Journal of Digital Convergence
Vol. 18. No. 6, pp. 17-32, 2020

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2020.18.6.017

Dilemma of Data Driven Technology Regulation : Applying Principal-agent Model on Tracking and Profiling Cases in Korea

Youhyun Lee[1], Ilyoung Jung[2*]
[1]Assistant Professor, Department of Public Administration and Police Science , Hannam University
[2]Research Fellow, Science and Technology Policy Institute

데이터 기반 기술규제의 딜레마 : 국내 트래킹·프로파일링 사례에 대한 주인-대리인 모델의 적용

이유현[1], 정일영[2*]
[1]한남대학교 행정·경찰학부 조교수, [2]과학기술정책연구원 혁신성장정책연구본부 연구위원

Abstract This study analyzes the regulatory issues of stakeholders, the firm, the government, and the individual, in the data industry using the principal-agent theory. While the importance of data driven economy is increasing rapidly, policy regulations and restrictions to use data impede the growth of data industry. We applied descriptive case analysis methodology using principal-agent theory. From our analysis, we found several meaningful results. First, key policy actors in data industry are data firms and the government among stakeholders. Second, two major concerns are that firms frequently invade personal privacy and the global companies obtain monopolistic power in data industry. This paper finally suggests policy and strategy in response to regulatory issues. The government should activate the domestic agent system for the supervision of global companies and increase data protection. Companies need to address discriminatory regulatory environments and expand legal data usage standards. Finally, individuals must embody an active behavior of consent.

Key Words : Technology Regulation, Data Industry, Principal-Agent Model, Tracking, Profiling

요 약 본 연구는 주인-대리인 모델을 적용하여 데이터 산업의 이해관계자인 정부, 개인, 기업의 규제 이슈를 분석해내는 데 목적이 있다. 데이터 산업은 거대한 딜레마적 상황에 직면해 있다. 데이터 경제의 중요성이 빠르게 부상하고 있으나, 데이터 사용에 대한 국가의 규제로 인해 산업 발전이 저해되는 한편, 데이터의 무분별한 활용으로 인한 개인의 프라이버시 역시 침해받고 있다. 본 연구에서는 기술적 사례연구의 방식을 이용하여 딜레마적 상황에서 각각의 행위자들의 이해관계에 기반한 규제 이슈를 분석하고, 그에 대응할 수 있는 전략을 제시하였다. 사례분석 결과 첫째, 국내 데이터 산업의 주요 정책행위자는 데이터 회사와 정부이다. 둘째, 데이터 기반 사회에서 가장 우려스러운 두 가지 문제점은 기업이 빈번하게 개인정보를 침해한다는 것과 국제적 기업의 데이터 독과점 현상이 나타난다는 점이다. 이러한 규제 이슈를 해결하기 위해 본 논문에서는 이에 대한 전략을 다음과 같이 제시하고 있다. 정부는 글로벌 기업의 감독을 위한 국내 대리인제도를 활성화하고 데이터 보호를 증대해야 한다. 기업은 차별적인 규제환경을 해결하고 합법적인 데이터 활용기준을 확장해야 한다. 마지막으로 개인은 능동적인 동의 행태를 구현해야 한다.

주제어 : 기술규제, 데이터 산업, 주인-대리인 이론, 트래킹, 프로파일링

*This study was supported by the research program of Science and Technology Policy Institute(STEPI), 2019.
*Corresponding Author : Ilyoung Jung(iljung@stepi.re.kr)
Received March 11, 2020 Revised April 24, 2020
Accepted June 20, 2020 Published June 28, 2020

1. Introduction

As the value of data rises, society is quickly transforming into a data economy paradigm [1]. With data becoming a major keyword in innovation, firms and individuals worldwide are fixing their attention on it to vitalize the data economy. Within this paradigm of data-based economies, capabilities such as creating, collecting, and utilizing data play an essential role in securing the competitiveness of a firm or a country. As such, a phenomenon, where firms that utilize data have monopolized the consumer data has also occurred [2].

South Korea (hereinafter Korea) has also perceived the importance of the data industry and has continuously established and executed strategies to vitalize the data industry [3]. However, data-related issues was addressed by in manner of being scattered by subjects such as clarification of the scope of personal information, anonymization guidelines, and evaluation of the adequacy of the EU's General Data Protection Regulation (GDPR). Therefore, this study analyzes the regulatory issues of firms, the government, and the individual as key stakeholders and actors in the data industry using the principal-agent theory; furthermore, the study identifies the causes and the key considerations to the issues and then provides corresponsive policy and strategies.

The causal factor behind regulatory issues in the data industry is the changes to how data is perceived [4]. Data, or private information, was considered as a target for protection; however, the changes to the paradigm of data have shifted this perception, with the data now being recognized as an object of value creation and as valuable assets. The principal-agent theory, which is the theoretical analysis framework of this study, explains a variety of problems that may arise when each transactional party forms a state of information asymmetry. The principal bestows discretionary power relating to his interest in the agent and rewards the agent when the agent acts in the interest of the principal [5-7]. Although the agent has the responsibility to work on behalf of the principal's interest, this relationship generally leads to issues such as information asymmetry, the incompleteness of oversight, and moral hazard [8].

The regulatory issues in the data industry present appropriate cases to apply the principal-agent theory and shed light on the fundamental determinants of the key issues in regulating the technological environment. The concept of contract in the early data ecosystem consisted of the government (agent) for protecting the information of the individual (principal). To achieve this, the government needed to execute regulatory policies that provided oversight and control to the firms collecting and utilizing data on behalf of the individual. However, the improvements in utilizing the value of data and subsequent changes to the ecosystem have led to the diversification of contracts between actors and the rise of agency problems such as misuse of information.

