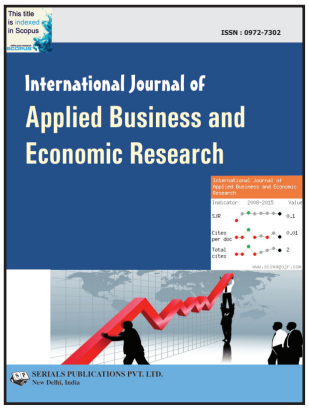

International Journal of Applied Business and Economic Research

ISSN : 0972-7302

available at http: www.serialsjournal.com

Volume 15 • Number 14 • 2017

Data Usage and Data Protection: Is it Possible to Pursue Both?[1]

Kiwhan Kim[2] and Sangoh Yun[3]

[1]*This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (NRF-2014S1A3A2044645).*

[2]*Professor, Department of Public Administration, Seoul National University of Science and Technology*

[3]*Corresponding Author, Professor, Department of Public Administration, Dankook University*

ABSTRACT

Despite public agencies' increasing commitments to and policy efforts for releasing and utilizing data, little is actually discussed about the use and value of personal data in both public and private sectors. This is probably because data security and privacy protection issues have taken up more policy attention than has data use. Presuming that data have value when they are used, not when they are protected in a safe place, this study tries to answer the following questions: (1) Why should personal data be used, and how should such data use be processed? (2) What are the exemplary cases of data use in developed countries, and what are their implications? and (3) Is it possible to achieve both data use and data protection in the personal data area, and if so, how? To answer these questions, this study investigates examples of excellent personal data usage from two developed countries. After reviewing two personal data use policies, comparisons and some policy implications are suggested.

Keywords: Data Usage, Data Protection, Smart Disclosure, Midata.

1. INTRODUCTION

We are rapidly moving toward a "digital era" in which a variety of unprecedented data are generated, transformed, and analyzed in multiple ways. Traditionally, personal data have been the target of protection against illegal data disclosure and fraud, which drives more attention to "protection" rather than "utilization," especially in Korea. In fact, Korea has one of the highest levels of governmental regulation in terms of personal data protection in the world. Strict regulation toward data protection results from their vulnerability to the risks that ensue due to inappropriate and illegal data usage. Personal data protection is particularly important because personal data are more highly exposed to illegal data disclosure and privacy intrusion

than any other kind of data. However, risks about privacy and concern for data protection do not necessarily justify accumulating but not utilizing personal data. Data are not generated and stored in order to be protected. Data have value when they are used, not when they are accumulated without anything being done with them.

Particularly since Korea does not have any explicit governmental policy to drive personal data to be used, we had to look outside the country and review foreign cases in which personal data are utilized in more active way. Smart Disclosure in the U.S. and midata in U.K. provide excellent examples of that.

In order to compare and analyze two international data-usage policies and draw policy implications, this analysis reviewed official reports, documents, and official directives published and/or promulgated by governmental agencies, international bodies, and academic institutions as well. Related websites are also referenced.

Korean governments have made data protection a higher policy priority than data usage, presuming that the value of privacy protection is something not to be challenged by any other values. This argument has also been dominant in academia. Previous literature sees the relation between data usage and data protection from a win-lose rather than a win-win perspective (Margetts, 2013). This trade-off perspective argues that enhancement of data protection results in limitations on data use, and vice versa. It is not difficult to find previous studies focusing on personal data protection rather than personal data use in a variety of academic areas, such as legal studies, social science, and natural science. Legal studies point out the importance of laws, rules, and regulations to protect individual privacy in the data-economy era (Rubinstein, 2012; Podesta, 2014; Krotoszynski, 2015). Scholars in public policy suggest that governmental decision-making is needed in reaction to individual data intrusion and privacy infringement (Richards, 2014). In technical and engineering fields, studies and recommendations on security and cryptography have also been prevalent (Executive Office of the President, 2014).

While there have been few studies insisting on the value created by data utilization specifically in academia, reports and documents published by business communities such as the World Economic Forum or business consulting groups have begun to emphasize the value of personal data (WEF, 2013).

