Hindawi
Mobile Information Systems
Volume 2018, Article ID 6792028, 6 pages
https://doi.org/10.1155/2018/6792028

Research Article

An Analysis of Economic Impact on IoT Industry under GDPR

Junwoo Seo,[1] **Kyoungmin Kim**,[1] **Mookyu Park**,[2] **Moosung Park**,[3] **and Kyungho Lee**[2]

[1]*Department of Cyber Defense (CYDF), Korea University, Seoul, Republic of Korea*
[2]*Center for Information Security Technologies (CIST), Korea University, Seoul, Republic of Korea*
[3]*Agency for Defense Development, Seoul, Republic of Korea*

Correspondence should be addressed to Kyungho Lee; kevinlee@korea.ac.kr

Received 19 January 2018; Revised 9 April 2018; Accepted 15 May 2018; Published 5 December 2018

Academic Editor: Jeongyeup Paek

The EU GDPR comes into effect on May 25, 2018. Under this regulation, stronger legislation than the existing directive can be enforced. The IoT industry, especially among various industries, is expected to be heavily influenced by GDPR since it uses diverse and vast amounts of personal information. This paper first analyzes how the IoT industry handles personal information and summarizes why it is affected by GDPR. The paper then uses the cost definition of Gordon and Loeb model to estimate how GDPR affects the cost of IoT firms qualitatively and uses the statistical and legal bases to estimate quantitatively. From a qualitative point of view, GDPR impacted the preventative cost and legal cost of the Gordon and Loeb model. Quantitative view showed that the cost of IoT firms after GDPR could increase by three to four times on average and by 18 times if the most. The study finally can be applied to situational awareness of the economic impact on the certain industry.

1. Introduction

On April 14, 2016, the European parliament passed the General Data Protection Regulation (GDPR). This regulation strengthens the privacy rights of information entities and ensures that personal information is freely transferred among EU member states. European citizens are expected to control their personal information and create a high level of privacy protection in the European Union. With the introduction of GDPR, companies dealing with personal information are expected to be heavily influenced. Amidst a variety of industries, this paper focuses on the IoT industry, which collects and analyzes vast amounts of information from users.

The IoT industry is used in a variety of areas such as automotive, security and surveillance, medical, smart home, and T2T wireless networks. According to Gartner, there will be 11.2 billion Internet of "things" by 2018 [1]. This means that each of the "things" stores, reprocesses, and distributes more than 50 billion personal information. Statista, however, issued statistical data that 39% of European consumers completely denied that they were given sufficient information about personal information collected by IoT manufacturers [2]. According to this status quo, the IoT industry, which significantly transfers control of information use to individuals, is expected to be heavily influenced by GDPR and it is important to raise awareness of the situation of the economic impact on the certain industry.

This paper is an updated and revised version of previous study [3]. Section 2, which is a background of this paper, presents the characteristics of GDPR and security and privacy issues of IoT. Section 3 analyzes how IoT handles personal information, and Section 4 examines why GDPR affects the IoT industry. Section 5 analyzes the firms cost under GDPR to determine the economic impact of the IoT industry through the Gordon and Loeb model. Section 6 introduces related studies on the economic impact of GDPR and compare it with the paper. Finally, the conclusions are described in Section 7.

2. Background

This section first describes how the GDPR differs from the existing Directive. As a result, one can know which industries violate the regulation. Moreover, it describes the

security issues of the IoT industry that is strongly relevant to GDPR.

2.1. General Data Protection Regulation. Basically, the EU legislation is divided into Directive and Regulations. While the Directive provides concrete results to be achieved, each member state has discretion over the transition to the national standard of the Directive. On the other hand, Regulations are legally binding on all member states and takes effect on the date set by all member states [4]. As a result of GDPR, Data Protection Directive 1995 (95/46/EC), which protects personal information in 1995, will be replaced. The following are key elements to discriminate between GDPR and Directive.