For data companies, agency problems occurred as they excessively collected, stored, and utilized them in manners that did not befit the original objectives, which is utilizing the data to provide services to the individual (principal). These issues have led to invading the privacy of individuals as principals, and monopolizing the data market by the firms (agents). As for governments, the original contract was to safeguard the information of individuals, who are the principals in this relationship. However, with developments in information recognition technology and excessive collections of data, as with firms, the governments also face similar agency problems, which leads to invading the individual's privacy, surveillance and, control of personal data. Lastly, the government was tasked

with a dual role: from the single contract of "protecting private information," they now are tasked, under a new contractual relationship, with the responsibility of vitalizing and nurturing data utilization.

From this perspective, this study has selected cases of technology regulations that occur within the relationships between the responsibilities and rights of key stakeholders in the data industry. The cases analyzed in this study involve regulatory issues of online customized advertising firms, the agent, utilizing, tracking, and profiling the data of the principal, the individual.

2. Institutional Backgroud

2.1 Oveview of the Data Industry

The scope of the data industry is generally defined as "the production and delivery of products and services that create value through creating, collecting, processing, analyzing, distributing, and utilizing data," and all industries involved in the processes and activities of value creation in the data value chain are included [9]. The data industry can be divided into four large categories: data solution, data construction and consultation, data services, and data infrastructure.

Currently, as the scope of these data industries grows, the influence of data platform firms that create and collect data is expanding. Chunlei Tang (2016) defines the data industry using both narrow and wide definitions(see figure 1). Narrowly, the definition remains similar to the previous definition; widely, the data industry can be defined as an industry that has developed technical processes involved in preparing, mining, and visualizing data [10]. In other words, the data industry encompasses developing and utilizing data resources, effectively managing data assets, innovating data technologies, and directly commercializing data products. According to this definition, the following list of existing industries is also considered to be part of the data industry: publishing, digital media, electronic libraries and information, digital content, and data services.

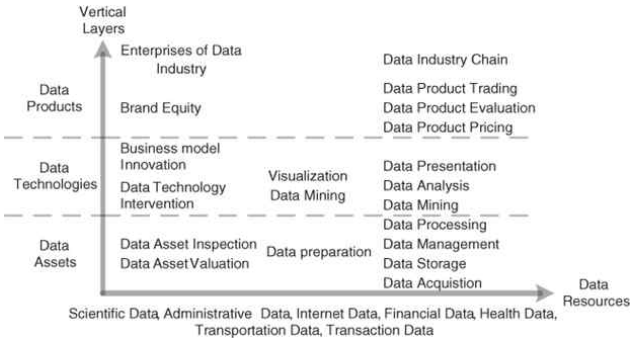

Fig. 1. The structure of the extended data industry
Source: Chunlei Tang (2016)

2.2 New landscape resulting from improvements in the value of data

The key policy actors at the core of the data industry are the firm, the individual, and the government. Then, which of these actors is the most important in the data industry? Surprisingly, at the core of the regulatory issues of the data industry is the individual. This is because the changing landscape of the data industry is very similar to changes in the perception of private information. The data industry is defined as "the production and delivery of products and services that create value through the creating, collecting, processing, analyzing, distributing, and utilizing data [9]" and is inclusive of all activities within the data value chain. However, given the realities of Korea, one sector that is essential in regulating technology of the data industry is the sector that pertains to the production and utilization of data [11].

The protection of private information in industrial society refers to the right to be free from physical harm. Privacy in this context, and in passivity, refers to the right to information

without the interferences of others. However, with the modern society trends, privacy focuses on the fact that an individual's information is as valuable as an asset [12], and privacy, in this context, creates value. The reason why regulatory issues arise in the data industry is based on this change in the perception of data, from the previously understood protection of private information to perceiving data as a value-creating and asset-like target with intrinsic value.

Table 1. Paradigm Shift in Data Protection

Industrial Society (Prior to 1960s)	Industrial /Information Society (1960 - 2010)	Ubiquitous Society (2010 -)
Restricted due to physical space	Spatio-temporal limitations	Merging between the real and the virtual world
Privacy is defined passively in a dictionary style manner	Privacy is defined passively	Privacy is defined actively
Right to be free from physical infringement	Right to be free from information infringement	Right to receive protection of the value of information

Source: Personal Data Protection Laws in Korea (Accessed: 2019.05.21.)

3. Principal Agent Model and Research Design

3.1 Principal-Agent Model

The principal-agent theory explains various problems that may arise when each transactional party forms a state of information asymmetry [13,14]. This theory, derived from economics, explains issues arising from a principal that asks an agent to use the agent's abilities to engage in actions that leads to the principal's interest [15]. In this case, the principal bestows discretionary power relating to the principal's interest in the agent and rewards the agent when the agent protects the principal's interest. The agent has the responsibility to act on behalf of the principal's interest. A typical principal-agent relationship may lead to issues such as information asymmetry [14], the incompleteness of oversight, moral hazard, and agency costs that may be incurred as a result of these problems [16].

A contractual relationship exists between the principal and the agent, and the basic premises of the contract are that the agent has more capabilities and knowledge about a certain matter than the principal. Therefore, the principal bestows the agent discretionary powers of delegation, for the agent to engage in the delegated tasks, and the effects of the delegated tasks affect the agency. Ultimately, the core issue of the principal-agent problem is compensating the agent to conduct tasks in a way that maximizes the principal's interest.

The regulatory issues in the data industry present appropriate cases to apply the principal-agent theory and shed light on the fundamental causes of key issues in regulating the technological environment. However, the application of the principal-agent theory in the data industry requires an essential consideration. This is the question of whether the individual owns the data. Much data on the Internet, ranging from financial data, medical data, and location data are collected from the individual. As a multitude of data sets are collected from the individual, it is important to establish whether the individual can be seen as the owner of the data. Legally, targets of ownership rights are "tangible assets," and it is difficult to define data as a tangible asset under law, or as a "corporeal thing," or as a part of "electricity," or "other natural forces which can be managed. Therefore, the reality is that rather than recognizing the individual's ownership of data in a direct manner, Korea's Personal Information Protection Act or EU's GDPR and other legal frameworks allow partial and indirect rights to the individual such as the right to ask for modification, deletion, and agreement [4]. Considering the realities of such legal systems, this study assumes the individual's ownership of the data and applies the principal-agent theory to the data industry.

