Dean&Francis
ISSN 2959-6130

Navigating the Intersection of Data Brokers and GDPR: Economic Impacts and Limitations in the Information Trade Industry

Tsz Lam Ke[1,*], **Yannuo Cen**[2]

[1]*Ulink College Guangzhou, Ulink College Guangzhou, Shenzhen, 511458, China, kezilin6@gmail.com*
[2]*Chase grammar school, Chase grammar school, Stafford, WS11 0UR, United Kingdom, cenyannuo@gmail.com*

Abstract:

This literature review presents and explains the basic information about the General Data Protection Regulation and Data broker in terms and words that are generally understood by the public. This paper attempts to explore the impact on the online information economy since the enactment of the European Data Protection Regulation of 25 May 2018. Previous literature has explored the impact of the GDPR on the internet industry and is more dedicated to GDPR and data brokers themselves. This paper delves deeper into how specific data brokers get access to users' private information and monetize it. This paper also summarizes and analyzes the influence of the GDPR on Data brokers in the information intermediary industry, and we will try to find solutions to limit the development and operation of data brokers.

Keywords: Data brokers, GDPR, information economy, internet privacy, information privacy

1. Introduction

The data broker industry has emerged as a major player in the digital economy, collecting, aggregating, and monetizing vast amounts of personal information from a diversity of sources, including online behavior, public records, and transactions. Data brokers are tools or organizations that collect, analyze and trade personal data. Their main business is to collect personal data, and then collate and analyze the data collected to understand the consumption tendency of the information subject, family situation and other commercially valuable data. The data manager will sell the processed data to other organizations to help them with precision marketing, risk assessment and other related businesses.

Data brokers play a key role in facilitating targeted advertising, market research and risk assessment by providing insights derived from individuals' data profiles. However, as awareness of privacy and data protection issues grows, the industry is facing increasing scrutiny, particularly in the context of regulatory frameworks such as the General Data Protection Regulation, which came into force in the European Union in May 2018 (European Commission, 2020).

The GDPR represents a paradigm shift in the protection of personal data., with stricter regulations

ISSN 2959-6130

on how personal data is collected, processed, and shared, aiming to protect the rights of individuals in an increasingly data-driven world. It not only regulates traditional data controllers but also extends its reach to data processors, including data brokers, ensuring transparency, accountability, and respect for individuals' right to privacy. The regulation has prompted data brokers to reassess their operational practices to adjust consent mechanisms, data processing transparency, and compliance strategies.

Section 2 introduces what the General Data Protection Regulation (GDPR) is by collating previous literature and explaining exactly what it does and who it does it for. What exactly are the circumstances under which those companies or corporations are in breach of the General Data Protection Regulation (GDPR) guidelines for the unauthorized processing of private data. A rough outline of the penalties that companies that do not comply with the law will face.

Section 3 introduce the basic information of data brokers industry and answered various questions: what are data brokers? How data brokers collect personal information and who are their target consumers? How will the collected data be used? Whether the data collection activities of the data broker are lawful. And it outlines the whole process from how private data is made public or leaked to how data operators profit from selling private data.

Section 4 analyses how data brokers will be affected by the enactment of the GDPR, discussing the economic aspects of market changes and the limitations of some technologies and platforms.

Section 5 suggests how some data brokers can respond to the GDPR regulation and what they have to change to comply with the law. It also mentions some of the difficulties and challenges that data brokers may face when regulating their company's operating model.

Section 6 analyzed the impact of GDPR on the entire information market industry and the future development trend of data brokers.