In contrast to the research mentioned above, Culnan and Bies (2003) tried to see the relations between data use and data protection with more comprehensive lenses, such as those of the corporate perspective, activist perspective, and centrist perspective. First, the corporate perspective is more concerned with data use than with data protection, demonstrating that when enterprises, as primary actors for economic growth, are prohibited from accessing personal data about consumers, neither market efficiency nor social responsibility can be achieved. Second, the activist perspective, by contrast, takes a negative stance toward collecting and utilizing personal data. Its proponents argue that without regulation and control, personal data can be available to anyone for any purpose, which eventually results in privacy violation and social harm. Lastly, the centrist perspective, as its name suggests, takes a middle position between these two. Thus this perspective proposes that consumers' choices on data usage and corporate access to personal data should balance each other. According to proponents of the centrist perspective, both reasonable corporate access to personal data and consumers' legitimate right to their privacy are (and should be) achievable.

In association with the centrist perspective, this study contributes to the existing literature in following ways. First, despite the relatively pessimistic tone of the previous literature on personal data use, this study

concentrates on the necessity of data use rather than data protection. Second, unlike previous studies, this paper reviews exemplary foreign cases in which personal data are actively utilized in the public as well as private sectors, and also tries to draw implications by comparing those two cases. Lastly, through case analysis, this study finds a balanced relationship between data use and data protection that may provide policy suggestions in applying the data-use policies to other countries.

Our three research questions are as follows:

(i) Why should personal data be used, and how should such data use be processed?

(ii) What are the exemplary cases of data use in developed countries, and what are their implications?

(iii) Is it possible to achieve both data use and data protection in personal-data areas, and if so, how?

The paper is structured as follows: First, it presents the significance of data usage in both the public and private sectors. Second, it describes the key concepts and new perspectives on data usage that provide theoretical background for this study. Third, foreign cases of data usage are reviewed and compared with each other. Finally, conclusions and policy implications are presented. The paper closes with the limitations of the study and suggested avenues for future research.

2. THEORETICAL FRAMEWORK

Personal data are defined as data created by and about people, encompassing volunteered data (e.g., social network profiles), observed data (e.g., location data when using IT devices), and inferred data (e.g., credit scores) (WEF, 2011). Whereas volunteered data are created and explicitly shared by individuals, observed data are captured by recording the actions of individuals, and inferred data are data about individuals based on analysis of volunteered or observed information.

When it comes to sectors where personal data are used, they are divided into two: one is public, the other private. In the public area, governments can provide individually customized public service by using personal data in areas such as welfare, education, safety, and transportation. For example, police departments can provide locally customized public-safety service by using crime statistics, incidents data, and criminals' personal data in a particular local area.

In contrast, in the private sector, data usage empowers people to make rational decisions in the marketplace by using their own or others' data in a safe way. For example, private firms provide customer-oriented or individually targeted marketing data to any customers or potential customers, and customers themselves can increase their own utility by accessing these data. The data that can be provided include things you purchased in the past, other related items that are purchased by those who purchased the same thing you purchased, items that you probably need based on your internet search records, and firms that you are probably interested in based on your preferences. In the private context, governments also can play a significant role in making the interactions between customers and markets function well.

Six major categories can be made according to data types and data-using entities (Table 34.1). Data-using entities, as mentioned above, can be public (e.g., governmental agencies), private (e.g., corporations), or individuals (e.g., customers or citizens). Similarly, the types of data used can be about products or services provided by governmental agencies, corporations, or persons who are either customers or citizens.

Table 34.1
Data Types and Data-Using Entities

Categories		*Types (contents) of data*	
		The Product or Service	*The Individual*
Data-using entities	Public Sector	Type I: Governments using data about public service	Type II: Governments using personal data
	Private Sector	Type III: Firms using data about products	Type IV: Firms using personal data
	Individuals	Type V: Individuals using data about products and/or services	Type VI: Individuals using personal data

Source: Modified from the original table shown in Executive Office of the President's National Science and Technology Council (2013), p. 11.

