LEIDEN-DELFT-ERASMUS
CENTRE FOR BOLD CITIES
WORKING PAPERS

Dr. Suyoung Kim

Ethical Dilemmas of Using Big Data in Social Welfare Administration

A South Korean Case

WORKING PAPER #12

CENTRE FOR BOLD CITIES
Universiteit Leiden The Netherlands
TU Delft Delft University of Technology
Erasmus University Rotterdam

Ethical Dilemmas of Using Big Data in Social Welfare Administration : A South Korean Case

Suyoung Kim

Visiting Fellow of the LDE Centre for BOLD Cities

Associate Professor of Department of Social Welfare, Seoul National University

Big Data has now become vital in public welfare administration. Extensive data collection, classification, and processing are necessary for social service application, recipient selection, and service provision. This paper examines the ethical issues of using big data in the surveillance of welfare recipients through the case study of the South Korea's Social Security Information System (SSIS). The South Korean government digitalised the administrative procedures for public assistance in 2000 and has continuously upgraded the social welfare information system, strengthening welfare fraud tracking tools and adding pre-spotting functions for disadvantaged groups who can be potential recipients. However, surveillance over the personal data of marginalised people is inevitable when conducting such investigations.

Dataveillance via information systems reignites the old debate about the true nature of social welfare: Does it serve as a tool for social control or social care? Welfare dataveillance also compels us to revisit classic ethical questions: "If the purpose (detection of welfare fraud) is just, can the means (dataveillance) be justified?", "If a practice benefits society (pre-detection of people in need), should we tolerate its infringement on individual freedom (dataveillance)?"

Taking South Korea's SSIS as an exemplar case, this paper examines ethical concerns that social welfare administration may face while conducting big data surveillance. The first part of this paper introduces the brief history of the Social Security Information System of South Korea and reviews the controversial debates surrounding welfare dataveillance. Then, drawing on in-depth interviews with eight welfare officials in South Korea, it explores the ethical problems in data surveillance according to the framework PAPA (Privacy, Accuracy, Property, and Accessibility). Subsequently, it discusses three fundamental dilemmas facing social welfare in the digital era: dilemmas between Assessment vs. Analysis; Data vs. Reality; and Social control vs. Social solidarity. The conclusion suggests policy alternatives to address the ethical challenges of social welfare digitalisation.

Comment: The previous version of this paper was published in Korean (Suyoung Kim, 2016, "Social welfare ethics in the information age: Focusing on dataveillance through social welfare information system", Korean Journal of Social Welfare, 68(1), 193-224). This updated and translated version of the study is to be presented at a BOLD Talk at the Centre for BOLD Cities on 14th May 2024.

Introduction

Information Technology (IT) has now become vital in public welfare administration. Extensive data collection, classification, and processing are necessary for social service application, recipient selection, and service provision. IT has computerized the documentation works public officials used to do manually during the analogue era, enabling faster identification of welfare applicants' qualifications. Due to these advantages, many governments, such as the Netherlands, the United States, United Kingdom, Germany, Australia, and Sweden, have adopted IT in public welfare administration (Geoghegan et al., 2004).

In South Korea, the digitalization of public welfare system has been rapidly advanced with the implementation of the National Basic Livelihood Security, which extended the entitlement of public assistance to the working-age population in 2000. As young adults and the middle-aged group could apply for the basic living allowances, there was an urgent need to investigate recipients' assets more thoroughly to 'sort out' appropriate deserving recipients. As a result, in 2000, the Client/Server System was introduced, which was later advanced into the Saeol Intranet in 2007, the Happiness-Connect in 2010 and finally the Social Security Information System (SSIS) in 2013. Since 2015, the South Korean government has been updating the current SSIS by strengthening the welfare fraud tracking and adding a pre-detecting function for people in need (MOHW, 2015). The utilisation of information systems in public welfare is acclaimed in South Korea as it improves the work efficiency of public servants and is attributed to the accurate investigation of recipients' assets (Kang, 2010; Ham, 2013).

