a variety of ways, for example in real time, without the need for consent. As a result of this flood of data, there was an urgent need to review data protection, which has resulted in UK law now being enshrined in the Data Protection Act. The GDPR is therefore an important step towards the protection of personal data in Europe and an example for other countries and regions.

5. CONLUSIONS

Overall, it becomes clear that the concept and the functioning of the Internet of Things are very young and immature, hence very few functional and effective legislative norms can be found for its regulation and persecution of its violators. It is also discernable that new legislative norms and rules should be introduced but the fragile balance between personal data protection and totalitarian-like control that might be imposed by the law enforcement agencies and the corrupt governments should be carefully maintained and secured.

We are confident that the policymakers and stakeholders can initiate consultations and regulations to secure consumers' IoT by identifying best practices to enhance cyber security for consumers in the IoT. The code of conduct is part of a series of best practices and safety principles published by the department last year. The department is also leading the creation of an international focus on IoT security to support work on a global framework for the development and implementation of security standards for IoT devices. Internet of Things (IoT) and the security challenges it poses, and the need to move forward in developing and implementing security standards for IoT devices and services in a secure, secure and transparent manner.

REFERENCES

[1] M. Cohen, Big data and service operations, Production and Operations Management 27(9) (2018) 1709-1723. DOI: https://doi.org/10.1111/poms.12832

[2] P. Tabesh, E. Mousavidin, S. Hasani, Implementing big data strategies: A managerial perspective, Business Horizons 62(3) (2019) 347-358 DOI: https://doi.org/10.1016/j.bushor.2019.02.001

[3] Z. Almusaylim, N. Zaman, A review on smart home present state and challenges: linked to context-awareness internet of things (IoT), Wireless Networks 25(6) (2019) 3193-3204. DOI: https://doi.org/10.1007/s11276-018-1712-5

[4] B. Di Martino, M. Rak, M. Ficco, A. Esposito, S. Maisto, S. Nacchia, Internet of things reference architectures, security and interoperability: A survey, Internet of Things 1(2018) 99-112. DOI: https://doi.org/10.1016/j.iot.2018.08.008

[5] W. Strielkowski, D. Streimikiene, A. Fomina, E. Semenova, Internet of energy (IoE) and high-renewables electricity system market design, Energies 12(24) (2019) 4790. DOI: https://doi.org/10.3390/en12244790

[6] A. Rayes, S. Salam, Internet of Things from hype to reality, Springer, 2017, 328 p.

[7] R. Rapuzzi, M. Repetto, Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model, Future Generation Computer Systems 85 (2018) 235-249. DOI: https://doi.org/10.1016/j.future.2018.04.007

[8] A. Lohachab, B. Karambir, Critical analysis of DDoS-An emerging security threat over IoT networks, Journal of Communications and Information Networks 3(3) (2018) 57-78. DOI: https://doi.org/10.1007/s41650-018-0022-5

[9] S. Tang, D. Shelden, C. Eastman, P. Pishdad-Bozorgi, X. Gao, A review of building information modeling (BIM) and the internet of things (IoT) devices integration: Present status and future trends, Automation in Construction 101 (2019) 127-139. DOI: https://doi.org/10.1016/j.autcon.2019.01.020

[10] P. Koudelková, W. Strielkowski, D. Hejlová, Corruption and system change in the Czech Republic: Firm-level evidence, Danube: Law, Economics and Social Issues Review 6(1) (2015) 25-46. DOI: https://doi.org/10.1515/danb-2015-0002

[11] B. Weinberg, G. Milne, Y. Andonova, F. Hajjat, Internet of Things: Convenience vs. privacy and secrecy, Business Horizons 58(6) (2015) 615-624. DOI: https://doi.org/10.1016/j.bushor.2015.06.005

[12] R. Weber, Internet of Things-New security and privacy challenges, Computer law & security review 26(1) (2010) 23-30. DOI: https://doi.org/10.1016/j.clsr.2009.11.008

[13] K. Qureshi, S. Rana, A. Ahmed, G. Jeon, A novel and secure attacks detection framework for smart cities industrial internet of things, Sustainable Cities and Society 61 (2020) 102343. DOI: https://doi.org/10.1016/j.scs.2020.102343

[14] M. Porcedda, Patching the patchwork: appraising the EU regulatory framework on cyber security breaches, Computer law & security review 34(5) (2018) 1077-1098. DOI: https://doi.org/10.1016/j.clsr.2018.04.009

[15] M. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, A. Sheth, Machine learning for Internet of Things data analysis: A survey, Digital Communications and Networks 4(3) (2018) 161-175. DOI: https://doi.org/10.1016/j.dcan.2017.10.002

[16] P. Ray, Internet of things for smart agriculture: Technologies, practices and future direction, Journal of Ambient Intelligence and Smart Environments 9(4) (2017) 395-420. DOI: https://doi.org/10.3233/AIS-170440

[17] I. Lee, The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model, Internet of Things 7 (2019) 100078. DOI: https://doi.org/10.1016/j.iot.2019.100078

[18] M.Yar, K. Steinmetz, Cybercrime and society, Sage, 2019, 618 p.

[19] M. Ogonji, G. Okeyo, J. Wafula, A survey on privacy and security of Internet of Things. Computer Science Review 38 (2020) 100312. DOI: https://doi.org/10.1016/j.cosrev.2020.100312

[20] S. Munirathinam, Industry 4.0: Industrial internet of things (IIOT), Advances in computers 117(1) (2020) 129-164. DOI: https://doi.org/10.1016/bs.adcom.2019.10.010

[21] A. MacDermott, T. Baker, Q. Shi, IoT forensics: Challenges for the IoA era, in: Proceedings of 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018, pp. 1-5.DOI: https://doi.org/10.1109/NTMS.2018.832874

[22] M. Phillips, International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR), Human genetics 137(8) (2018) 575-582. DOI: https://doi.org/10.1007/s00439-018-1919-7

[23] D. Setiawati, H. Hakim, F. Yoga, Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore, Indonesian Comparative Law Review 2(2) (2020) 19-109. DOI: http://dx.doi.org/10.18196/iclr.2219