3.2 Triangle of Contract (Business-Government-individual)

The government, the firm, and the individual, as core actors in the data industry, become stakeholders in government regulations in the traditional sense within the triangle of regulation composed of the regulator (the government), the regulated (the firms), and the beneficiary (the individual). However, the logic of this regulatory triangle cannot be strictly applied to the data industry. This is because data is no longer regarded as a passive target for regulation for data protection, but rather as an asset that creates value. It has not been long since the importance of data has been emphasized as intangible assets. With the 4th Industrial Revolution, firms and institutions began to place higher values on data, and individuals began to perceive their own data as assets.

The reason why it is difficult to regulate the data industry is that as data is perceived as a valuable asset, a dual contractual relationship occurs. As seen in the figure below, the level to which the firm utilized the data of individuals or consumers was low at the beginning of the data ecosystem. Furthermore, the government was only responsible for protecting the data of the individual, who were owners of the information. Therefore, the government was only mandated to carry out its duties under the contractual relationship on behalf of the individual, and to achieve this, it had to establish regulatory policies and provide oversight for firms that may invade the privacy of the individual.

However, as the asset value of data increases, firms began to utilize the data of individual consumers for purposes other than providing services, leading to issues of moral hazard and information asymmetry. This agency problem currently continues to expand beyond the invading the privacy of the individual as a consumer to monopolizing the data market. The issues that occur as the agent, the firm, misuses the data owned by the individual, the principal, for objectives other than providing the services for the individual are hereby defined as Business to Consumer (B2C) regulatory issues. Typically, in management studies, the term B2C refers to a business model that is based on transactions between the firm and the consumer.

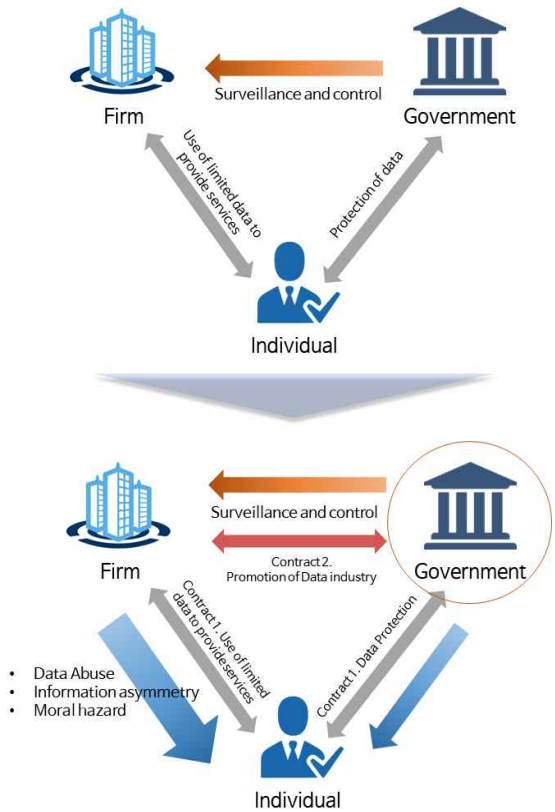

Fig. 2. Shift of Contract

Table 2. Principal Agent Model and Expected Regulation Issues

Classification	Higher protective value of information	Higher utility value of information
Principal-Agent	Individual (Information owner) - government	Individual (Information owner) - data firm
Expected issues with techno-logical regulation	·Loss of incentives for technological development ·Lower levels of entrepreneurial spirit ·Locked-in markets (Entry barriers) ·Lower ability to respond to environmental changes ·Regulatory time lags	·Invading privacy rights ·Lower self- determination rights ·Decreasing human dignity ·Intensifying information asymmetry ·Moral hazard

As shown in the above table, focusing excessively on the protection of information, which is the first contractual relationship, can lead to lower incentives for technological development, decrease entrepreneurial spirit, cause market lock-in, lower adaptiveness, and cause regulatory time lags. However, focusing on the second contractual relationship of utilizing the information can lead to invading rights to privacy, decreased self-determination rights and human dignity, intensifying of information asymmetry, and moral hazard. Therefore, in today's paradigm where data is a valuable asset, it is essential for the government, as the main regulator that is responsible for vitalizing the data industry, to carefully design and regulate the industry.

3.3 Research Question and Methodology

This study has two purposes; one is to develop the framework based on the principal-agent theory to analyze technology regulation policy and data industry, another is to provide the policy and strategy in response to main regulation issues. In previous chapter, this paper already discussed the principal agent theory and current situations. Therefore, these research purposes are transformed to following research questions.

Q1. Who are key policy actors in data tracking and profiling issues in Korea ?

Q2. What are main regulatory issues for each parties; firm, government, individual?

Q3. What strategies can be suggested for each regulatory issues?

In order to find answers for each research questions, this paper used a explorative approach and in-depth case study method. To formalize a explorative approach, we employed a context and frequency analysis. The data was obtained by extracting the evidence intensively from literature review. The time frame of this study is mainly from May 2017 to December 2019. We used context analysis with Government Report year of 2017, 2018, 2019 (Ministry of Science & ICT, Korea Data Agency, Korea Communications Commission, Korea Internet & Security Agency), and newspapers, journal articles and books. The frequency analysis was also applied to identify the core policy actors of tracking and profiling cases in Korea. A article search site, Big Kinds(www.bigkinds.kr), was used to analyze the core actors. Research questions and analytical framework can be summarized below the figure 3.

