Advances in Social Science, Education and Humanities Research, volume 615
Proceedings of the 2021 4th International Conference on Humanities Education and Social Sciences (ICHESS 2021)

Host States Should Maintain a Balance Between the Protection of Domestic Data and Attracting Multinational Enterprises

Xinji Jin[1, a, †, *] Chunhui Li[3, c, †, *] Ze Yu[2, b, †, *]

[1] *School of Law, Shanghai Maritime University, Shanghai, China*
[2] *NOIC ACADEMY, Toronto, Canada*
[3] *Harbin No.3 High School, Harbin, China*
[*]*Corresponding author. Email: [a]201810931147@stu.shmtu.edu.cn, [b]info@neworientalgroup.org,*

[c]*zangyonghhui@hrb3z.org*

[†]*These authors contributed equally.*

ABSTRACT
As one of the most currently important commercial entities, multinational enterprises have great impacts on both host states and home states in almost every industry, such as energy, telecommunications, and manufacturing industry. This work aims to review the state-of-the-art balance for host states to maintain between protection of domestic data and attracting multinational enterprises by comparing the host states' regulations in the new field of data processing and conventional industries. However, there exists some legislation that has aroused some disputes. This article presents some thoughts to problems that host states may have encountered and focused on the General Data Protection Regulation to solve these problems. Some suggestions are finally given with clear justifications.

Keywords: *Multinational Enterprises, Data Protection, Host State Regulations.*

1. INTRODUCTION

We are in a flourishing information age, where data processing is the core of everything. The importance of data has beyond all doubt been a basic human right, yet many states are ignoring legislation on data protection, whether by accident or design. This has given multinational enterprises opportunities to enter the states with simple and crude legislation on data protection and infringe the data to make profits. For example, Tiktok was found violating personal privacy in America. Data protection is essential to national security as some confidential information becomes more fragile with modern technology. In that case, the host states have to enforce regulations on foreign investors, especially multinational enterprises' data action. However, to seek the opportunities to develop the digital economy and boost innovation, the power of host states on data regulation needs to be limited; otherwise, it will practically cause damages to itself. To further explore the acceptable and reasonable legislation mode, this essay will analyze the latest and most stringent legislation on data protection in the European Union, General Data Protection Regulation, in the hope of setting an example for other states and making improvements on the regulation itself.

2. LITERATURE REVIEW

Data has become a vital piece of infrastructure in the Internet age, and it can even make the difference between life and death for a business. For multinational enterprises, the importance of data protection extends even to national security. But at the same time, the electrification of data, people's pursuit of high efficiency, and so on bring new challenges to safety management. This is like a gamble. Many enterprises in daily security awareness are not strong enough, but the consequences are often very serious once the core data leak. Because of this game state of data security, the development of the whole industry is usually driven by security events. This paper analyzes the difficulties faced by multinational corporations in data protection and puts forward some measures for them.

The data privacy protection of minors can be traced back to the personal information privacy protection of minors. In 1974, the Family Educational Rights and Privacy Act provided Privacy protection for minors. Currently, many countries have implemented special protections for minors' data privacy such as GDPR, COPPA, "UN Convention on the Rights of the Child", and so on. Many countries have clear definitions of the age of minors. Also, some countries set the digital age to protect minors' data. Most of them are 13 years old. However, the United Nations has paid less effort to protect children's data privacy in recent years. Therefore, to make children's data protection more effective, international organizations should play a greater role in this field.

The European Union established a rigid regime on data protection for its residents through a series of legislation. The General Data Protection Regulation (GDPR) is the latest and most strict, thus arousing some criticism. Layton stated before the Senate Judiciary Committee the 10 problems of the GDPR [1]. Bergkamp questioned the desirability and necessity of the EU data protection regime and examined the "other side" of data protection law and identifies its paradoxical and adverse effects [2]. However, these views are theoretical assumptions without evidence. The research used the Differences-in-Differences model based on data from Crunchbase seemed to have confirmed some of these assumptions of GDPR's effects on the EU economy [3]. On the contrary, another empirical research focused on the data from online advertising intermediaries suggested that the increasing value of remaining customers offset the drop of lost customers. There was no significant difference in advertisement revenue [4]. This essay will be based on the assumptions and empirical researches to analyze the effects of GDPR on the EU and world economy and gave some solutions.