2. The General Data Protection Regulation

2.1 The Principle of the General Data Protection Regulation

The General Data Protection Regulation (GDPR) is the most rigorous privacy. and security law in the world. Although this is a law of the European Union, it can be used in fields involving European data around the world. The regulation's commencement date on May 25, 2018. The GDPR will penalize enterprises that violate their privacy and security standards up to tens of millions of euros. As more and more people entrust personal data to cloud services, data breaches occur every day, and Europe has expressed its firm position on data privacy and security through GDPR. The regulation itself is large in scale and has a far-reaching impact, but there are quite a few specific details, which leads to a few people complying with this regulation, especially some small and medium-sized companies. We can first learn more about the right to privacy, which is part of the 1950 European Convention on Human Rights, which stipulates: "Everyone has the right to respect his private and family life, his residence and his correspondence." On this basis, the EU has been seeking to pass legislation to ensure the protection of this right. However, with the progress of technology and the invention of the Internet, the EU recognized the necessity of modern protection, so the European Data Protection Agency announced that the EU needed a "comprehensive method of personal data protection" and began to update the 1995 directive. GDPR came into force in 2016 after the adoption of the European Parliament, and as of the 25th of May 2018, all associations must comply with it. Secondly, the fine for violating the GDPR is very high. The fine is divided into two levels, up to 20 million euros or 4% of global sales. In addition, the data subject has the right to seek compensation for loss or damage. We will also discuss GDPR fines more. This rule is also divided into many regulations, and we will also talk about some in the following article.

2.2 Cases of Company Being Fined by GPR

When data broker is regulated by GDPR, it will reduce the risk of information leakage. The GDPR regulations themselves are large in scale and far-reaching, but the specific details are quite small, which leads to few people complying with this regulation, especially for some small and medium-sized enterprises. However, version 2.0 of GDPR has also appeared, which will solve the inefficient handling of major cases, especially those involving large technology companies. Before version 2.0, fines for violating GDPR were very high. The fine is divided into two levels, up to 20 million euros or 4% of global revenue. In addition, the data subject has the right to seek compensation for damages. Here is an example. Specifically, the CNIL found that Tagada had breached Article 6 of the GDPR, which allows companies to process consumer data with the consumer's consent, or to fulfill the company's legal obligations and protect its vital interests if this is necessary for the performance of an existing contract between the two parties. Benefit, perform the tasks necessary for public interest requirements, or promote the legitimate interests of the company unless these interests are replaced by the basic rights and freedoms of the data

subject. CNIL found that Tagada has no legal basis in the way it processes users' personal data. (Tagada collects and sends data to clients for advertising purposes from internet users who participate in competitions or product tests.) This example had a great influence at that time, which also made many people pay more attention to GDPR.

2.3 General Impact of the General Data Protection Regulation

Following the enactment of the GDPR in 2018, it has had a significant impact on data privacy issues around the world, shedding light on privacy legislation in other countries and raising the global profile of data privacy protection. According to recently published literature, more than 100 countries have set new standards for data privacy use three years after the introduction of the GDPR. For example, Brazil's Personal Data Protection Act, Canada added a Digital Charter to its Personal Information Processing and Electronic Documents Act (PIPEDA) covering cookies and opt-out options, and the US state of California's legislation draws inspiration from the GDPR. On top of that, the hefty fines that need to be paid for breaches of the regulations will make organizations more focused on protecting data privacy. Not only companies within Europe, but all multinationals that should operate from Europe must follow the GDPR, so some companies may adjust their business strategy in Europe in fear of the strict requirements of the GDPR. the GDPR also enhances the basic rights of users on the web, giving data subjects more control to correct inaccurate information and to erase data.

3. Data Broker

3.1 The Data Broker Industry

A data broker is a global industry that makes money by collecting your personal information, analyzing it, and licensing it to other companies to use for various purposes such as marketing, advertising, credit scoring, insurance, etc. Data brokers company collect information from various sources to establish up a detailed image of who you are and then sell it to other companies. The companies derive their principal revenue from providing data or inferences, especially about individuals, and this information originates primarily from sources other than the data subject themselves. People are usually unaware that their data is being collected because data brokers do not have a direct relationship with the people they collect data from. After collecting information, data brokers might know people's income levels, social status, health status, and even political views; this activity is legal when the data are obtained from public records.

3.2 How Do Data Brokers Collect and Sell Information

Data brokers select information through many sources such as newspapers, surveys, payment handling companies, travel agencies, government records, etc. The collection and analysis of data enables companies to conduct targeted advertising, market research and consumer behavior analysis, ultimately influencing the way products and services are marketed to consumers. Data brokers have thus constructed an environment in which individuals are "constantly surveyed and evaluated, investigated and examined, categorized and grouped, rated and ranked, numbered and quantified, included or excluded, and, as a result, treated differently" (Christl, 2017).

3.2.1 What Information Do Data Brokers Collect

Data brokers typically gather information through publicly available. information on the Internet and by purchasing information from other organizations, such as credit card companies. This collected data includes and is not limited to users' names, current and previous addresses, birth date, sex, civil status, family status, social security number, educational level, assets, profession, telephone number, email address, consumption habits, and even personal interest and bobbies.