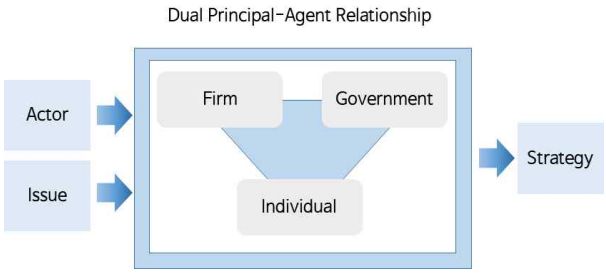

Fig. 3. Analytical Framework for Case Analysis

4. Case Analysis

4.1 Case Overview

Consumers that purchase products online often see advertisements for the products that they are wondering to purchase or not on the lower parts or the sides of their screens when they are online. The limitation of traditional advertising is that the products were not able to be shown on time to the consumers that need them. However, technological advancements and customizing online advertisements have led to collecting and analyzing consumer behavior for subsequent advertisements of products that fit consumer behavior [17]. Online customized advertisements are defined as "online advertisements provided to users on a customized basis after processing of behavioral data, followed by analysis and estimates of user interests, tastes, and preferences" [18].

A key income source for global Internet firms like Google or Facebook is online advertisements. However, the online customized advertisements have advantages and disadvantages and constitute a case that can highlight key considerations for diverse and new technological regulations. Online customized advertisements allow advertisers to effectively market products to a certain group of consumers, and the acquisition of consumer information allows consumers to save time and economic costs. Moreover, effectively utilizing network resources also gives related industries a competitive advantage. On the other hand, advertisers may unintentionally leak consumer information, which can be misused, or incite impulsive purchase behaviors in consumers.

Tracking technology is often used for online customized advertisements. Tracking refers to real-time tracking of various data sets of users, and cookies are universally used for user behavior tracking. A cookie is a small text file that is saved on the user's computer through the web browser when the user visits a website, and it is saved onto the user's computer or smartphone. This file has a unique identifier number and is normally saved on a web browser. When the consumer revisits the online site, the individual can be identified using the unique identifier on the cookie [4].

The excessive use of tracking technology, such as cookies, can lead to violating private information. Firstly, consumer profiling, which merges the data collected through the cookie and the member registration information, may violate the rights of anonymity of users who did not log in intentionally. Profiling is generally defined as the collection of information on individuals or groups, subsequent analysis of characteristics and behaviors based on the collected information, classifying individuals and groups into a certain range, and the evaluation of work capabilities, interests, and potential behaviors [19]. GDPR defines profiling as "any form of automated processing of personal data, evaluating the personal information of a natural person, in particular, to analyze or predict the data owner's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, where it produces legal effects that significantly affect the data owner" [20]. Although, from the perspective of the firm or institution processing the private information, profiling provides the benefit of automated estimation and evaluation of the information, the individual, as the owner of the data, can be put at risk of exercising their rights in processing their private data, and the individual's privacy may be invaded.

When user profiling is combined with a "third-party cookie," the chances of invading private information becomes higher. When a consumer visits a specific website, they may often download the cookie from the visiting website and cookies from other sites, and the latter is referred to as third-party cookies. According to Ko et al. [4], tracking is relatively active in the Korean Internet environment, and it occurs whether the user logs onto a specific account or not. A survey of 91 Korean websites indicated that on average, third-party cookies from doubleclick.net ware being used in an average of 40 sites to collect consumer data. Furthermore, the overall average of cookies collected in the desktop environment was approximately 57, and 54 on the mobile environment.

The evolved form of third-party cookies is the embedding of Youtube clips and the "Like" buttons on Facebook. The data from the clips embedded on specific websites or web pages are sent directly from the Youtube server along with cookies. The "like" button on Facebook acts similarly to this method. The tracking technology, which enables online customized

advertisements, can provide convenience to the individual consumer through customized services despite risks of invading private information. As individual assessments of the same technologies and services may vary and generational differences in perspectives exist, it is difficult to generalize; however, because there is a higher negative perspective of customized advertisements, this study opts to discuss regulatory issues relating to customized advertisements.

4.2 Key Actors and Regulatory Parties

Besides individuals and the government, tracking- and profiling-enabled online customized advertisements have a diversified series of data firms as key actors. Advertisers, publishers, and network providers constitute the data firm group. Advertisers want to advertise their products to individuals, who are website users who are more likely to purchase their products or services. Publishers generate income by providing web-enabled advertisement spaces and allowing web users to view advertisements. These publishers are owners and operators of websites. Lastly, network providers connect and provide the network for advertisers and publishers. For the online customized advertisements to be shown directly to the individual website users, a variety of policy actors within the data firm group participate,

Big Kinds, a newspaper article search site, was utilized to analyze the core actors who follow regulations governing the online customized advertisements. A search was conducted spanning from May 10, 2017, to July 22, 2019, with the subject of "online advertisements" and a mandatory search term of "regulation," and this indicated that industry actors such as "Google," "EU," "NAVER," "Apple," "Korea Communications Commission," "Ministry of Science and ICT," "Ministry of Justice," "Financial Services Commission," and "Korea Internet & Security Agency" had high degrees of connectivity with indicators of centrality as nodes.

In the regulatory case of online customized advertisements through tracking and profiling, the key policy actors are divided into data firms (Google, YouTube, NAVER, Apple, Amazon, Kakao, etc.) and the government (Ministry of Science and ICT, Korea Communications Commission, Financial Services Commission, Ministry of Justice, Korea Internet & Security Agency). Although the case is of a B2C nature, the core policy actors are divided into data firms and government agencies because the government acts as an agent to protect the consumer's right to privacy. Therefore, as the agent to the consumer, the government becomes a direct actor along with the firm in the regulatory case. Some significant words and related searches stemming from the Big Kinds search of "online advertisements" and mandatory search term of "regulation" are "Google," "Facebook," "NAVER," "YouTube," "Chinese government," "EU," and "firms." Furthermore, the frequency of newspaper articles that contain both "online advertisements" and "regulation" has remained high since the beginning of the Moon Jae-in administration.