First, the definition of personal information has been further expanded [4]. According to Article 4 of GDPR, personal information is all information related to identified or identifiable information subjects. Location information, online identifiers, and genetic information that were not included in the definition of Data Protection Directive 1995 were included.

Second, there will be a two-tiered sanction regime on penalties [4]. Violations of the GDPR, which is considered a small-scale case, could result in a fine of either 10 million or 2% of a firm's global turnover (whichever is greater). The most serious violations may result in a fine of either 20 million or 4% of a firm's global turnover (whichever is greater). This is the maximum penalty that can be imposed for the most serious violation, such as if the customer's data processing consent is insufficient or if the design concept of the firm violates the core of personal information.

Third, the consent, requirement of the GDPR, is reinforced beyond the Directive [4]. If consent is required, clear and specific information should be provided, and a simple and easy language should be used. The subject also has the right to withdraw consent at any time.

2.2. IoT Security Issues. IoT has become an increasingly attractive target for global hackers. Recent studies have categorized and described various security issues that arise in IoT environments which have heterogeneity and large scale of objects. Zhi-Kai Zhang et al. categorized these issues into identification, authentication, lightweight cryptosystem, and software vulnerability analysis [5].

These technical security issues are a threat to IoT devices that contain private information. Even if these various vulnerabilities occur, the most important thing is the security update problem. According to HP News, one IoT device has an average of 25 vulnerabilities [6]. There have also been many studies that have confirmed that IoT devices have vulnerabilities exposed to attackers [7–9]. As mentioned earlier, the number of IoT devices will be over a billion, and of course, the number of vulnerabilities will be the much huge amount. Since there are security updates on various devices, users are inevitably overwhelmed with the update. This causes 1-day vulnerabilities to be steadily generated, and various hacking incidents are likely to occur. Even if the firm provides automated updates, they often stop when they focus on constructing the next device, leaving customers with slightly outdated hardware that can become a security risk.

Under these circumstances, various studies are underway to solve the security issue of IoT environment. Ping Zhang et al. investigated the potential privacy risk of mobile Internet users and proposed an extensible system based on a public cloud service to hide the mobile user's network location and the traffic of the other party [10]. Bugra Gedik and Ling Liu recognized that privacy-aware management of location information is a very important task in the widespread deployment of location-based services [11]. They used a flexible privacy personalization framework to support location anonymity for a wide range of mobile clients with context-sensitive privacy requirements. Tianyi Song et al. found that smart home inevitably causes security and privacy problems [12]. They propose an improved stability and privacy protection communication protocol for smart home systems. In the proposed scheme, data transmissions within smart home systems are protected by a symmetric encryption scheme with secret keys generated by a chaotic system.

2.3. IoT Privacy Issues. This section describes what privacy issues are in the IoT. The following sections describe how IoT handles personal information specifically, but this chapter explains the rough privacy issues occurred in IoT environment. Due to the close correlation between personal physical characteristics and status, the adoption of cyber-physical-social systems (CPSSs) has inevitably been challenged by users' privacy concerns [13]. The first step is about collecting data. In the case of the Internet, information about user behavior is collected while surfing the Internet. IoT will analyze not only search history but also the individual user's various life patterns. Thus, more diverse and sensitive information can be collected. There are also data collection policies for each IoT device, including the access control policies of each "things" and the types of data. This may conflict with the articles of the GDPR in establishing control policies.

In addition, the digital forgetting process that requires the deletion of personal information may be difficult [14]. One of the processes of processing personal information is that the current trend allows people the right to forget. If an individual requests to delete information, it is difficult to completely delete it technically because it has so many diverse and massive amounts of personal information in the IoT situation, and it is necessary to revise the information held by the company.

3. How IoT Handles Personal Information

This section analyzes how the IoT industry handles personal information and shows that the industry is under GDPR. The following subsections describe the personal information usage features of IoT devices that may conflict with the GDPR.