3. MULTINATIONAL ENTERPRISES POSE A THREAT TO THE DATA SECURITY OF THE HOST STATE

3.1. The importance of data

Since the Council of Europe issued the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) which was the first legally binding international treaty concerning privacy and personal data in 1981, the dualistic structure of the protection of privacy and personal information has been established in Europe. As far as the treaty's legislative aspects, there are two different conceptions. First of all, the objects of right are distinct. Personal data contains all of the information related to someone, yet the private one can be classified as privacy. Secondly, the subjects of right are different. A legal person can be a subject of the right to privacy. Nonetheless, it is ruled out of Convention 108, Directive 95/46/EC on the protection of individuals concerning the processing of personal data and the free movement of such data (Directive 95) and General Data Protection Regulation (GDPR). However, due to the inherent connection between privacy and personal data, the overlap between the two is inevitable, and courts have found it hard to distinguish them in practice. For example, in M.M. v. the United Kingdom, the court reiterated that both the storing of information relating to an individual's private life and the release of such information come within the scope of Article 8 §1. In this case, personal data hereinafter is going to be the overlaps with privacy.

In the internet era, applications in computers and mobile phones are growing, which means that personal and corporate data are exposed to the network provider. Collecting users' data has become easier, cheaper, and easier to exploit. The complexity of the Internet also makes data's privacy and security more vulnerable to infringement. Once personal data is exposed to the internet, information containing personal information, such as home address and telephone number, will put individuals in danger. Personal reputations and property will be at risk. Also, once the corporate body's data is breached, the enterprise will face serious loss of reputation and property. For the country, such data breaches can implicate national security concerns when that data contains sensitive information whose exposure could create dangerous situations [5].

3.2. Multinational enterprises existing damages to underage's behavioural data

The definition of minors is different in different countries. In the United States, people under the age of 18 are regarded as minors. In Japan, a minor is defined as people under the age of 20. However, they all have data issues on the internet. When people register for a website or an application, users have to submit specific information such as names, ages, email addresses, phone numbers, and so on to the application, which means that many users' private information about themselves will be exposed to the Internet. Most adults are wary of such data collection actions from apps and websites. In contrast, children， especially under the age of 13 that Children's Online Privacy Protection Act of 1998 (COPPA) stipulated "digital age" showed no protection against such information. On account of that children are passive social groups, they have less experience in society than adults. In addition, children's values, which determine their susceptibility to the external environment, are not fully formed. They are unable to identify what is positive or negative. As they enjoy the internet services from multinational enterprises, they would not pay attention to whether the information they hand over is private and important. They can't distinguish what is private and whether it is beneficial to give it to the enterprises

without parents' supervision. It is a potentially dangerous act for minors to provide their private information online because it is likely to affect the physical and mental safety.

Another way to get information about underages is when they are using an app. The Internet records information posted by them while using an app, such as comments, preferences, and interactions with others. This information for children is very likely to be violated on the factors. For multinational enterprises, data of children in a country contains an extremely high value. Children are decisive to host the state's future preference and market. Powerful multinational enterprises are fully capable of inducing value orientation of host state's children if multinational enterprises obtain children's data for a country, which will bring multinational enterprises numerous profits. On the other hand, from the global perspective, multinational enterprise applications have a wide geographical range, which means they have more users. This factor will also lead to the undesirable condition that the personal information of underage users is more likely to be infringed.

TikTok is an international short video app in which users can post their pictures and videos on the application platform to the public. All users of the application can see the open information and communicate with the publisher. In addition, each user has a detailed profile, including name, phone number, belief/religion, and so on. All the information is outlined, which gives people opportunities to access others' private information. For adults, this information is more often used to let people using the app get to know each other. Nevertheless, for children, this information can lead to a lot of safety concerns. Tiktok was also accused that by using the biological identify mechanism, Tiktok could collect the appearance of children. Tiktok collected 13-year-old children's information without parents' supervision. As a result, TikTok agreed to settle for $5.7 million for violating U.S. children's privacy laws and will impact how the app works for kids under the age of 13 [6]. In an app update being released today, all users will need to verify their age. The under 13-year-olds will then be directed to a separate, more restricted in-app experience that protects their personal information and prevents them from publishing videos TikTok. America considers children's privacy as a priority, and American legislation on the privacy of children's data is rigorous. COPPA is a great example of America valuing children's privacy that is tailored to protect children's online privacy. COPPA sets out several new rules to protect children, including digital age and self-regulation. "The digital age for children is limited to 13, and in its revision, the FTC is considering expanding the definition of a child to include children between the ages of 13 and 17. Providing mechanisms for self-management [7]. The COPPA framework provides incentives for industry self-regulation through the Safe Harbor Program." Furthermore, in 2020, TikTok has faced scrutiny again because it was accused of misusing and handling the private information of a 12-year-old girl in London, which means TikTok still poses a threat to the host state's under-ages data security. In addition, we could also reference the legislation on children's privacy in European and American countries, Including General Data Protection Regulation (GDPR).