4.3 Regulatory Issues

4.3.1 Firm (agent): Comprehensive invasion of privacy rights by global data firms

The key source of income of global IT firms such as Google and Facebook are online customized advertisements. Google operates Gmail, a global email network, and Chrome; and Facebook operates its Facebook platform, WhatsApp, and Instagram to provide customized advertisements based on behavioral data collected from their users. Firms leading the digital online advertisement revenues are Google and Facebook, and their advertisement revenues have consistently grown from 2012 to 2018 [21].

More than 90% of Google's revenues come from advertisements.

Google has utilized programs that connect users to the Internet, Internet Explorer and Safari, to collect private information, and continue to collect data using the smart devices that have Safari as its basic application such as iPhones, iPads, iPods, and Mac computers. Although Safari and Explorer both have safety measures, Google bypassed such safety measures by sending false signals to install cookies when these programs had disabled their security measures; the US Federal Trade Commission fined Google $22.5 million because of that. The debate over Google's customized online advertisements has come under increasing scrutiny by the European regulators as the new General Data Protection Regulation (GDPR) comes to effect. Commission Nationale de l'informatique (CNIL), the French data protection agency, fined Google 50 million euros, arguing that Google violated GDPR, and this constitutes the largest-ever fine since the introduction of GDPR. CNIL received reports that Google had no legal rights to process advertisements using private information, and the reports were received from None of Your Business (NOYB), a digital rights advocacy group, and La Quadrature du Net (LQDN), a French Internet privacy advocacy group. CNIL imposed the fine because Google did not provide sufficient explanation about using private information for online customized advertisements [22].

Issues with leaked data and information, and invading privacy through tracking and profiling have been a global concern. Although Internet firms have earned revenue by collecting website users' cookies and providing advertisements that meet the users' needs, the issue is that the cookies collection activity occurs without the consumers knowing the presence of such activity. Certainly, consumers are able to block customized advertisements through opt-out processes and blocking cookie collection. However, there are three fundamental issues. Firstly, the website users are not aware of the existence of the cookies; secondly, there is no agreement on collecting the information, and lastly, even if they wanted to block the use of cookies, the users do not clearly understand the opt-out process. The consumer, the individual, has an unclear perception towards data collection, and particularly in the case of Korea, the notification of the collection of behavioral data is not mandatory, which poses a significant threat to invading privacy, as private information leaks out without the users knowing about it. Furthermore, the collection of individual behavioral data without one's perception of such collection can invade the right to informational self-determination of the online user [18].

4.3.2 Firm (agent): Market monopolization of the data industry by data firms

Currently, a key issue emerging is the market monopolization of the data industry by large tech firms, such as Google and Facebook. The reason why the market monopolies of large tech firms have become vital is that market monopoly leads to the monopolization of consumer data. Facebook began services in 2004, and gathered 350 million users over three years; in 2012, it had a billion active users a month. As of March 2019, there were over 2.38 billion users on Facebook, indicating that some 1/3 of the global population were on the Facebook platform [23].

Although the fact that Facebook has a large user base does not constitute the rationale for it to become a regulatory issue, Facebook's invasion of privacy is on the rise in recent times. Notable invasions include the collection of private information and internet usage information not only on the Facebook domain, but also other linked websites and mobile services, collecting not only the articles that the user reads, but also internet shopping trends,

status messages, and comments that have been entered but not posted. For Android users in the U.S., Facebook also has access to their cell phone records, and Facebook earns massive advertisement revenues on the back of such data; of the $40 billion revenues in 2017, over 98% was advertisement revenues. Besides corporate profits, consumer targeting through Facebook is having a significant impact on the U.S. presidential elections.

The reason why market and data monopolization by data firms are regulatory issues is that the monopolizing firms respond differently before and after the market monopolization. Prior to its market monopolization, Facebook introduced the Beacon service in 2007. The Beacon service is an advertisement program that informs a third party through a news feed when the user visits a Facebook affiliate site to purchase products [24].

The users were able to agree or reject the beacon services, but Facebook still tracked external service usage after users had rejected the beacon services, and continued to track external service usage even after the users had logged out of Facebook. After the research results were announced, mass lawsuits followed in Texas and California, and Facebook closed down the Beacon service in September 2008. During this time, the number of MySpace users was more than double that of Facebook, and the competition in the social network market was fierce with competitors such as Google's OpenSocial and Bebo in the United Kingdom.

In 2010, as the competitive landscape took a more monopolistic structure, the "Like" button was introduced. External service agencies could add a simple Facebook HTML code to identify the users' usage details in a manner that was very similar to the Beacon service. These functions led to some 50,000 websites adding this plug-in within a week. When a Facebook user visits a website that they had "liked," Facebook collected the particular website's login cookies, the articles that the user had read, and information on the products the user had purchased. Furthermore, similar to the Beacon service, it was confirmed that Facebook was tracking the internet usage histories after the user had logged out. Facebook responded to this event in a very passive manner, introducing a new privacy policy, rather than ceasing the service.

In 2014, when Facebook had tightened its grip on the market monopoly, a large number of competitors (MySpace, Friendster, Mixi, Cyworld, hi5, BlackPlanet, Yahoo's 360, AOL's Bebo, etc.) had disappeared. In June 2014, Facebook announced that it would track the internet usage histories of users to engage in customized advertisements. Unlike in 2007, Facebook had control over the majority of the market and had enough influence to control external agencies as well as the market ecosystem. Facebook strengthened its user tracking to allow the usage information to remain on the Facebook profile even if the user deleted its cookies, Facebook did not provide its users with the rights to reject tracking and continued to track even if the user had set the web browser settings to "Do Not Track." This case indicates that a firm strengthening of its monopoly over a market leads to the loss of the self-healing capabilities of a business model, and to significantly higher possibilities of invading private information.