3.1. Usage and Exchange Information between IoT Devices. Each endpoint in the IoT environment, the "things", automatically transmits data, communicates with other endpoints, and works together. In IoT, "things" occasionally trade and operate on behalf of the user. For example, if a smart refrigerator perceives that food is scarce, it connects to the Internet and buys necessary items for the user. In this case, information utilization is automated and user information is exchanged to various subjects. GDPR, managing the use of personal information, can bring the result of diminishing advantages of IoT.

3.2. Analysis of Information Aggregated from IoT. Currently, IoT manufacturers are collecting huge amounts of information generated in IoT environments and research methods to analyze this huge amount of data to better understand the system and user behavior. To bring more value and revenue, IoT manufacturers analyze data that appear to be irrelevant and ascertain the relationship between a consumers behavioral and usage patterns. In other words, data delivered from one endpoint is less likely to cause a privacy issue, but data collected and aggregated at various endpoints can trigger privacy issues. Therefore, this aggregated information has a possibility to be included in the extended definition of the personal information to which the GDPR applies and corresponds to the personal information control domain.

For example, Vizio, electronic product development company, was recently fined $ 2.2 million for using content-aware software to track users pattern without consent. The company sold 11 million IoT TVs with a software program installed intentionally to track customers' detailed viewing habits. They linked the data to specific household statistics and sold that information to third-party marketers. Vizio insisted that they never paired TV data with personally identifiable information such as name or contact information. However, the data were collected as an analysis of personal TV habit information, so it is considered as sensitive information and a fine was imposed. If the GDPR is applied, the fine would have been $ 292 million, more than 100 times larger than the previous judgment [3].

4. Why the IoT Industry Is Affected by GDPR

This section analyzes the characteristics of IoT and the provisions of GDPR, which were introduced above, and explain why the IoT industry is strongly influenced by GDPR.

4.1. Consent. The personal information required in the IoT environment is not only sensitive information but also has enormous amounts. Although there is no privacy protection law specific to the IoT field, the Federal Trade Commission (FTC) is conducting policy discussions on security and privacy protection in the IoT environment [15]. The FTC provided comments on the concerns of privacy breaches of IoT devices and the direction of information protection activities related to IoT through the "Benefits, Challenges, and Potential Roles for the Government in Fostering the Advantage of the Internet of Things [16]."

In this statement, the FTC said that IoT devices that can collect, transmit, and share sensitive consumer information about their physical and lifestyle habits are dangerous when combined with information collected from other devices. Due to the characteristics of collection and sharing of personal information of IoT, there is a possibility of more difficulties in the consent process. In addition, when considering the sharing of personal information among T2T and the personal information utilization of companies, we can see that the consent is much difficult. According to the GDPR, there are conditions in which it is necessary to inform the purpose of collecting personal information in easy-to-understand terms and to simplify the consent process. By interfering with the consent process, consumers will be more hesitant to collect sensitive and diverse personal information, and these regulations will have a major economic impact.

4.2. Right to Compensation. Right to Compensation is an article that is directly related to all companies as well as IoT firms, but the reason why IoT industry has a big influence is that one attack vector can lead to various types of personal information leakage. From a business perspective, if the firm complies with the provisions of the GDPR, the firm can acquire rights to Right not to Compensate. However, IoT companies find it difficult to obtain these rights. There is a high probability that it will not be able to keep up with the security updates of a vast amount of devices, and the conditions for protecting the personal information that each device collects are much harder than for other industries' firms.

5. Situational Awareness for Measuring Economic Impact in IoT Industry under GDPR

This section analyzes the economic impact of the IoT industry. The paper uses the cost definition of the Gordon and Loeb model to estimate how GDPR affects the cost of IoT firms qualitatively and uses statistical and legal basis to estimate quantitatively.