3.3. Multinational enterprises potential damages to national security

With the advent of the era of big data, data is undoubtedly an important asset for enterprises and individuals, and the boundary of data security and privacy is becoming more and more important. But when it comes to data security, both the Internet giant Facebook and the US credit service Equifax have been exposed to user data breaches. Therefore, countries have to deepen the understanding of big data security, including the United States, the United Kingdom, the European Union, and China have begun to formulate laws and regulations related to big data security. The fact that big data security is threatened and loose is causing such a stir because data permeates every aspect of life in this day and age. Similarly, data security has infiltrated every aspect of national security. National security is defined as political, economic, military, and other aspects of security. In the current era of big data, any security aspect cannot be separated from data security. Data security refers to ensuring the effective protection and legal use of data by taking necessary measures and keeping the data in a safe state continuously. Unlike network security, the core of data security is to ensure the security and legal and orderly flow of data. At present, as a new factor of production, data is profoundly affecting the development of the national economy and society. The ability to guarantee data security is a direct reflection of a country's competitiveness. It is an important issue to promote the healthy development of the digital economy and improve the country's governance capacity and an important aspect of national security. As a large unit that grasps the information of various countries to different degrees, multinational corporations have different degrees of mastering various data and information of host countries according to their own business and dabble in different directions. But as long as there is data related to the host country, data security and even other aspects must be taken seriously. For example, as a new technology emerging in recent years, intelligent vehicles developed by many multinational companies lack practical measures to effectively regulate them. At present, the security supervision of the Internet of Vehicles is prominent, and there is a lack of data security guarantee and management mechanism. How to ensure the security of the owner's information and privacy, avoid virus attack and malicious damage, and prevent the loss or misappropriation of personal information, business

information, and property will be a major topic that needs to be broken through the development process. It involves far more than its field. By collecting map data, intelligent vehicles can obtain the travel data of people in a region. The data of human flow plays an important role in national security and defense. The purposeful leakage of data will directly threaten the safety of a region. Therefore, it can be seen that data security is the basic guarantee for the normal operation of each link. At the same time, multinational corporations have numerous and complex data and involve a wide range of aspects. Therefore, the data management of multinational corporations is a test for the control of the host country and a potential risk.

4. THE OBLIGATIONS OF HOST STATE TO REGULATE MULTINATIONAL ENTERPRISES' DATA ACTIONS

4.1. General sources of host states' obligation to regulate multinational enterprises

Before seeking methods to regulate multinational enterprises, the definitions of host states and home countries need to be made clear. Host states are the countries that would like to attract investment of multinational enterprises. Home countries are the characters that would like to gain profits by investing money to host states. They have different goals, but both of them want to obtain benefits from each other. However, despite that host states would like to attract multinational enterprises' investment, they still want to prevent damage that inward FDI may bring [8]. Inward FDI means foreign direct investment to one's own country. Excessive inward FDI may lead to tremendous management rights of multinational enterprises over some industries or even complete control of these industries. Currently, home states are more willing to invest in host states and protect their corporations. Therefore, the host states have to adopt a number of preventive strategies, such as banning multinational enterprises from entering national cultural industries that are particularly essential and sensitive in a country. If this industry is monopolized, a country is likely to lose its cultural heritage and characteristics. This can lead to the loss of the material and spiritual property of a country.