3.2.1 How Do Data Brokers Sell Information

There are two ways in which information is sold, which are the direct sale of information and the indirect sale of information. In the terminology reported by the Federal Trade Commission (Fed. Trade Comm. 2014), the term 'original list' is used. An original list is the primary sales group for marketing and lead generation companies and financial data providers. An original list is typically just a group of customers who tend to have certain prospect characteristics. (Bergemann, & Bonatti 2019)

Direct sale of information is a type of information transaction in which private or commercial data is sold directly to a buyer, which can include a business or other marketing organization. The practice has grown considerably in recent years due to the growing need for targeted marketing, consumer insights and data-driven decision-making on the part of businesses that are becoming more and more web-enabled. Data sold in the direct sale of information includes personal data (e.g., a person's purchasing habits, demographics, household information, residential address), as well as commercial information (e.g., consumer records, market research, consumer shopping intentions). These data come from different social media, consumption records on online tasting tables, and what people say on social media. Data brokers will aggregate this collected information to analyze and categorise each person's living situation and financial needs. The direct sale of infor-

ISSN 2959-6130

mation is subject to various legal frameworks and regulations, such as the General Data Protection Regulation (GDPR), which governs how personal data is collected, stored, and shared.

Indirect sale of information means that data is not sold directly to the end user but is shared, licensed, or aggregated by an intermediary such as a data broker or analytics company. This approach is usually through partnerships, collaborations, or data-sharing agreements that allow businesses to monetize data without direct transactions. The information involved in this method of selling information may include anonymized user data, aggregated statistics, market trends, and insights derived from various data sets. Such data is typically collected from multiple sources, including online websites, applications, customer interactions, and third-party providers, and, subject to compliance with the law, can be aggregated and analyzed by data agents without exposing sensitive personal data. Indirect data sales are often widely used for market research, consumer behavior analysis, trend forecasting and strategic decision-making, enabling companies to refine their products and strategies. The indirect sale of information enables organizations to leverage data for competitive advantage while dealing with complex regulatory compliance and ethical considerations.

3.3 Lawfulness of GDPR

According to Article 6 of the GDPR, there are six lawful bases for processing and the most appropriate one will depend on the purpose of the organization and its relationship with the individual. These lawful bases are called the legal basis, which is used to regulate data control.

a. The data subject has consented to the processing of his or her personal data for one or more specific purposes.

b. Processing is essential for the performance of a contract to which the data subject is party or to take steps at the request of the data subject is prior to entering into a contract.

c. Processing is essential for compliance with a legal obligation to which the controller is subject.

d. Processing is essential to protect the vital interests of the data subjects or another natural person.

e. Processing is essential for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

f. Processing is essential for purposes of the legitimate interests of the controller or of a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.

If data brokers collect and process data in a way that complies with all six of these regulations, the profits they make are legitimate. In general, data brokers should operate within a compliance framework, audit the process of data collection, and keep a trace of all operations. Harmonization mechanisms must be transparent to both users and recipients of collection and allow for voluntary opt-in or opt-out options prior to any processing. The data collected should be anonymized to protect the user's privacy and reduce the risk of identification and should preferably be combined for proximity analysis. Data brokers should make sure that data is secure and encrypted with controlled access to ensure that any data being processed is not compromised. Communicate the privacy policy to users in clear and concise language, explaining clearly what the data will be used for and making clear to consumers who purchase data the importance of protecting private data from disclosure. To sum up, on the positive side, in compliance with the law, data brokers can reasonably collect and analyze data to provide valuable market information for relevant enterprises, which is conducive to the promotion of stable and sustainable economic development. However, if the data broker collects and uses data with illegal access to data, misuse of data, and other issues of principle, it will face legal sanctions. Whether a data broker is lawful or not depends on whether it strictly complies with the relevant data protection laws, whether the sources of data are authorized, and whether security measures are taken to protect the data.

4 Economic Impact of GDPR on Data Broker

Prior to the adoption of the General Data Protection Regulation (GDPR), EU data privacy laws applied to data brokers that processed the data of EU residents if the data broker had an establishment in the EU or used equipment located in the EU to process the data. Some smaller data brokers are already facing the challenge of complying with EU data privacy laws, but many others remain unaffected. Data brokers that process the personal data of EU residents from any organization, anywhere in the world, and using any device will be subject to legal action by EU law enforcement agencies in May 2018, when the EU's General Data Protection Regulation (GDPR) comes into force.