According to the Gordon and Loeb model, the amount of damage can be calculated as follows: direct costs, indirect costs, explicit costs, and implicit costs [17]. First, the direct cost refers to damage cost that is directly caused by a specific infringement event. In other words, it is the amount of hardware or software lost due to an accident. On the other hand, indirect cost refers to prevention cost that is incurred to inhibit information security breaches. Furthermore, the explicit cost is the cost that is explicitly visible due to a specific infringement violation. The explicit cost includes a preinvestment cost to avoid damages and damage cost and a cost to recover damages caused by infringement. On the contrary, implicit cost does not include damage cost caused by an infringement, but the damage cost for situations that may arise thereafter. This involves, for example, the cost of

legal liability for an infringement event, including falling stock prices or reduced sales due to a declining reputation of the affected company. Using the Gordon and Loeb model, this paper analyzes and indicates the defined costs that are expected to alter due to GDPR.

According to Article 82 (Right to Compensation and Liability), any person who has suffered material or nonmaterial damage due to a violation of GDPR rules has the right to demand compensation for damages [4]. Especially, the Directive mentions only damages; however, GDPR can be compensated for pecuniary and nonpecuniary losses.

Article 83 explains the general conditions for imposing administrative fines, which are not automatically applied and are imposed on each individual case. Therefore, it is beyond the bounds of possibility to measure the fines accurately, due to characteristics of ones imposition and absence of judgment. However, by utilizing the definition of the Gordon and Loeb model, the paper presents the increment of certain cost elements. In this regard, the Article 82 and 83 result in an increase in the *legal cost* from the Gordon and Loeb model.

In addition, Articles 37, 38, and 39 describe the designation, status, and obligations of the Data Protection Officer (DPO), respectively. Controllers and processors must designate a DPO in following three cases: (1) public authorities, (2) large-scale regular and systematic monitoring of intelligence entities, and (3) large-scale processing of sensitive information or criminal records. Moreover, DPO should also have an in-depth understanding of GDPR and personal information processing tasks and expertise in national privacy laws. Since the designation of the DPOs is mandatory and their qualities must be proven, Articles 37, 38, and 39 will affect the *preventative cost*.

To sum up, GDPR affects two costs (legal cost and preventative cost) of the Gordon and Loeb model as written above. In order to analyze the economic impact of GDPR, the estimated cost of damages before and after GDPR should be compared. According to the Ponemon Institute, in 2016, the average number of breached records reached 24,089 [18]. Based on the research, the paper selects four average personal data breach cases to analyze the economic impact of the GDPR on the IoT industry.

Table 1 provides information on how much data breach has occurred and how much annual turnover the company has for each case. The paper firstly estimates how much four cases, regardless of GDPR, resulted in the cost loss of the firm. According to the Ponemon Institute, the average cost per data leakage (capita) of a data breach for the past four years is $150 [18]. The average cost per capita of a data breach includes both the direct and indirect costs incurred by the breach. Based on this research, estimates of the four cases' costs can be derived by multiplying the number of breached personal data by the average data breach cost per capita. In order to analyze how GDPR affects, the paper then examines the cost assuming GDPR application to the cases. As shown in Figure 1, two component costs of the Gordon and Loeb model that GDPR affects were derived, the legal cost and the preventative cost. The paper assumes that each violation of GDPR was considered to be a case of lesser infringement, due to an averageness of the cases, resulting in a fine 10 million or 2% of a firm's global turnover (whichever is greater). Taking into account each of these costs, Figure 2 shows how disastrous the prospective cost of a firm is.

Table 1: Four personal data breach cases in the IoT industry.

	Number of breached personal information	Annual turnover of a firm *EUR (millions)*
A	43,000	10.0
B	28,000	3,133.8
C	23,200	386.6
D	20,000	17.5

Unlike the rest of the cases where the cost of a firm increases three to four times, the cost of firm B is expected to increase by about 18.6 times because of the provisions of GDPR. GDPR determines fine based on the annual turnover of a firm for the previous year, which is based on total sales of the firm, not the sales of the single branch or corporation that violates the regulations. This is a measure to secure the punitive penalties by preventing bogus companies or affiliated companies from using the methods to circumvent regulations. Therefore, firms with large annual turnover can be fined well exceeding 10 million.