When it comes to regulating multinational enterprises, there are several sources. Initially, there are some non-binding measures mainly given function by moral force. These include codes of conduct developed by individual companies or industry sectors, NGO codes, codes drawn up by governments, or IGOs. The codes of conduct developed by the International Labor Organization (ILO) are of especial importance. It seems that they have little effect when it comes to enforcement. Nevertheless, they actually could obtain legal force in private law [9]. The evaluation of an enterprise, including products, reputation, and so on, will make multinational enterprises have to pay attention to non-binding measures, which means these voluntary codes are becoming more crucial and effective than before. Besides, there are several "regulating sites" that should be mentioned. For instance, self-regulation, national regulation, bilateral regulation, and so on. Self-Regulation means multinational enterprises create their system to regulate themselves. More individuals gradually maintain this method in society. National Regulation is the most significant measure to regulate multinational enterprises. In some situations, national legal jurisdiction is ineffective to multinational enterprises because multinational enterprises are not restricted by ordinary national law. What this means is that host states should prescribe laws that are specifically for multinational enterprises.

Also, host states should identify and impose legal duties to parents and subsidiaries of multinational enterprises.

4.2. Host states obligations in conventional fields

In conventional fields, what the host states have been done to regulate the multinational enterprises is remarkable. Some industries with high energy consumption, high pollution, and high water consumption are gradually inclined to transferring to host states. A number of developing countries, as host countries, are having severe environmental problems because some host states value benefits brought by multinational enterprises and the lack of public awareness of environmental protection. One of the characteristics of environmental problems is that it takes a great cost and long-paying recovery after being destroyed. Therefore, most host states will set up special access mechanisms for multinational enterprises on environmental issues. Host states will assess such environmentally unfriendly multinational enterprises when they enter the country. Also, the host states will assess the procedure that has environmental risks to enterprises before attracting multinational enterprises to their own countries. Another behavior that host countries need to prevent from multinational enterprises is a monopoly. Host states would prevent multinational enterprises from monopolizing the emerging industries in the domestic industry by prohibiting multinational enterprises from entering the relevant industries in the country. The country will also enrich the content of the anti-monopoly law. Additionally, monopoly leads to the unicity of consumers' purchases, which infringes consumers' right to choose products. Therefore, the host country will also prioritize the protection of consumers' interests to prevent monopoly.

4.3. Stronger obligations of multinational enterprises in data protection

On the importance of data security, data protection and security are important aspects of national security, data and the country's economic operation, and social governance. Public services, national defense, and security are closely related. The leakage of some personal privacy information, enterprise operation data, and national key data may lead to the disclosure of personal information, enterprise core data, and even national important information. That will bring various hidden dangers to national security. As transnational corporations, their wide range of operations and cooperation areas and access to a wide range of markets gives them access to enormous data on host countries. With the expansion of business, more and more multinational enterprises need to deliver internal data to the external unit users to cooperate with the completion of the process. There is no audit record, and there are some hidden dangers. Both external regulations and internal regulations of multinational enterprises put forward higher requirements for the security and audit of the data transmission process, especially some related to enterprises' core sensitive electronic data assets. Once intercepted maliciously in the transmission process, the loss is incalculable, but the existing data transmission means appear a little weak in terms of security. Or, excluding external factors, the transnational corporations themselves may leak the data of the host country due to their interests or political positions. All these require the host country to strictly control the data protection of the transnational corporations.

Data security capability involved in data control is also a direct reflection of national competitiveness. In the era of big data, it is becoming the main ability of a country to develop a digital economy and an important indicator to evaluate the level of national competitiveness. For the host countries where the subsidiaries of multinational enterprises are located, it is feasible to require multinational enterprises to localize their information storage. But this also requires host governments to establish regulations on the limits of what data can be released. Without much introduction to each of the regulations related to the localization of data storage, it is easy to see a larger problem for a multinational corporation on a global scale: how does it manage its enterprise to meet multiple technical, legal, and business challenges? Successfully meeting the challenge means moving beyond case-by-case solutions to in-depth exploration: reviewing the business and operating models to see how they can be customized in volume to better suit jurisdictions with storage localization requirements. The good news is that most multinational institutions have the capacity, qualifications, and resources to do just that. For those without such large budgets, strong and well-managed risk will go a long way. Risk management must point out that the challenge for regulators is not just to clarify technical guidance related to the localization requirements of new data storage. It extends to working with other regulators across the region and globally to simplify and standardize the requirements. This could help regulators better protect their national interests and further smooth the path for international investment and growth. This is an approach where localization and globalization go hand in hand.