4.1 Changes in the Quantity and Quality of Users

The number of users will drop as the GDPR requires data brokers or websites to obtain consent from users before any data collection is carried out, with a clear opt-in or opt-out option. These remaining users who are still will-

ing to continue to use the website or platform are likely to use it for a longer period of time than those who refused to opt in, and they are more willing to use it, so these users are likely to have a higher usage time and activity value. This means more browsing history will be left behind, and more information may be analyzed. At the same time, because the filtered users browse the web page or use the program for a longer period of time, the exposure to advertisements and the time spent browsing will also increase, which makes the commercial value of these web pages or programs will increase. Data brokers analyze this legally obtained user information and sell it to advertising companies and related businesses that require relevant targeting. Advertisers then use the data analyzed by the data brokers to target their advertisements to different platforms, thus making the advertisements more effective and potentially driving more spending.

4.2 Cost and Investment

In addition to changes in the quality and quantity of users, the most intuitive impact of the enactment of GDPR on data brokers is a large increase in operating costs. Data brokers will need to invest heavily in ensuring that their business models are compliant. The first is to strengthen technical measures. For data processing activities involving high risk, data agents must take appropriate protection measures for the data, such as strengthening data encryption technology and restricting access to ensure data security and confidentiality. These things require the involvement of more professionals, as well as the maintenance and updating of technology and equipment which may involve substantial expenditure. Some small and medium-sized data broker companies may not be able to afford these innovations, which may lead to closure or the need to close down many of their operations and downsize their company's operations. However, as small and medium-sized businesses exit, larger companies that can face and pay for these costs in a timely manner can quickly capture significant market share. In addition, due to the fact that in order to respond to the more complex provisions of the GDPR, data brokers may need to revert to additional legal counsel to ensure compliance, thus producing more consulting fees.

As a result of the GDPR's erosion of data broker' rights to use data, companies will need to reorganize their entire business models and there are many data processing activities that will be restricted. Difficulties in analyzing, using and accessing data may force some businesses to close down. At the same time, uncertainty in the information market will increase due to the complexity of the GDPR and the nature of the GDPR as a dynamic regulation. The GDPR also imposes a shared risk and responsibility between those who collect data and those who use it, which means that cloud service providers and others who provide data processing services will be held liable. The reduction in the amount of investment in small and medium-sized companies and start-ups caused by the GDPR is likely to result in a significant number of jobs being lost in the EU each year, leading to an increase in unemployment.

5 Strategies for Data Brokers after GDPR Enforcement

5.1 How GDPR Regulates Data Brokers

The advent of the General Data Protection Regulation (GDPR) has had a significant impact on both the commercial activities of data brokers and the operations of businesses. The GDPR has imposed higher regulations on the acquisition, use and sale of data to protect the privacy rights of EU citizens. The scope of data regulated by GDPR is any information that can be used to identify an individual directly or indirectly. The GDPR stipulates that there must be a lawful basis for any information collected and processed by data brokers in any way, and this is detailed in Part III on the lawfulness of data brokers. The General Data Protection Regulation (GDPR) regulates the data processing activities of data managers in several ways. Data brokers must seek explicit consent from data subjects for all data collection, and consent must be free, specific, informed, and unambiguous. And data brokers only collect data that is necessary for a specific purpose; they cannot collect too much data or misuse it. Most importantly, users have the right to access their personal data held by data brokers and to request corrections if the data is inaccurate. In some cases, users can also request that their data be deleted, which means that the rights of the data subject have increased significantly.

5.2 How Data Brokers Respond and Change according to the GDPR

According to the GDPR, data brokers are required to appoint a Data Protection Officer (DPO) in certain situations where data is processed. The position of DPO will be assigned responsibilities in the following stages of data processing, with the relevant human and financial resources and budget, and will be managed as an independent department. The data broker company is also required to train employees on the GDPR, to raise awareness of data protection and to ensure that all employees are aware of and know how to comply with the GDPR in their work. In addition to training and reviewing employees, data brokers should also review suppliers and partners for GDPR compliance and ensure that agreements are signed in com-

ISSN 2959-6130

pliance with the GDPR.