4.3.3 Individual (Principal): the privacy paradox

Privacy paradox is a term that refers to the gap between the interest and attitude of a user towards privacy and their actual actions [25]. In other words, it refers to a phenomenon where an individual expresses concern over the protection of private information and demonstrates a positive attitude towards privacy protection, but fails to take steps to protect their privacy.

A PwC report found that 92% of consumers responded that they should be able to control information about themselves on the internet,

and 71% responded that they would not do business with firms that provide unauthorized (third-party) access to sensitive information. However, despite such high perceptions of privacy, an IBM survey found that only 45% of users had updated their personal information settings, 16% had ceased doing business with problematic businesses and 18% had deleted their social media profiles, indicating that the consumers are not actively protecting their private information.

Empirical studies on the privacy paradox confirm similar phenomena. Acquisti and Grossklags [25] details how consumers recognize the risk of privacy invasion but still share their private information for service benefits, and Rosenblum [26] indicated that only a small number of users had shared their social network profiles with only their friends. According to a study on Facebook users, 87% of users are using default or open settings; although they are aware of options to protect their privacy, less than half of the users actually changed their settings to something else other than the default [27].

There are a number of theoretical explanations on the existence of the privacy paradox [28]. The majority of studies on privacy paradox have been conducted while rejecting the theory of reasoned action that is based on the uniformity of attitude and action, and there are studies that deal with "the paradoxical relationship between attitude and action intention," and "the paradoxical relationship between attitude and action." From the economic perspective, and based on the privacy calculus theory, the privacy paradox explains that users still provide private information for certain benefits despite high concerns about privacy. In theories of social sciences, the privacy paradox explains that SNS users voluntarily share private information for social capital, despite its conflict of privacy risks [29].

4.4 Strategies

4.4.1 Government: Activation of a local agent system for the oversight and investigation of global firms

The market monopolization by Google and Facebook continues to intensify. The EU ruled that Google had violated antitrust regulations on three cases and enforced high fines on it [30-31]. In Korea, it may be difficult to execute regulations for global platform firms. To resolve these issues, Korea introduced a system of domestic agents beginning on March 19, 2019, under Article 37-5 under the Act on Promotion of Information and Communications Network Utilization and Information Protection. ("Information and Communications Network Act"). The domestic agent system is a mandated assignment of domestic agents by providers of information and communication or similar services with no domicile or place of business in Korea, and global firms are typically subject to this law.

The agent is responsible for managing personal information, notifying and reporting cases of loss, theft, and leakage of personal information, and submitting related information when under administrative reviews by Korean regulatory authorities [32]. With the introduction of the Information and Communications Network Act, Google has appointed its agent, and Facebook and Apple each has Facebook Korea and Apple Korea, as their respective agents. As of November 2019, there have not yet been cases of reviews through the agents. For the domestic agent system for the global firms to be effective and achieve its original objectives, it is essential to regularly respond to citizens' complaints and regulators reaffirming their ability to quickly respond to reviews. This would allow the domestic regulators to secure real regulatory executability over global firms and ensure that the privacy of Korean consumers remains unviolated.

4.4.2 Government: Rapid increases to derivative data and the rising importance of their protection

The private information that can be formed through tracking can become more diversified than it is currently. The definition of private information in Korea is recorded in relevant laws, such as the Personal Information Protection Act and the Information and Communications Network Act. According to Article 2 of the Personal Information Protection Act, personal information refers to information relating to a living individual that makes it possible to identify the individual by his or her full name, resident registration number, image, and so on. Article 6 of the Information and Communications Network Act defines personal information as information identifying a specific person with a name, a national identification number or similar in the form of a code, letters, voice, sound, motion picture, or any other form.

Although the definition of private information under GDPR is similar to the Korean definition, the concept of the online identifier was added in 2018. Online identifiers relate to the information provided by devices, applications, tools, and protocols, such as cookies and radio frequency identification (RFID) tags (GDPR, Article 30). Data will be produced in large amounts in increasingly varying sources.

With the introduction of innovative technologies and their application to the society, it is essential to focus on the protection and management of not only direct information for individual identification, but also information that can be used to indirectly identify individuals. Although the leakage of direct identifiers such as names and resident registration numbers lead to severe damages, the importance of protecting indirect information such as online identifiers and derivative data should not be overlooked.

4.4.3 Firm: Resolving discriminatory regulatory environment and accessing practical ability to execute on regulation

As a policy recommendation for resolving the regulatory issues in the data industry, this paper has mentioned the strengthening of oversight functions of the Personal Information Protection Commission and the formation of cooperative relationships between relevant government branches. However, when executing these essential regulations, it is vital to refrain from forming a discriminatory regulatory environment. Although domestic firms bear the responsibility of adhering to various regulations that exist in Korean law, some overseas firms are not bound by the same laws or the effectiveness of such laws may be limited in their cases, and thus overseas firms may be able to carry on their businesses in an unfair regulatory environment. Therefore, it is vital to revamp the regulatory system so that overseas and domestic firms are not placed within a discriminatory regulatory environment in the data industry ecosystem. This may require revising the regulations, strengthening oversight, and investigating private information.