5. OBSTACLES FOR HOST STATES IN DATA PROTECTION

5.1. Exchanging for profits

Regarding data protection, two of the biggest obstacles for multinational enterprises are diminishing self-interest and the difficulties for multinational enterprises to keep up with the technological developments. In corporate trades, customer's data is often exchanged to achieve the benefit of sharing customer resources. Or, companies with no sense of rule may sell their customer's privacy to realtors or insurance companies for profits. Last year, British consulting firm Cambridge Analytica gained access to millions of people's Facebook profiles without their consent, which was accused of using those data to push advertisements to affect the election [10]. Severely, this wasn't the first time Facebook has leaked customer's privacy. In response to the growing data problems, governments in Europe and the USA have begun to step up-regulation. A new bill presented by US senator Ron Lee Wyden imposed stiff penalties on companies who touched the bottom line intentionally or not. The bottom line includes collecting private data secretly, leaking data, buying or selling it, and even lying about it when data leaking happens [11]. As one big challenge to data protection, transactions involving personal data must be restricted in greater detail.

5.2. Difficulties for host states to follow the development of technology

Another biggest barrier to protecting data is the difficulties in following the development of technology. To put it another way, it's also considered difficult to update information. Globally, major economies have formulated their data privacy laws, which are quite different and unlikely to be unified in the short term. Consequently, it's hard to say what kind of personal information can be kept in the country and what kind of it can be sent abroad. This straight concerns if multinational enterprises can find a proper balance between governments and individuals, higher profits, and bottom lines [12]. In conclusion, the preferred solution

for dealing with the obstacle should be where the regulations will be followed and how.

6. CASE STUDY: GENERAL DATA PROTECTION REGULATION

6.1. Background

General Data Protection Regulation (GDPR), one of the most stringent rules concerning the protection of the European Union's (EU) residents' data by regulating the data processors and controllers' behavior was passed on April 27th, 2016, and took effect two years later on May 25th, 2018. Until now, GDPR has been enforced for three years. There have been criticism and compliment. What's more, some positivism researches have been done to study the effects of GDPR.

There are several changes in GDPR comparing with the EU's former legislation on data protection.

The first and foremost change is that GDPR takes the form of regulation which is distinguished from Directive 95/46/EC and the OECD Guidelines. Regulation means 'a rule or order prescribed for management or government.' [13] and has the same effect as law while failing to comply directive or guidelines which do not have binding legal force won't result in a citation and fine.

The second change is that the EU expanded its power through applying protective jurisdiction. There are three main types of jurisdiction normally: personal, territorial, and protective. Personal jurisdiction is the authority over a person, regardless of their location. Territorial jurisdiction is the authority confined to a bounded space, including all those present therein and events. Protective jurisdiction is the authority over actions committed anywhere in the world that affect its citizens. Usually, territorial jurisdiction is applied not only because it reduces the conflicts between sovereign states but also because it's hard to enforce the law aboard. Yet, the GDPR applied protective jurisdiction to the processing of personal data regardless of whether the processing takes place in the EU and whether the processor establishes it in the EU.

The third change is that GDPR set up some new rules to protect data. For example, GDPR creatively established the right to data portability and the right to erasure (Right to be forgotten). The prior one means the right to transmit data to another controller without hindering the controller to which the personal data have been provided. The latter means the right to obtain from the controller the erasure of personal data concerning him or her without undue delay. The controller shall have an obligation to erase personal data without undue delay where one of the following grounds applies. Another crucial rule of GDPR is administrative fines which can be up to 20 000 000 EUR or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

6.2. Criticism

Since the regulation came into force, there has been criticism on its disproportionate burden over data processors and controllers, i.e., enterprises, especially multinational enterprises which process data overseas.

Some argue that GDPR is strengthening the largest players while small- and medium-sized firms are being weakened [1]. The huge amount of compliance costs can only be afforded by large firms. It is reported that Fortune's Global 500 companies will spend roughly $7.8 billion to comply with GDPR. On the contrary, small- and medium-sized firms find it difficult to do so. Fewer than 50% of survey respondents report they are "fully compliant" with the GDPR, and nearly one in five admits that full GDPR compliance is truly impossible [14].