However, the digitalisation of public welfare administration raises ethical dilemmas regarding "dataveillance". Dataveillance refers to the "constant monitoring and identification of an individual or a particular group by using an information system (Clarke, 1988: 499)". Searching for welfare fraud and identifying at-risk populations through information systems are typical examples of big data surveillance applied to low-income populations. The government classifies "deserving" recipients from "undeserving" applicants by conducting data matching across various big data sources on income, assets, and family history stored within the SSIS. Since 2015, the SSIS has also been performing data analysis to pre-identify potential welfare recipients. These big data analysis procedures involve extensive collection and continuous monitoring of data on marginalized people. The crux of the issue lies in the lack of transparency: Marginalised individuals are largely unaware of the extent to which their information is collected, disclosed, shared, and utilised.

Digital ethicists identify dataveillance as a major ethical concern arising from digitalisation (Moor, 1985; Spinello, 2006). Indeed, dataveillance via information systems reignites the old debate about the true nature of social welfare: Does it serve as a tool for social control or social care? Welfare dataveillance also compels us to revisit classic ethical questions: "If the purpose (detection of welfare fraud) is just, can the means (dataveillance) be justified?", "If a practice benefits society (pre-detection of people in need), should we tolerate its infringement on individual freedom (dataveillance)?"

Nevertheless, reflective arguments on the ethical problems that digitalisation of social welfare may bring about have been barely done. In the beginning, social welfare scholars presented an optimistic view of the digitalisation of welfare administration because IT was expected to reduce the processing time of paperwork and enable communication with remote welfare users (Marlowe-Carr, 1977; Giffords, 1998). However, it has recently been pointed out that the implementation of IT is subordinating social welfare workers into coded algorithms and making welfare users be evaluated with numeric data rather than encouraging social welfare values based on humanism (Kreuger et al., 2006; Parton, 2008; Pithouse et al., 2009). These critics contributed to revealing the hidden side of information systems that have been praised for improving the efficiency of administrative work so far. However, there is still a more in-depth critique needed of the essential ethical risks of social welfare information systems.

Therefore, taking South Korea's SSIS as an exemplar case, this paper examines ethical concerns that social welfare administration may face while conducting big data surveillance. The first section provides

a historical summary of the information systems in the field of public welfare. Then, the second section discusses conflictual opinions surrounding dataveillance. The third section briefly explains this study's data collection and analysis methods, and the fourth section scrutinises the ethical limitations of dataveillance with South Korea's SSIS. The fifth section of this paper identifies fundamental dilemmas of social welfare in the informational age. Finally, it suggests policy alternatives to tackle the ethical issues of social welfare digitalisation.

A History of Social Welfare Information Systems

The history of personal data collection is inseparable from state control. According to Weber (1986: 901), a state refers to a supreme political organisation that exclusively dominates a definite territorial area and its inhabitants utilising exclusive oppression, unified authority, and various legislative and administrative apparatuses. A state can hold exclusive dominance over citizens because, roughly speaking, it ensures public order, security, and welfare. Giddens (1995) explains this as a legal "social contract" between the modern state and its citizens. The modern state is granted the authority to forcefully collect citizens' information related to residence, income, assets, or family history to draft and levy taxes in exchange for social security and public order. States have been developing administrative systems that collect and process public data for taxation, national security, and social welfare. Since the early 19th century, modern Western states have been investigating their citizens extensively through administrative institutions. Statistical information on citizens' ages, household types, income, residential environments, criminal records, occupations, and health conditions has been widely accumulated. Indeed, the term "statistics" has a root in "state." In this regard, Giddens viewed the information society as a characteristic of the modern state, rather than a recent phenomenon, as follows.

> *Modern societies have been 'electronic societies' longer than we ordinarily imagine and 'information societies' since their inception. There is a fundamental sense, as I have argued, in which all states have been 'information societies' since the generation of state power presumes reflexively monitored system reproduction, involving the regularised gathering, storage, and control of information applied to administrative ends. But in the nation-state, with its peculiarly high degree of administrative unity, this is brought to a much higher pitch than ever before (Giddens, 1985: 178).*

Early computers and internet networks were adopted to facilitate information collection and analysis for state governance. The very first computer, Colossus, famously decrypted German codes during World War II. Similarly, ARPANET, a precursor to the internet, was established by the US Department of Defence for sharing vast amounts of confidential information with remote bases. After the war, IT became widely used in state governance beyond national defence. In 1971, the US FBI created the first computer database containing personal information on 2.5 million ex-convicts. Other information systems for criminal records, like automated fingerprint identification systems, were developed and utilised around the world. Tax collection is another area where information systems are actively employed. Every government, including South Korea, conducts data matching to find tax evaders by collecting individuals' data on income, assets, financial activities, occupational status, and credit card transactions.