Following the enactment of the GDPR, the majority of data broker organizations have reassessed their past data processing business activities and transactions for compliance with the GDPR. As mentioned in previous articles, the GDPR requires that the data processing process of any business should be open and transparent, and it is recommended that companies keep records of their data processing, which can prove their legitimacy and fairness. Along with this re-examination, data brokers should also set up clearer privacy policies such as clearly spelling out the data collected and the purpose on the user's terms of use and obtaining the user's consent before any data collection activities. Data brokers should also conduct a comprehensive assessment of the risk of the business and operations of the organization to identify potential data security risks. The company updates its technology to ensure that data encryption is strong and that the business does not have the right to divulge any private information.

There are many data brokers that may not be able to continue their business under the GDPR, so companies need to continue to innovate and find a business model that works in order to grow steadily. The GDPR is also a dynamic piece of legislation, so data broker companies need to keep an eye on the changes to the GDPR and make adjustments and changes in a timely manner.

5.3 How Can Data Brokers Ensure the Accuracy and Integrity of the Created Data

Data brokers are expected to set up data validation procedures that can use automated and intelligent tools to detect and screen data that has not been rigorously processed. Regular audits and inspections of collected and processed data should be carried out to remove data that is incorrect, outdated, or no longer useful. All data collected must come from legitimate and reliable sources, and good relationships should be established with organizations that adhere to strict data quality standards. Systems are to be put in place to update data on a regular basis, which may include automated data capture from reliable sources, periodic re-verification with data subjects or the use of real-time data updating techniques.

6. Conclusion

6.1 Future Trends in the Information Market under GDPR

In the future, the focus of data privacy will restrict access to data according to location, give users better control over their personal information, and implement strict regulations. Organizations need to adapt to these changes, maintain compliance, and win the trust of consumers. This will also make data brokers comply with the regulations, and they will also have better future development, better control of customers' personal information, and implement strict regulations. Organizations need to adapt to these changes (gdpr2.0), maintain compliance, and win the trust of consumers.

In the long term, as data privacy regulations continue to evolve and strengthen, the industry's need for data agents to ensure that data is lawfully collected, used, and shared is likely to increase. The information market will also become more specialized with the emergence of more professional bodies and accreditation standards. At the same time, as technology continues to evolve and innovate, there will be more techniques and technologies to improve data management and ensure data security, such as the incorporation of artificial intelligence and blockchain. There will also be an increase in international business cooperation, and due to the cross-border nature of data incursions, data brokers are likely to cooperate with more international partners to address cross-border data transfers and privacy protection challenges.

6.2 Summary

This post summarizes the basic definitions of GDPR and data brokers, their role and how they relate to each other. It then analyses the impact of GDPR on data brokers from an economic point of view and how the overall operational strategy will change, bringing changes to the information market. Then, based on the content of other previous papers, we put forward some suggestions on how data brokers can cope with the difficulties and constraints. In conclusion, the enactment of GDPR has brought many changes and uncertainties to data brokers in the future information market. More and more data brokers may now be able to continue their business in a compliant manner, but the GDPR will continue to improve as technology continues to evolve and new issues arise. Therefore, data broker companies need to keep focusing on the GDPR and provide better data management and privacy protection services to users by continuously improving their professional competence, enhancing technological innovation, and establishing good relationships with users.

References

[1] Admati, A. R., & Pfleiderer, P. (1990). Direct and Indirect Sale of Information. *Econometrica*, *58*(4), 901–928. https://doi.org/10.2307/2938355

[2] Anat R. Admati, & Paul Pfleiderer, (2024). Direct and Indirect Sale of Information - The Econometric Society. Retrieved August 13, 2024, from Econometricsociety.org

website: https://www.econometricsociety.org/publications/econometrica/1990/07/01/direct-and-indirect-sale-information#:~:text=In%20a%20direct%20sale%20buyers%20observe%20the%20seller%27s

[3] Baker, L. (2017). The impact of the General Data Protection Regulation on the banking sector: Data subjects' rights, conflicts of laws and Brexit. *Journal of Data Protection & Privacy*, *1*(2), 137. https://doi.org/10.69554/eiyo6659