Some argue that GDPR is practically a trade barrier to keep small enterprises from nations that have loosening regulation on data protection and a prosperous information industry, e.g., America and China. Among the world's top 20 Internet companies by market capitalization in 2015, 11 of them are American enterprises, and 6 of them are from China, another 3 are also from East Asia. That means when GDPR was visioning, the lawmakers probably didn't take industry leaders' advice and were divorced from practice.

Some argue that GDPR is not only damaging the foreign enterprises, indigenous enterprises are also under pressure. According to short-run research, the implementation of GDPR resulted in a 26.5% drop in the aggregate dollar amount for each state and a 17.6% decrease in the number of EU venture deals [3].

6.3. Potential solutions

6.3.1. Territorial jurisdiction and exemption for small companies.

As mentioned before, GDPR is applying protective jurisdiction over enterprises all over the world and practically damaging small enterprises. The potential solution is for the EU to restrict its power to EU-established enterprises only and gave back the obligation of regulation over foreign enterprises to the home states. Another improvement can be an extension of the existing exemption for small companies. The GDPR can follow the example of the California Consumer Privacy Act (CCPA) and exempt small enterprises with little profits and consumers, which can hardly cause damage to data objects. For example, the smart bulb company Yeelight was forced to stop its service in the EU for it couldn't afford the cost of compliance, yet its mere data

processing was recording the opening and closing of a bulb.

6.3.2. Self-discipline organizations and industry rules.

Instead of a universal and stringent regulation, the lawmakers could consider setting up a loose. Still, general system, then let each industry form a self-discipline organization and make refined industry rules to refill the system. The aim is to let people who know the industry make regulations instead of working behind closed doors.

6.3.3. Consider the developing digital economy and innovation.

As mentioned before, GDPR is damaging the development of the digital economy by enforcing disproportionate liabilities to enterprises. The essence of the regulation is that it is a political announcement to cater to consumers' need for data protection as a basic human right, regardless of the development of the digital economy, which is clearly affecting people's passion for innovation in the digital era.

7. CONCLUSION

For governments aiming at effective protection, it's important to pass new legislation to ensure that consumers have clearer information so they can control how their information is used and decide whether their data is shared, with whom and how it is used. Also, correct and efficient regulation should be implemented, existing competition rules should be improved, mergers and acquisitions should be strictly restricted to prevent them from eliminating their potential' rivals' and ensure justice and equity. And rules should be put to change the business model if necessary.

REFERENCES

[1] L. Roslyn, The 10 Problems of the GDPR: The US Can Learn from the EU's Mistakes and Leapfrog Its Policy, in: AEI Paper & Studies, 2019, 1.

[2] L. Bergkamp, EU data protection policy: the privacy fallacy: adverse effects of Europe’s data protection policy in an information-driven economy, in: Computer Law & Security Review, 2002, 18(1), pp. 31-47.

[3] J. Jia, G. Zhe Jin, L. Wagman, The short-run effects of GDPR on technology venture investment, in: National Bureau of Economic Research, 2018.

[4] G. Aridor, YK. Che, T. Salz, The economic consequences of data privacy regulation: Empirical evidence from gdpr, in: NBER working paper, (w26900), 2020.

[5] D. Lyon, Surveillance as social sorting: Privacy, risk, and digital discrimination, Psychology Press, 2003.

[6] FTC v. Musical.ly, a corporation; and Musical.ly, Inc. a corporation, CD Cal, Civil Action No. 2:19-cv-01439.

[7] S. Van der Hof, No Child's Play: Online Data Protection for Children, in: Minding minors wandering the web: regulating online child safety, TMC Asser Press, 2014, pp. 127-141.

[8] B. Choudhury, M. Petrin, Corporate duties to the public, Cambridge University Press, 2019.

[9] P. Muchlinski, Multinational enterprises and the law, Oxford University Press, 2007.

[10] N. Confessore, Cambridge Analytica and Facebook: The Scandal and the Fallout so far, Retrieved from https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html, 2018

[11] The Fourth Amendment Is Not For Sale Act

[12] G. Yongqin, Study on Internation standards of Data Privacy Mangement in Enterprises, Journal of Technical Economics & Management(08), 2016, pp. 76-80.

[13] Black's Law Dictionary (4th ed), 1968, pp. 1451.

[14] The International Association of Privacy Professionals, IAPP-EY Annual Governance Report 2018, 2018.