In addition to national security and taxation, social welfare is one of the core fields in which states have promoted digitalisation. Governments have initially deployed social welfare information systems to identify welfare frauds. In the 1970s, US initiatively experimented with data matching to find welfare frauds. Coincidentally, neoliberal welfare reforms were active in the West from the 1970s to the 1980s, when IT spread across. As a result, IT was naturally used to curtail welfare budgets. In 1981, President Reagan notably launched 'President's Council on Integrity and Efficiency to reduce frauds and misuses. The Council conducted a core project called 'Computer Matching Project' (Kusserow, 1984: 543). The Reagan administration stated in a law that state governments must enforce the Computer Matching programmes to receive welfare budgets from the federal government. Through this, about 500 matching programmes were developed and began cross-examining data on citizens' income, taxes, automobiles, criminal records, and banking and credit activities to track fraudulent recipients of various social services, including social benefits (Clarke, 1988: 504).

Whereas 'data matching' for identifying welfare frauds was the first generation of information system utilisation, 'data mining', which conjectures the recipient's patterns by analysing big data, has recently been in the spotlight. Prior to this, private enterprises had been analysing big data to understand consumers' behaviours since the beginning of the digital era. For instance, automobile insurance companies have calculated risk rates by types of drivers by using big data on automobile accidents and priced the insurance premiums of driver types appropriately (Davenport et al., 2010). Hence, McKinsey (2011) suggested that more efficient policy-making would be possible if the public sector also actively analyses and uses the citizens' big data. Indeed, governments are paying attention to data mining that discovers characteristics of particular population groups by combining the existing public data, going beyond simple data matching. For instance, in the mid-2000s, Germany's Federal Employment Agency launched an employment support programme using big data to estimate workers' tendencies and patterns and providing targeted employment services according to the types of workers. This programme is highly praised for significantly reducing the unemployment rate by 27%, from 4.4 million in 2003 to 3.2 million in 2010 (McKinsey, 2011: 59).

South Korea’s Social Welfare Information Systems

Current South Korea’s information system, SSIS was developed after several revisions of information systems introduced with the National Basic Livelihood Security implementation in 2000. Until 2000, public officials used to conduct the means-test of welfare applicants manually, screening every related document. However, with the introduction of the National Basic Livelihood Security, the total number of recipients reached 1.5 million, making it hard to investigate the means-tests and management of recipients through the handwork system. In 2000, the Ministry of Health and Welfare established ‘Client-Server System’, the first welfare-specialised information system. Client-Server System computerised the recipients’ data on income and assets, which had been filed in cabinets of municipal governments and local (village-level) community service centres, so that accurate investigation of the rapidly growing recipients could smoothly proceed. Followingly, the central government introduced the ‘Local Public Management Information System (called *Saeol* Intranet)’ that linked information between municipal and central administrations.

The detection of welfare frauds using the information system became earnest in 2010 with the introduction of the 'Integrated Social Security Information System (Happiness-Connect).' Happiness-Connect is a welfare-specialised information system which integrates 589 types of income, property, and service history data from 45 public institutions, including those on <Table 1>. Through the Happiness-Connect, more precise and detailed data matching for recipients has become possible. In 2010, the government prepared the legal ground for justifying data matching. According to article 23 of the National Basic Livelihood Security Act, the government can perform regular and random investigations on the data of all groups of recipients every year. During the investigation, social welfare public officials conduct data matching and monitoring of existing welfare service recipients. Then, they suspend or change the benefits once welfare frauds are detected. Finally, the latest information system, the 'SSIS (Pan-Government SSIS)' was launched in 2013, connecting information data of 360 welfare projects from 22 administrative departments. Through the Pan-Government SSIS, public welfare officials could share the recipients' histories of welfare programmes each administrative department has separately implemented and prevent double benefits and welfare frauds as a whole (MOHW, 2014a). The Happiness-Connect (original SSIS) and the Pan-Government SSIS are generally referred to as the SSIS all together because these two systems are closely interconnected.