This study concentrates on three types—Type II, Type IV, and Type VI in Table 34.1—all of which are about personal data despite different entities using the data. In Type II, governmental agencies collect and manage data on individuals in order to enable customized public service to citizens in such policy areas as health or welfare policy. In Type IV, private entities collect and make use of personal data to make a profit and provide customized marketing as well. This is the private version of the customized access service of the public sphere mentioned above. Although Type IV emphasizes the relationship between companies and customers, governmental efforts are also needed as a safeguard, facilitator, or regulator in order to securely maintain the data-flow. Lastly, in Type VI, individuals utilize their own or other people's personal data that are available through governments and/or private entities. By using these personal data, individuals can improve the utility of their decision-making process in the market. As in Type IV, governments also can play a pivotal role by motivating the private sector to make personal data available to customers in an efficient and safe way.

When it comes to data use, two perspectives can be compared: the traditional perspective and new one. The new perspective on data use raises the following questions: (1) Why should personal data should be used? (2) What is the new role of the data subject? and (3) Why is it important to pursue both data use and data protection at the same time? (Figure 34.1).

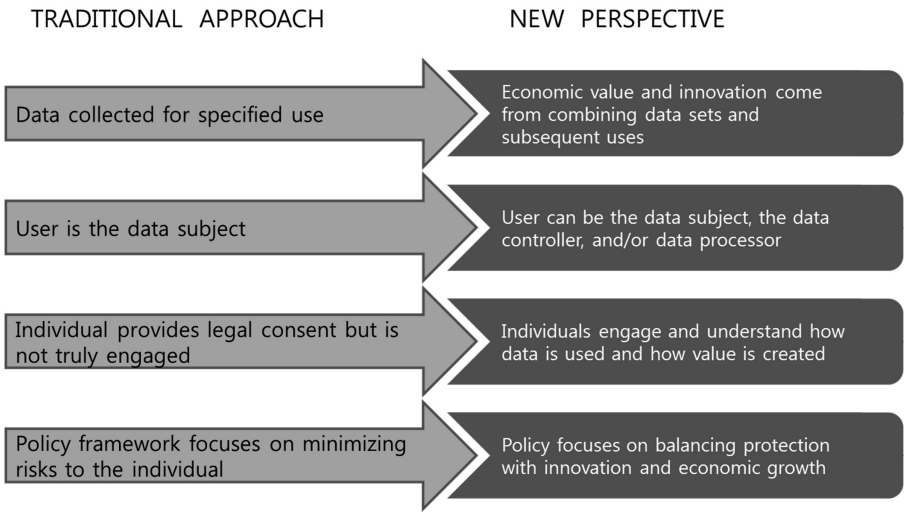

Figure 34.1: Comparison of traditional and new perspectives on personal data use
***Source:* Modified from WEF (2013), p. 7.**

People contribute to collecting data in multiple ways in their daily lives. Data are collected not only in traditional ways, such as filling out registration forms, but also in new ways, such as web browsing with internet devices, traveling with smartphones, and purchasing with credit cards. Sometimes people do not even recognize that their individual data are collected, processed, and transferred. As shown in Figure 34.1, stakeholders become actively involved in the data collecting and utilizing process. Individuals who used to be limited to being data subjects now act as data controllers and/or processors. Governments, in the new perspective, are supposed to be concerned with data use in a safe way because as more data are collected and transferred, privacy-related harm is more likely to occur. It is governmental policy that can balance data use and data protection.

3. DATA USE PROGRAMS

Smart Disclosure

In the U.S., President Obama made "Open Government" one of his top policy agendas by pledging his Administration to an unprecedented level of openness in government. "Smart Disclosure" is one of the most important action strategies that implemented Obama's Open Government agenda (Thaler and Tucker, 2013). Since then, a variety of federal agencies and presidential offices have done a great deal to make government more transparent and more accessible through task forces, directives, and action plans.