The economic impact of data breach incidents can be an important indicator of decision making. "Situational Awareness (SA)" is an essential concept in this decision-making process. SA means a process that recognizes the time and environmental factors that an event occurs and responds to future threats. This process is used as a framework to respond to threats such as disaster, financial, and cybersecurity. SA's representative framework is based on Endsley's model. Endsley's model consists of recognition of the elements of the environment within the volume of time and space, an understanding of the meaning, and a process of projecting the state in the near future conditions [19]. The economic impact of GDPR, which can arise from data breach incidents, can be projected from SA to future conditions and used to predict damage.

6. Related Works

There were several studies on the economic impact of GDPR. Hofheinz Paul and Michael Mande argued that the GDPR is a "regulatory wall" to expand privacy [20]. They said the GDPR will have a major impact on the opportunities for US companies which provide digital services in the EU. Several studies have concluded that GDPR would be detrimental not only for foreign companies but also for economies in Europe. Christensen Laurits et al. argue that the GDPR will raise the production costs of companies in the EU by 20%. This could result in a 0.3% employment decline and a 3% decline in the company [21]. Avi Goldfarb and Catherine E. Tucker said the GDPR could hurt the efficiency of digital advertising and hinder its ability to generate revenue through digital content [22]. This paper first explains why a specific industry, IoT, is affected by GDPR, and it is meaningful to measure the loss magnitude to measure the risk of IoT industry under GDPR.

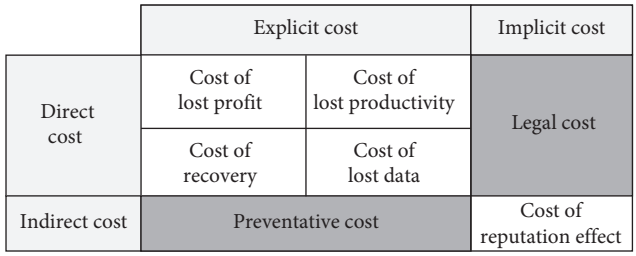

Figure 1: The Cost of Gordon and Loeb model that GDPR affects.

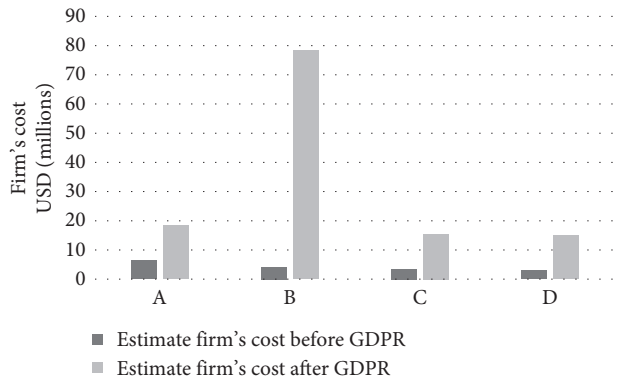

Figure 2: Comparison of estimate firm's cost before and after GDPR.

7. Conclusion

The impact of GDPR and its regulatory scope have heightened the tension of the firms. In this tension and concern, this paper first shows that by application of GDPR, the IoT industry is affected by GDPR in Sections 3 and 4. Section 5 uses the cost definition of the Gordon and Loeb model to estimate how GDPR affects the cost of IoT firms qualitatively and uses the statistical and legal bases to estimate quantitatively. Although there is a constraint to progress with limited data, the paper analyzes the economic impact of the certain industry from legal changes in two aspects (qualitative and quantitative), thus identifying industries that are vulnerable to legal changes.

The 2015 Icontrol State of the Smart Home study found that 44% of all Americans were "very concerned" about the possibility of their information getting stolen from their smart home and 27% were "somewhat concerned [23]." These public perceptions show the psychological concerns of people using IoT. In the presence of these concerns, the GDPR will add to the security of the user's personal information. However, companies will have to prepare and respond in order to find a way to fully utilize the IoT's functions under the GDPR.