<Table 1> Data Examples of Integrated Social Security Information System (Happiness-Connect)

Personal Data		**Service Usage History Data**	
National Tax Service	Income tax; Daily labour income, Labour subsidy; Business registration certificate; Business closure certificate; Business suspension certificate, etc.	National Health Insurance Service	Long-term care insurance for the elderly; Medical benefit qualification and comprehensive statistical services; Health insurance payment; Assistance devices for the disabled, etc.
Ministry of the Interior and Safety	Property tax; Acquisition tax; Union member occupancy right; National ID card photo; Resident registration, etc.	National Pension Service	Basic pension; Consignment service for the severely disabled; Support for the disabled, etc.
Ministry of Justice	Immigration data; Prison inmate data; Domestic residence certificate; Certificate of exit and entry, etc.	Social Service Manager	Electronic voucher service; Childcare service, etc.
Ministry of Land, Transport and Maritime Affairs	Cadastral information; Building ledger; sale right; Land and forestry ledger; Individual (communal) housing prices; Building management ledger; Vehicle registration, etc.	Ministry of the Interior and Safety	Financial reduction for basic living and the disabled; Welfare beneficiary certificate, etc.
The Supreme Court	Family relationship certificate; Building registration' corporate registration; Land registration certificate, etc.	Public Health	Public health care services, etc.
Others	Confirmation of military service; Industrial accident insurance benefits;	Others records	Health and Welfare Call Centre consultation record; Welfare Boucher

	Vehicle standard value; National pension benefit; Health insurance monthly remuneration, etc.		card service; E-kindergarten; Self-Support Service, Dream Start, etc.

Source: Korea Social Security Information Service (2012: 5-7)

Since 2015, the government has been preparing the 'Next-Generation SSIS (open called Next-Generation SSIS),' an upgraded version of the existing SSIS. One noteworthy aspect of the Next-Generation System is the strengthened function of detecting welfare frauds. To intensify the welfare fraud tracking and make data-matching easier, the government started to standardise the qualification processes of the government welfare programmes. Besides the data from public administration, it also utilises big data from internet blogs, online communities, or SNS in order to scrutinise potential welfare fraud cases (MOHW, 2015: 16). Moreover, another notable change in the Next-Generation System is the addition of a function to detect 'blind spots' of current public welfare. Because Korea's welfare services are based on voluntary applications, it isn't easy to offer public services unless an individual applies on their initiative. Therefore, the government has been trying to pre-detect blind sports (potential recipients at risk) by using citizens' information on power or water outages, case management records of community service centres, or reports from village leaders (Kim, 2015). In this context, the Next-Generation SSIS began to advocate ‘active’, ‘humane’, and ‘warm’ social welfare information system and suggested a function to pre-locate welfare blind spots as the core axis of the SSIS. In particular, with the enactment of the Enforcement Decree of the Act on the Use and Provision of Social Security Benefits and Search for Eligible Beneficiaries, the usage of personal data owned by public institutions to identify potential welfare recipients has been legal since July 2015. Through this, 24 big data of risky groups are newly integrated into the SSIS as shown in <Table 2>.

<Table 2> Newly-Linked Data for Detection of Potential Recipients

Data ---------- (Institution)	Data ---------- (Institution)
Households of power outage----------(Korea Electric Power Cooperation)	Rent deposit----------(Ministry of Land, Infrastructure and Transport)
Households of water outage----------(Waterworks Authority)	Monthly rent----------(Ministry of Land, Infrastructure and Transport)
Household of gas outage----------(Citygas)	Those eligible for extended benefits---(Ministry of Employment and Labour)
Health insurance arrears----------(National Health Insurance Service)	Unemployment benefits----------(Ministry of Employment and Labour)
Maximum copay price----------(National Health Insurance Service)	High-suicide risk groups - (Public Health Centres /Suicide Prevention Centres)
Annual insurance arrears----------(National Pension Service)	Suicide/self-harm attempters----------(Emergency Medical Centres)
Users of intensive home health care----------(Public Health Centres)	Residents/dischargers of living facilities -----(Ministry of Health and Welfare)
Users of premature infant support----------(Public Health Centres)	Students at risk----------(Ministry of Education)
Victims of criminal offences ----------(Korean National Police Agency)	Former welfare recipients ---------- (Ministry of Health and Welfare)
Victims from fire and disasters------ (Ministry of Public Safety and Security)	