The purpose of Smart Disclosure is to empower consumers or citizens to make better-informed decisions. To do so, consumers need data about products and services, the agencies and companies that supply them, and/or consumers or citizens themselves (Table 34.2). Among these, personal data, which are the focus of this study, are provided securely to the individuals who are the subjects of those data and/or to others who want to use those data to make a better choice. For example, when consumers search for colleges, health insurance, airline flights, or energy providers, they can find the product or service that best suits their need via smart disclosure. Consumers can make better choices when they have information about the economic consequences not only of their own past choices but also the choices of others. Governments can use smart disclosure to discover the type of public service that is most accountable to citizens in areas such as health, education, energy, public safety, etc. Third parties can also analyze and reuse those data to help individuals make better and more tailored choices in the market.

Table 34.2
Types of Smart Disclosure Data

Types	*Definition*	*Examples*
Product or service data	Comprehensive information on the products and services being offered	Full pricing information, geographic availability, and complete listings for features, terms, and conditions of products
Data on providers	Information about providers to make informed choices	Financial position of the company, or whether other consumers have complained about the company
Individualized consumer data	Information pertaining to a particular consumer that is made available directly to that consumer	Individual's past purchases and product usage history

Source: Executive Office of the President (2011), p. 4.

Cases of smart disclosure can be presented in both the public and private spheres. In the public sector, for example, the Department of Education develops data sets and makes them available to help students and their families choose a college and decide how to finance their children's education. Specifically, the Department's College Navigator websites offer net price calculators that allow prospective students to fill out information about themselves in order to find out what other students with similar characteristics paid for each academic institution in the past.[1]

As an example of smart disclosure in the private area, payment card authorization and transaction information can be used to create patterns of card use, such as purchase size, frequency, and type of transaction (WEF, 2013). By using these data, card issuers can notify cardholders of fraudulent or suspicious account activity so that future transactions are blocked and potential losses minimized.

In order to make data use effective and efficient, several principles should be implemented (Executive Office of the President, 2011). First, smart disclosure should generally make information as accessible as possible to consumers through government or providers' websites. Second, data should be machine-readable, which means that the data are electronically stored to be easily processed and analyzed by computer. Third, the data should be available in a timely way so as to promote consumers' ability to make immediate decisions in the market. Lastly, agencies dealing with data should comply with laws and regulations to protect privacy against improper disclosure of personally identifiable information. In order to ensure these principles, the role of the government in securely operating Smart Disclosure is particularly necessary (Executive Office of the President's National Science and Technology Council, 2013). Governmental agencies can make the personal data they gather securely available to the data subjects, and can encourage companies to do the same. The government can also develop technological standards that become fundamentals for implementing smart disclosure. Furthermore, the government guides businesses to operate fairly and transparently in dealing with data collection and management.

midata[2]

While the U.S. Smart Disclosure was a key action strategy for the government's top priority agenda—namely, Open Government—midata was the key project in the U.K.'s 2011 governmental consumer empowerment strategy known as "Better Choices Better Deals: Consumers Powering Growth." The strategy gives consumers more control and access to their personal data, empowering consumers so that they are able to get the best deals for themselves in the market. Thus consumers can use the data to better understand their own consumption behaviors and patterns, as well as make more informed and utility-improving purchasing or consumption decisions.

Like Smart Disclosure, midata also emphasizes the role of government in driving economic transparency, along with businesses and consumer groups, in order to give consumers access to their personal data in a portable and electronic format (BIS and Cabinet Office Behavioural Insights Team, 2012). Although the midata program has proceeded on a voluntary basis among businesses in the U.K., the government adopted rules and regulations to make the program function properly. For example, through the Enterprise and Regulatory Reform Act, the U.K. government requires businesses to release necessary information to the public, and the Consumer Affairs Minister asks CEOs what companies are doing to make customers' data

1 https://nces.ed.gov/collegenavigator/

2 midata is originally written in all lowercase letters.

available to them (BIS, 2014). Additionally, the government works with third-party intermediaries toward managing data in a safe and secure way.