Finally, situational awareness is an important step in the decision-making process. This study can be applied to situational awareness of the economic impact on the certain industry. Our next study is to develop the study to build an IoT risk management framework to anticipate and reduce risks based on the FAIR methodology, rather than simply measuring postaccident losses.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by Defense Acquisition Program Administration and Agency for Defense Development under the contract UD060048AD.

References

[1] R. van der Meulen, "Gartner says 8.4 billion connected things will be in use in 2017, up 31 percent from 2016," 2017, http://www.gartner.com/newsroom/id/3598917.

[2] Statista, "Level of agreement regarding internet of things (IoT) manufacturers sufficiently informing consumers about information the devices can collect in europe in 2016," 2016, https://www.statista.com/statistics/609021/trust-in-iot-device-manufacturers-eu/.

[3] J. Seo, K. Kim, M. Park, M. Park, and K. Lee, "An analysis of economic impact on IoT under GDPR," in *Proceedings of 2017 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 879–881, IEEE, Jeju Island, Korea, October 2017.

[4] C. of the European Union, "Regulation (EU) 2016/679 of the european parliament and of the council," 2016, http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

[5] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: ongoing challenges and research opportunities," in *Proceedings of 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications (SOCA)*, pp. 230–234, IEEE, Matsue, Japan, November 2014.

[6] K. Rawlinson, "Hp study reveals 70 percent of internet of things devices vulnerable to attack," 2014, http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WjJ_ld9l_BV.

[7] A. Costin, J. Zaddach, A. Francillon, D. Balzarotti, and S. Antipolis, "A large-scale analysis of the security of embedded firmwares," in *Proceedings of USENIX Security Symposium*, pp. 95–110, San Diego, CA, USA, August 2014.

[8] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Information fusion to defend intentional attack in internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 337–348, 2014.

[9] V. Sharma, K. Lee, S. Kwon et al., "A consensus framework for reliability and mitigation of zero-day attacks in IoT," *Security and Communication Networks*, vol. 2017, Article ID 4749085, 24 pages, 2017.

[10] P. Zhang, M. Durresi, and A. Durresi, "Enhanced internet mobility and privacy using public cloud," *Mobile Information Systems*, vol. 2017, Article ID 4725858, 11 pages, 2017.

[11] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: architecture and algorithms," *IEEE Transactions on Mobile Computing*, vol. 7, no. 1, pp. 1–18, 2008.

[12] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for IoT applications in

smart homes," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1844–1852, 2017.

[13] X. Zheng, Z. Cai, J. Yu, C. Wang, and Y. Li, "Follow but no track: privacy preserved profile publishing in cyber-physical social systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1868–1878, 2017.

[14] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: design challenges and opportunities," in *Proceedings of 2014 IEEE/ACM International Conference on Computer-Aided Design*, pp. 417–423, IEEE Press, San Jose, CA, USA, November 2014.

[15] FTC, *The Internet of Things: Privacy and Security in a Connected World*, FTC, Washington, DC, USA, 2015.

[16] R. Hagemann, "The benefits, challenges, and potential roles for the government in fostering the advancement of the internet of things," 2016.

[17] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 4, pp. 438–457, 2002.

[18] Ponemon Institute, *2017 Cost of Data Breach Study*, Ponemon Institute, Traverse City, MI, USA, 2017.

[19] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human Factors*, vol. 37, no. 1, pp. 32–64, 1995.

[20] P. Hofheinz and M. Mandel, "Bridging the data gap: how digital innovation can drive growth and create jobs," *Lisbon Council-Progressive Policy Institute Policy Brief*, vol. 15, 2014.

[21] L. Christensen, A. Colciago, F. Etro, and G. Rafert, *The impact of the data protection regulation in the EU*, Intertic Policy Paper, Intertic, USA, 2013.

[22] A. Goldfarb and C. E. Tucker, "Privacy regulation and online advertising," *Management Science*, vol. 57, no. 1, pp. 57–71, 2011.

[23] Icontrol Networks, *Icontrol State of the Smart Home Report*, Icontrol Networks, Austin, TX, USA, 2015.