Source: Kim(2015: 494)

As such, South Korea's social welfare information systems have evolved through many stages and paved the way for systematic and extensive investigation of welfare frauds and potential recipients, which have been the core problems of welfare services. Nonetheless, behind the SSIS, an important ethical problem lies – i.e. dataveillance of marginalised populations.

The Advent of Dataveillance

Surveillance refers to the act of constant monitoring and observance of a person or an object (Clarke, 1988: 499). After novels like Orwell's (1948) 『1984』 rose the alarm about the dystopian surveillance society, many scholars have criticised the surveillance systems of modern society. Particularly, Foucault (1979) criticised modern knowledge, like medicine and psychopathology, for dividing 'normal' subjects and 'abnormal' objects and constructing social surveillance system in which subjects (social majority) discipline and control objects (social minorities). Notably, he pointed out the 'panopticon,' devised by utilitarian Bentham for the efficient supervision of prisoners, as a prototype surveillance system of modern society. He denounced that the panoptic system was now universalised in current public administrative institutions, schools, workplaces, and hospitals, as well as prisons, under the pretext of efficient management.

Scholars influenced by Foucault have condemned the current information system using digital technologies as an electronic panopticon (Lyon, 1993). Whereas at Bentham's panopticon, a warder hid at the central tower and monitored prison cells, current information systems can more extensively manage individuals at a distance (Lyon, 1993). The noteworthy feature of surveillance through information systems is that those being watched are not only unaware of it, but also accept the monitoring without questions. Surveillance in the informational age targets nonmaterial data rather than a body of human being. Therefore, it is difficult to perceive the gazes of surveillance directly. Additionally, because people receive certain services from the state and enterprises in exchange of data, they take data provision for granted. For instance, we permit collecting personal data by internet platforms and allow tracking of our search history in return for the use of 'free' services like email accounts, blogs, or web drives. Although it increases the risk of privacy invasion, people have adapted to the data-service exchange without many criticisms due to its convenience. As a result, a South Korean information scientist Hong (2002: 101) indicated that a distinct characteristic of the electronic panopticon is the 'voluntarily cooperation' of those under surveillance in providing their own personal information required for surveillance.

While Foucauldian scholars have generally criticised surveillance systems, Clarke (1988) has analysed surveillance through information systems more practically. Clarke (1988:499) termed surveillance using an information system as 'dataveillance' and separated the dimensions of dataveillance into personal and mass dataveillances. Firstly, personal dataveillance is "an act of reviewing and analysing data of an individual who is suspicious or known to have problems" and is generally used to monitor criminals, accused, and suspected terrorists. On the other hand, mass dataveillance is "an act of monitoring on a specific group of people known to have, although unconfirmed, 'generalised suspicion'" (Clarke, 1998: 503). In the late 1980s, the early days of information systems, Clarke observed that mass dataveillance was used in the government's search for tax evasion and welfare frauds. In recent days, digital platforms, governments, and conglomerates are now widely conducting mass dataveillance to

conjecture members, welfare users, and consumers' behavioural patterns and characteristics by systematically analysing big data collected by information systems (Espoti, 2014; van Dijck, 2014).