4.4.4 Firm: Expand legal data usage boundaries for legitimate interest

As data firms excessively collect and utilize private information, often for purposes outside the actual provision of services, the situation has increasingly led to concerns of violating privacy. Although such a phenomenon happens both globally and domestically, it is vital to revisit why such issues occur. Under the understanding that the firm must utilize limited information to provide services to the individual, violating such regulations constitutes a violation of private information. The social paradigm changes with innovative technologies and consumers are receiving useful services. However, it may happen that the standards governing the

violation of private information have remained in the past. In other words, the limited scope of utilizing data, especially amidst changes in the society, may have led a number of firms to become unlawful. Therefore, it may be necessary to prepare the legal framework to logically process and utilize private information and expand the scope of utilizing private information.

Article 6 (f) of the European GDPR defines "legitimate interest." Although the domestic version of private information protection laws is very similar to the European GDPR, one difference is that under the domestic private information protection laws, a firm can only collect private information when the legitimate profits of the information processor are clearly prioritized over the rights of the information owner.

As the demand for protecting and utilizing private information continues to grow with the 4th Industrial Revolution and innovative technologies, one alternative to finding a balance between protecting and utilizing data would be to expand the standards of utilizing data by firms.

4.4.5 Individual: Implement an active form of agreement

The core method of protecting private information under domestic private information protection laws is consent. For private information to be protected via consent, the process of consent must be voluntary. However, for a global process, it happens that the individual is not in full command of the contents of the consent agreement. Moreover, it is also perceived as a mandatory step in utilizing services, and as such the individual rights are not being protected.

Under the European GDPR, 6 standards must be followed for processing private information, rather than the standard criteria of "consent," the regulations recommend the use of standards such as the fulfillment of a contract, adherence to legal responsibilities or fair profits [22].

As pointed out in the tracking and profiling case, the individual has a dubious level of perception towards data collection. Therefore, in collecting the information under consent, it is essential that such information is actively driven by the individual, and the development of consent should differentiate between the age of the individual or what the information will be used for. The active realization of the consent process can be achieved through methods such as manually checking the consent boxes, filling out the important sections, and confirming and testing the agreement that the individual consented to.

5. Discussion & Conclusion

This paper discussed the technology regulation policy and issues with framework of principal agent theory and in-depth case study. Our findings are as below.

First, three groups of policy actors were found in traking and profiling regulation policy. The key policy actors are divided into data firms (Google, YouTube, NAVER, Apple, Amazon, Kakao, etc.) and the government (Ministry of Science and ICT, Korea Communications Commission, Financial Services Commission, Ministry of Justice, Korea Internet & Security Agency).

Second, three main regulatory issues were analysed for each parties. Firstly for firms, invading and individual's privacy and market and data monopolization by global firms were found. For individual, privacy paradox issue were emerged.

Finally, the response strategies were suggested for government, firms, and individual, and whole ecosystem of data industry. For government, we suggest two points; one is activating a local agent system for investigating global firm and another is enhancing to protecting policy from the increasement of derivative data. For firms, resolve the discrimination of regulation and

acces of excuting regulation, expansion of fair profit of data usage were suggested. For individual, implementation of active for of agreement was suggested. For data economy ecosystem, the concept of spreading “data as labor“ was suggested. Table 3 summarizes main discussions of this paper.

This study has selected case studies on regulatory issues that may occur between key stakeholder of the data industry, which are the individual, the firm, and the government. Online customized advertisements through tracking and profiling cover the regulatory issues of the firm and the individual (B2C). Tracking and profiling technologies are often used for online customized advertisements. Tracking refers to a technology that tracks various user data in real-time; “cookies” are universally used to track user behavior, and excessive use and misuse of such technology leads to the invasion of one’s privacy. One essential issue is that of consumer profiling, which merges the data collected through the cookie and the member registration information.

Table 3. Summary of Analysis

Case	Regulatory issues	Response strategies
Tracking & profiling	(Firm) 1.Invading an individual’s privacy 2.Market & data mono-polization by global firms	(Government) Activating a local agent system for the oversight and investigation of global firms
		(Government) Rapid increases to derivative data and the rising importance of their protection
		(Firm) Resolving discriminatory regulatory environment and access to practical ability to execute regulations
		(Firm) Expanding legal data usage boundaries for “legitimate interest”
		(Individual) Implementing an active form of agreement
	(Individual) Privacy paradox	(Ecosystem) Data as labor

This may violate the rights of anonymity of users who did not log in intentionally. Profiling is generally defined as collecting information on individuals or groups, analyzing their characteristics and behaviors based on the collected information, classifying individuals and groups into a certain range, and evaluating work capabilities, interests, and potential behaviors. When user profiling is combined with a “third-party cookie,” there are higher chances of invading private information. The regulatory issues that relate to this case include the comprehensive invasion of privacy rights by global data firms, market and data monopolization, and the privacy paradox for individuals. Invading privacy rights directly harms individuals.

If global data platform firms such as Google and Facebook excessively collect user behavior data through cookies and related technologies, the individuals will be faced with issues such as information leakage and invasion of privacy. The reason why market and data monopolization by data firms constitute regulatory issues is that the response of the monopolizing firms become different after their market monopolization, and the consumers cannot take meaningful action against decreasing service quality due to the lock-in phenomenon. Along with these issues, individuals face the privacy paradox.

Our study derived practical policy recommendations in dealing with complicated regulatory issued in data industry. Moreover, we extended the application scope of principal-agent theory model in data policy with a qualitative and descriptive approach.. This approach can be useful in all industries related to the fourth industrial revolution.

Recently in January 2020, the national assembly of Korea passed three bills for ameliorate the data related regulation for enhancing the data economy, which was the pending issue over a year. Three bills of data

regulation will allow the use of personal information with concealing the provider's identity. Along with these three bill, we hope that our study can suggest a guidance to reconstruct the reasonable, and adequate data regulation with the balance of two conflicting aims: protection of personal data and promoting data economy.