In order to effectively implement the midata program, the following principles should be established (BIS, 2012). While some of them are already mentioned in the Smart Disclosure case, others are not. First, data should be in reusable and machine-readable format in a standard form. Second, consumers should be able to access, retrieve, and store their data in a secure way. Third, standardization of the data storing and sharing process is pursued across sectors. Fourth, once requested, data are made available as quickly as possible. Fifth, any organizations should not restrict or hinder reusing data. Sixth, breaches of data security should be avoided by all organizations. Lastly, customers should be provided with clear explanations of how the data were collected and what they represent, and who to consult if problems are raised.

Like examples of Smart Disclosure, examples of midata are also abundant. The difference is that most examples of midata are found in the private sector. Leading businesses in which midata implements the release of customers' data back to customers are the energy, retail, mobile phone, and finance sectors. For example, telecom companies have analyzed customers' mobile phone usage records and behaviors. And third parties provided with those data then recommend the most appropriate rate to customers regardless of their current affiliation to a telecom company.

To sum up, midata is the U.K.'s project to encourage companies holding data about customers to release the data back to customers in a portable, reusable form. While the program is backed by governmental agencies (e.g., BIS), especially for data security, significant stakeholders are non-governmental actors, including customers, businesses, and customer advocacy groups.

4. DISCUSSION AND IMPLICATIONS

This study investigates and compares two data use policies and elicits implications that contributes to finding a balanced relationship between data use and data protection. Both the U.K.'s midata and the U.S.'s Smart Disclosure are well-known policy tools that help consumers make better-informed decisions and create more transparent, efficient markets for goods and services. The data provided by those two policies are about consumer products and services, the companies that supply them, and consumers themselves. They particularly provide "machine-readable data," so that information is expressed in formats which computer programs can analyze and combine in ways that are directly useful to consumers.

There are similarities—and differences as well—between midata and Smart Disclosure. The first similarity consists of the contents of personal data that are used in each open-data policy. Second, both policies empower individuals as consumers and the main economic actors in the data-ecosystem. Access to one's own information in usable data formats can make consumers' choices dramatically easier, and they increasingly have access to updated personal data and tools that analyze their own data to provide personalized recommendations about a product or service in both private and public areas. Third, both midata and Smart Disclosure pursued relatively non-regulatory and voluntary partnerships among companies as well as public-private collaborative relationships. Especially Smart Disclosure emphasizes the concept of an ecosystem in which various stakeholders interact with each other in beneficial ways. Fourth, in addition to data utilization, both policies are interested in data protection. They try to create and maintain a balanced relationship between utilization and protection via policy incentives and governmental regulations.

The first difference between the two policies is that the scope of personal data use is different. While the U.K. initiated midata mainly in private sectors such as markets, the U.S.'s Smart Disclosure is interested in both the private and the public arena. Examples of public data utilization refer to the policy area of environment, safety, and risk management. Second, whereas midata tries to empower consumers in economic decision-making in markets, Smart Disclosure relates to the Open Government agenda that was launched by Obama Administration. Third, when it comes to the level of governmental regulation, midata minimizes the role of government by letting the market function in its own way. Instead, the U.S. relies more on regulation by the federal government for personal privacy in the process of data collection, integration, and utilization (Table 34.3).

Table 34.3
Comparison of midata and Smart Disclosure Data

Comparison	*midata*	*Smart Disclosure*
Background and purpose	Customer-empowerment/Decision-making capacity improvement in market	Transparent and open government/Individual rationality improvement
Implementing agencies	BIS/Corporations/Customer groups	Office of Management and Budget/National Science and Technology Council/White House Office of Science and Technology Policy/Corporations
Laws and regulations	Non-regulatory or minimized governmental regulation	Relatively more regulatory than midata
Types of data used	Market data (financial, purchase, etc.)	Market data and public data (education, health, energy, environment, food, public safety, etc.)
Stakeholders	Individuals/Citizen groups/ Enterprises/Government	Individuals/Enterprises/Government

This study suggests several implications for implementing personal data use policy. First, although governments have tried to protect personal data in the past, they now need to play a critical role in driving data-utilization policy in the data era. To do so, a variety of incentives and regulatory tools should be developed by governmental agencies. Second, the value of data sets comes not only from the quality of the data they contain, but from their ability to be interpreted and used together with other data through data standardization and interoperability as well. Third, the data ecosystem should be run cooperatively by stakeholders in the system. Individuals, companies, and governments, which are the most important stakeholder groups, would particularly benefit from voluntary and non-selfish behavior in data production, management, and value creation. Finally, the data protection issue should not be neglected in discussing the importance of personal data use. By reviewing two exemplary cases, the present study demonstrates the possibility of balanced relations between data use and data protection. To accomplish this, governmental regulation (soft rather than strict), corporations' voluntary self-regulation, consumers' capability of controlling their own data, and consumers groups' awareness of privacy are suggested.