The enablement of dataveillance cannot be possible without IT development. Surveillance on big data must be preceded by technological development for making vast databases of personal data, connecting each institution's databases, and integrating the shared data (Espoti, 2014). However, the development of IT did not directly lead to an activation of dataveillance. Besides the technological development, a spread of neoliberal ideology valued efficiency functioned as a background of the full-scale dataveillance (McLaughlin et al., 2002). In the 1980s, US President Reagan implemented computer data matching to identify fraudulent welfare recipients to reduce the welfare budget and increase financial efficiency (Kusserow, 1984). In addition to the US, other countries, including South Korea, have seen dataveillance within the field of social welfare as a way to reduce budgets and boost administrative work efficiency (Lee, 2012; Ham, 2013). Sociocultural climate is expanding dataveillance as well (Lyon, 1993). As society is fragmented and individualised, social trust between community members has decreased. There becomes a growing tendency to feel secure when surveillance is in place, and the members voluntarily agree to dataveillance, such as installing CCTV in schools, banks, public institutions, and every corner of the streets.

Pros and Cons of Dataveillance

Clarke (1988:498) argued that the Foucauldian perspective, which tends to interpret social control as the primary purport of dataveillance, should be avoided. It is because dataveillance not only contains the feature of a coercive form of social control but also has the feature of providing social security by preventing illegal activities and problems. Hence, he acknowledged the need to consider dataveillance's positive and negative aspects balanced instead of stubbornly refusing it. Indeed, the double-sidedness of dataveillance has been a debate topic since the introduction of information systems.

Regarding the advantages of dataveillance, it saves the cost of monitoring. Physical surveillance of human behaviour and communication is a labour-intensive act. Yet, because IT systems do dataveillance, it cuts down the labour costs for monitoring (Clarke, 1998:501). The second distinct aspect of dataveillance is the possibility of daily surveillance. Whereas only intermittent surveillance on suspicious individuals had been possible during the analogue era, automated information systems now allow continuous personal data monitoring (Marx and Reichman, 1984). Thirdly, data processing through computers is more accurate than manual labour. Because it is possible to collect and analyse a vast amount of data through computers, accurate results are more likely to be achieved (Davenport et al., 2010). Fourthly, it is highly advantageous that prediction and estimations about particular groups are possible. Information systems enable predictions on types of people and their behavioural patterns by employing data mining and profiling a tremendous amount of data. Through this, detection of tax evaders, social risk populations, and suspected criminals is feasible. The observation and analysis of the big data are expected to be a revolutionary contribution as it can foresee and resolve social problems by offering empirical evidence and shrewd grounds that we had not known clearly or had only suspected.

On the other hand, the risks of dataveillance have also been steadily pointed out. Firstly, scholars like Garfinkel (2001) criticised dataveillance for threatening privacy. Although dataveillance began with a just

purpose, such as crime prevention, it can surely result in an invasion of privacy. Secondly, it has been asserted that if dataveillance is not based on accurate data, it could produce severe damage to an individual (Mason, 1986). Although decreasing errors can lessen the cracks, victims are inevitable since there is no perfect information system. Thirdly, dataveillance has been receiving criticism because the surveillance occurs unconsciously. Many people readily agree to contracts stating that governments and IT enterprises, like Google, Apple, Microsoft, and Meta, can freely use personal data in return for services. But they merely press the 'Agree' button for private data provision rather than thoroughly read the contracts' terms and try to understand the dataveillance process comprehensively. Facebook (current Meta) would take advantage of this, revising the contract terms regarding providing and utilising personal data without notice to existing users (van Dijck, 2014: 205). Fourthly, another indicated risk factor is the monopoly of power of the institution operating the information system (Kim, 2008). Institutions with extensive personal data, such as governments or global platform companies, monopolise knowledge power in this information society. Terms like 'Big Brother' or 'Googlearchy' are innuendos of enormous knowledge power that a government and Google possess.

There are pros and cons to welfare dataveillance as well. There was a heated debate in the US in the 1980s, when dataveillance was first used for public assistance. Kusserow (1984), who led the establishment of a data matching program for public assistance in the US, emphasised the following advantages. First is the fair provision of welfare benefits and the reduction in the welfare budget. He pointed out that the most significant advantage of dataveillance is that it can punish those who unlawfully receive benefits and prevent the welfare budget from being used unnecessarily. Second, Kusserow saw that dataveillance would reduce the possibility of invasion of privacy. Because dataveillance through computers is unlike inspecting persons directly, it cannot be seen as a threat to the invasion of privacy. Furthermore, since governments have always collected recipients' data for means-tests for a long time, data matching through a computer cannot be an entirely new concept of surveillance. Fourth, he pinpointed the impartial nature of dataveillance towards recipients as another advantage. Within the analogue monitoring system, there was a possibility of public officials' prejudice to be intervened during the process of identifying fraudulent recipients. For instance, some public officials might believe that certain races, gender, age, or education level may have a higher potential of committing welfare frauds and thus stake out them intensively. Yet, because every piece of data within an information system is expressed through bits and numbers, a blind investigation is possible without prejudice against certain groups of people.