[4] Bergemann, D., & Bonatti, A. (2019). Markets for Information: An Introduction. *Annual Review of Economics*, *11*(1), 85–107. https://doi.org/10.1146/annurev-economics-080315-015439

[5] Birckan, G., Dutra, M., De Macedo, D., & Viera, A. (2018). Effects of data protection laws on data brokerage businesses. *ICST Transactions on Scalable Information Systems*, 165673. https://doi.org/10.4108/eai.22-7-2020.165673

[6] Elizabeth Denham, E. D. (2020). *Investigation into data protection compliance in the direct marketing data broking sector*. Retrieved from https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf

[7] *EPIC* (2024).Electronic Privacy Information Center. Retrieved from: https://epic.org/issues/consumer-privacy/data-brokers/

[8] Federal Trade Commission. (2014). *Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission (May 2014)*. Retrieved from https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

[9] Glory France, (2017). Data-Driven Marketing and the GDPR: the Data Brokers' Conundrum | Privacy & Security Law Blog | Davis Wright Tremaine. (n.d.-b). Retrieved from https://www.dwt.com/blogs/privacy--security-law-blog/2017/07/datadriven-marketing-and-the-gdpr-the-data-brokers

[10] Information Commissioners' Office. (2023). Organizations using marketing services of data brokers: what you need to know. Retrieved from ico.org.uk website: https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/organisations-using-marketing-services-of-data-brokers/

[11] IT GOVERNANCE PRIVACY TEAM. (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide - Second edition* (2nd ed.). IT Governance Publishing. https://doi.org/10.2307/j.ctt1trkk7x

[12] Lexxion..https://edpl.lexxion.eu/data/article/13101/pdf/edpl_2018_03008.pdf

[13] Latto, N. (2024). Data Brokers: Everything You Need to Know. Retrieved from Data Brokers: Everything You Need to Know website: https://www.avast.com/c-data-brokers

[14] LinkedIn: Log in or sign up. (n.d.). Retrieved from https://www.linkedin.com/

[15] Jones, A. (2021). GDPR Three Years Later: What Impact Has It Made? Retrieved from https://www.ispartnersllc.com/website: https://www.ispartnersllc.com/blog/gdpr-one-year-later-impact/

[16] Kaspersky. (2020). *Data Brokers & Data Brokerage*. /.][https://usa.kaspersky.com/resource-center/preemptive-safety/how-to-stop-data-brokers-from-selling-your-personal-information\

[17] Kazemi, R. (2018). *General Data Protection Regulation (GDPR)*. tredition.

[18] Mary Rendle, M. R. (2023). Global Data Hub. Retrieved August 11, 2024, from Taylorwessing.com website: https://www.taylorwessing.com/en/global-data-hub

[19] Mishra, S. (2021). The dark industry of data brokers: need for regulation? *International Journal of Law and Information Technology*, *29*(4), 395–410. https://doi.org/10.1093/ijlit/eaab012

[20] Otto, P. N., Anton, A. I., & Baumer, D. L. (2007b). The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information. *IEEE Security & Privacy Magazine*, *5*(5), 15–23. https://doi.org/10.1109/msp.2007.126

[21] Morris, H. &. (2024). Understanding the new data broker registration laws — Hosch & Morris, PLLC. Retrieved from https://www.hoschmorris.com/privacy-plus-news/data-broker-registration-laws

[22] Reviglio, U. (2022). The untamed and discreet role of data brokers in surveillance capitalism: a transnational and interdisciplinary overview. *Internet Policy Review*, *11*(3). Retrieved from https://policyreview.info/articles/analysis/untamed-and-discreet-role-data-brokers-surveillance-capitalism-transnational-and

[23] Štarchoň, P., & Pikulík, T. (2019). GDPR principles in Data protection encourage pseudonymization through most popular and full-personalized devices - mobile phones. *Procedia Computer Science*, *151*, 303–312. https://doi.org/10.1016/j.procs.2019.04.043

[24] Stevens, G. (2007). *Data Brokers: Background and Industry Overview*. Retrieved from https://www.ipmall.info/sites/default/files/hosted_resources/crs/RS22137_070503.pdf

[25] Voigt, P., & Von Dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.

[26] Yeh, C.-L. (2018). Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers. *Telecommunications Policy*, *42*(4), 282–292. https://doi.org/10.1016/j.telpol.2017.12.001