5. CONCLUSION

We are living in the data era. Every day more and more data are being generated that contain information about people and the choices they make. Two data-use programs discussed in this study enable people to access their personal data more easily than before. People who are able to apply those data to their decision-making can access new opportunities as customers in the market. Businesses use these data to develop

new products and services, and help consumers use their data to make better consumption decisions. These vibrant interactions will benefit the whole national economy. It is the government's work not only to motivate those actors to participate in the data-use process, but also to ensure that the data are collected and processed in a secure way.

For data protection, all parties must be concerned with the existing requirements and regulations (e.g., Data Protection Act of U.K) when handling personal data. The two data-use programs studied here have been considering issues of privacy and consent in relation to data collecting and data sharing. This data security has been a critical issue to both business and consumers, and the government has been working with participants of those programs to address the security issues.

Some limitations of this study should be presented. First, this study deals with a limited number of international cases of data-use policies, which raises the generalization issue of applying a policy to other countries. Since personal data-use programs have attracted international interest and influenced other data-related policies, a variety of social, economic, and legal contexts and constructs should also be studied, especially in benchmarking any program. Second, this study lacks social and economic outcomes or impacts of data-use policy. Thus future research can investigate the data-use policy effectiveness with empirical evidence.

References

BIS. (2011), Better Deals-Consumers Powering Growth. Department for Business Innovation and Skills. United Kingdom.

BIS. (2012), Midata Company Briefing Pack. Department for Business Innovation and Skills. United Kingdom.

BIS. (2014), Review of the midata Voluntary Programme. Department for Business Innovation and Skills. United Kingdom.

BIS and Cabinet Office Behavioural Insights Team. (2012), 2012 review and consultation.

Caplan, Robyn, Alex Rosenblat, and Danah Boyd. (2015), Open Data, the Criminal Justice System, and the Police Data Initiative. Data & Civil Rights: A New Era of Policing and Justice. Data & Society.

Culnan, Mary, and Robert Bies. (2003), Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues, 59(2)*: 323-42.

Executive Office of the President. (2011), Memorandum for the Heads of Executive Departments and Agencies.

Executive Office of the President's National Science and Technology Council. (2013), Smart Disclosure and Consumer Decision Making: Report of the Task Force on Smart Disclosure.

Jigsaw Research. (2012), Potential Consumer Demand for Midata.

Krotoszynski, Jr., Ronald. (2015), Reconciling Privacy and Speech in the Era of Big Data: A Comparative Legal Analysis. *56 Wm. & Mary L. Rev.* 1279.

Margetts, Helen. (2013), The promises and threats of big data for public policy-making. http://blogs.oii.ox.ac.uk/policy/promises-threats-big-data-for-public-policy-making

The National Archives. (2012), Government, business and consumer groups commit to midata vision of consumer empowerment. 04/05/2012. Department for Business Innovation and Skills.

Podesta, John. (2014), Big Data and the Future of Privacy. January 23, 2014.

Rubinstein, Ira. (2012), Big Data: The End of Privacy or a New Beginning? *NYU Public Law & Legal Theory Working Papers, Paper No. 357*.

Thaler, Richard, and Will Tucker. (2013), The Big Data: Smarter Information, Smarter Consumers. *Harvard Business Review*. January-February.

The White House. (2012), Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.

World Economic Forum. (2011), Personal Data: The Emergence of a New Asset Class.

World Economic Forum. (2013), Unlocking the Value of Personal Data: From Collection to Usage.