However, Shattuck (1984), a human rights activist, strongly opposed to dataveillance. Firstly, unlike Kusserow, he refuted that dataveillance invades privacy more cleverly than physical surveillance in which an inspector checks upon recipients' livelihood conditions from door to door. Generally, in-person visits and interrogations are carried out with the individual aware that they are the subject of investigation. However, within the dataveillance system, people are usually unaware that one's data is regularly monitored. Particularly, for dataveillance of recipients, data from various administrative and financial institutions must be collected and matched. In this data comparing process, each piece of information is inevitably utilised beyond the original intention of data collection conducted by each institution. Shattuck argued that this kind of data connection infringes individuals' discretion. Secondly, he asserted that another weakness of dataveillance is the violation of the presumption of innocence. Whereas Kusserow maintained that there is little room for bias in dataveillance, Shattuck condemned its implicit bias. Data matching conducted on all recipients is based on implicit speculation that all recipients can become

fraudulent. Borrowing Clarke's (1988: 153) expressions from earlier, mass dataveillance on all recipients is conducted to verify 'generalised suspicion'. Shattuck contended that this violates the presumption of innocence, a right for individuals to protect themselves and refuse random investigations without reasonable grounds. Lastly, another problem of dataveillance arises from the fact that data accuracy is not guaranteed. Unless the data is 100% complete and perfect, there exist discrepancies between the results of dataveillance and actual welfare fraud cases, leading to a waste of administrative power and generating innocent victims.

Nevertheless, as information systems became universalised, the early critiques on dataveillance disappeared. Nowadays, discourses on social welfare information systems mainly focus on the efficiency and convenience of administration, leaving the risks and criticisms unattended. The purpose of this chapter is to revive the critical debate on the ethical dangers of social welfare information systems that have been currently under-mentioned.

Analytical Framework and Data Collection

A pioneering scholar on computer ethics, Moor (1998: 266) observed that "the ethical problem of the informational age arises because there is a policy vacuum about how IT should be used." Although the advancement of IT actualises unimaginable tasks that were impossible in the past, it also creates social risks that need to be reflected. Moor thus viewed that an in-depth analysis on ethical issues, which the utilisation of IT will bring, should be preceded. Richard Mason (1986) then proposed four ethical topics, termed 'PAPA' model, that should be considered in collecting, managing, and distributing data through IT – Privacy, Accuracy, Property, and Accessibility.

① **Privacy:** Under what conditions, to what extent should personal information be disclosed? Who should protect personal information under the pressure of revealing it to others?

② **Accuracy:** Is the information accurate? Who is accountable for the accuracy of the information? What kind of rewards is possible for those who have lost or been damaged due to information errors?

③ **Property:** Who has the property over the information? How is the ownership of data distributed? What is the fairest way to disseminate information, and how much is proper for information distribution?

④ **Accessibility:** Under what conditions, who has the accessibility to the information? Is there a responsibility corresponding to the information access privileges? How should the damage caused by inaccessibility to information be compensated?

As the PAPA comprehensively embraces issues that must be addressed when dealing with data utilisation, this chapter goes through the risks of Korean SSIS around the themes of PAPA.

Sources of the case study come from the government's policy reports and internal data as well as the interview data of public welfare officials who use SSIS. As described in <Table 3>, eight welfare officials

participated in this study. The semi-structured interview lasted about 40 minutes to 1 hour and 30 minutes, discussing the four issues above. The interview data was collected according to research ethics, such as explaining the study purpose before an interview, confidentiality, and records by consent.