REFERENCES

[1] T. Symons & T. Bass. (2017). *Me, my data and I: The future of the personal data economy*. London: DECODE, Nesta. Retrieved October 22, 2018 from https://www.decodeproject.eu/publications/me-my-data-and-ithe-future-personal-data-economy.

[2] M. Micheli, M. Blakemore, M. Ponti & M. Craglia. (2018). The Governance of Data in a Digitally Transformed European Society. *Second Workshop of the DigiTranScope Project, European Commission*, 2018,

[3] H. Y. Kang & H. Y. Kwon. (2019). Policy Suggestions on Personal Data Utilization by Analyzing Domestic and International De-identification Policy. *Convergence Security Journal, 19(1),* 41-48.

[4] H. Ko & Y. Im. (2019). *Data Ownership,* Pakyoungsa : Seoul.

[5] D. H. Guston. (1996). Principal-agent theory and the structure of science policy. *Science and Public Policy, 23(4),* 229-240. DOI: 10.1093/spp/23.4.229

[6] D. Braun & D. H. Guston. (2003). Principal-agent theory and research policy: an introduction. *Science and public policy*, 30(5), 302-308.
DOI: 10.3152/147154303781780290

[7] R. Gauld. (2007). Principal-agent theory and organisational change: lessons from New Zealand health information management. *Policy Studies, 28(1),* 17-34.
DOI: 10.1080/01442870601121395

[8] T. P. Hagen. (1997). Agenda setting power and moral hazard in principal-agent relationships: Evidence from hospital budgeting in Norway. *European journal of political resea*rch, 31(3), 287-314.
DOI: 10.1111/j.1475-6765.1997

[9] Ministry of Science and ICT (2019), *Key Findings from 2018 Data Industry Survey.*

[10] Chunlei Tang (2016), *The Data Industry: The Business and Economics of Information and Big Data*, NY: John Wiley & Sons.

[11] Korea Internet & Security Agency (2018.03), *Report on overseas private information protection trends.*

[12] Korea Data Agency (2018) *White paper on data industry.*

[13] K. J. Arrow. (1985), "The economics of agency," In Pratt, J. W. & R. J. Zeckhauser (eds.), *Principals and Agents: The Structure of Business*, Boston, MA: Harvard Business School Press, 37-51.

[14] Gerber, Brian. J & Teske. Paul (2000). Regulatory policymaking in the american states: A review of theories and evidence. *Political Research Quarterly*, 53(4), 849-886.
DOI: 10.1177/106591290005300408

[15] Hwang. (2005), Principal-Agent Relations in the Policy Process: Reinterpreting the Formation Process of the "Drug Prescription & Dispensing Separation" Policy. *Korea Policy Review 14(4),* 29-57.

[16] Pavlou, P. A., Liang, H. and Xue, Y. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective," *MIS Quarterly*, *31(1)*, 2007, pp. 105-136.
DOI: 10.2307/25148783

[17] S, Lee. (2017), Contents and implications of guidelines for online customized advertisements, *KISO Journa*l.

[18] Lee, I. (2017) *Study on Development Methods of Personal Information Protection in Korea*. Personal Information Protection Commission Research Report.

[19] Park, N. (2017). *A Legal Analysis of the Profiling Provisions in the EU GDPR.*

[20] European Union (2016), REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[21] Google and Facebook advertisements have it too easy, targeted by the EU(2017.01.12.) *JoongAng Ilbo.*

[22] Jung, I. et al. (2019), The Analysis of Industrial Ripple Effect of GDPR and Issues in Innovative Technologies, *STEPI Insight*

[23] 3 in 10 World Citizens Are on Facebook"(2019.04.25.), *Statista.*

[24] 10 years of Facebook... 10 services that are now no longer in service (2014.02.03), *ZDNet Korea.*

[25] Acquisti, A., & Grossklags, J. (2005), Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3(1), 26-33.
DOI: 10.1109/MSP.2005.22

[26] Rosenblum, D. (2007), What anyone can know: The privacy risks of social networking sites. *IEEE Security & Privacy*, 5(3), 40-49
DOI: 10.1109/MSP.2007.75

[27] Govani, T., & Pashley, H. (2007), *Student awareness of the privacy implications when using Facebook*,

[28] Barth, S., & De Jong, M. D. (2017), The privacy paradox-Investigating discrepancies between expressed privacy concerns and actual online behavior-A systematic literature review. *Telematics and Informatics*, 34(7), 1038-1058. DOI: 10.1016/j.tele.2017.04.013

[29] J. Kim et al. (2018), *Study on information privacy paradox, 2018* NAVER Privacy White Paper.

[30] Google Fined Record $2.7 Billion in E.U. Antitrust Ruling(2017.06.29.), *The New York Times.*

[31] E.U. Fines Google $5.1 Billion in Android Antitrust Case (2018.07.18), *The New York Times.*

[32] 'Domestic Agent system to come online' Survey of value-added telecommunications service providers is reverse discrimination for domestic firms (2019.09.22), *Law Times.*

이 유 현(Youhyun Lee) [정회원]

· 2017년 1월 : 파리 1대학교 팡테옹-소르본느 박사 Ph.D. in Legal Science, University of Paris 1 Pantheon -Sorbonne)
· 2019년 12월 : 국회입법조사처 입법조사관
· 2020년 3월 ~ 현재 : 한남대학교 행정·경찰학부 조교수
· 관심분야 : 정부규제, 에너지 및 환경정책, 비교행정, 정책분석과 평가
· E-Mail : valerie315@hnu,kr

정 일 영(Ilyoung Jung) [정회원]

· 2014년 8월 : 뉴욕주립대 경영학 박사 (Ph.D. in Operations Management, State University of New York at Buffalo)
· 2014년 9월 ~ 현재 : 과학기술정책연구원 연구위원
· 관심분야 : Digital healthcare, Data policy, Science and Technology innovation
· E-Mail : iljung@stepi.re.kr