<Table 3> General Information of Interviewees

Code	Position	Administrative Level	Years of Service	Gender	Age
Official 1	Junior official	Town Community Service Centre	2 years	M	Late 20s
Official 2	Senior official	Village Community Service Centre	11 years	F	Late 30s
Official 3	Senior official	Village Community Service Centre	7 years	M	Late 30s
Official 4	Junior official	District Administration Office	6 years	F	Early 30s
Official 5	Junior official	County Administration Office	5 years	F	Mid 30s
Official 6	Senior official	County Administration Office	13 years	F	Early 40s
Official 7	Junior official	District Administration Office	8 years	F	Mid 30s
Official 8	Senior official	District Administration Office	15 years	F	Late 40s

Collected data were categorised and analysed using thematic analysis. Thematic analysis is a research methodology that analyses data by repeating the following process – ① familiarisation, ② identification, ③ indexing and charting, and ④ mapping and interpretation. The next section is the analysis of collected data, around the theme of PAPA.

Four Ethical Questions of Welfare Data Surveillance

1. Privacy: Does dataveillance invade the privacy of recipients?

With the enactment of the National Basic Livelihood Security, public assistance has become publicly declared as a welfare right, not a governmental favour for low-income people. However, to obtain the welfare right, a person needs to give up a certain extent of privacy rights, because an applicant ought to undergo a sorting out process whether one is a deserving recipient or not. A recipient cannot receive welfare benefits without the consent to disclose one's assets and income to the state. Indeed, like Kusserow's (1984) assertion, disclosing recipients' data for means-tests have been around for a long time. However, as shown in <Table 1>, IT advance enables the collection of a tremendous amount of personal data compared to the past. SSIS now collects daily income data as well as monthly income data. Like

explanations of public officials below, a world has become "where everything is known after the introduction of the information system (official #4)." The Ministry of Welfare and Welfare conducts regular investigations on recipients using the real-time information system. Also, to detect welfare frauds, the Board of Audit and Inspection of Korea has constantly matched various personal data such as automobile insurance, taxation reports, certificate of entry and exit, etc.

> *The system identifies individual data that has not been detected so far. In the past, we could only ask an applicant if they were working and couldn't help but trust their answer. If they say, "I am just helping my friend for a few days, not receiving money", we could not say anything or interrogate further about it. But, because real-time income is now updated on the system, detecting welfare fraud has been qualitatively improved (official #6).*

> *The Board of Audit and Inspection of Korea (BAIK) constantly distributes a list of suspicious recipients. For example, the BAIK screens recipients' certificates of exit and entry to check whether they are travelling abroad. Since the recipients travelling abroad might have more income undeclared the BAIK sends these data down to us and asks for inspection (official #8).*

However, this multilateral data matching has several limitations associated with privacy. Firstly, there is no standard for how far it is reasonable to collect and survey the data of recipients and their families as the scope of data that the system can technically collect is rapidly enlarging. Although it is technically possible to enter someone else's house, it is ethically unacceptable. In the same context, although it is technically possible to monitor all private data of recipients through the information system, there must be a principle regarding how much data can be ethically allowed for looking in. Nonetheless, there is a lack of public debate regarding this issue. For instance, in the first half of 2015, the Board of Audit and Inspection of Korea decided to add the income from the part-time jobs of recipients' middle and high school children into the total household income of recipients. Although the income from children's part-time jobs is too little and sporadic to be helpful to the household's livelihood costs, the Board considered it a hidden family income and cut back the welfare benefits of the family. The intensively detailed investigation of assets even made welfare officials reluctant as below.

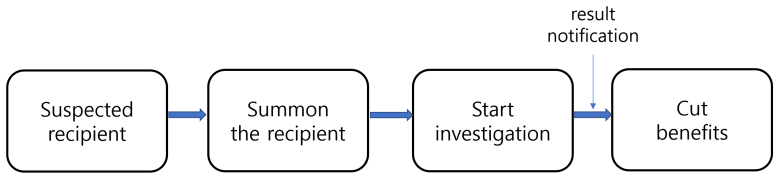
> *It is ridiculous that the child's pocket money neither parents nor the child remembers is viewed as an income and regarded as welfare fraud. I thought that was too harsh and hard to understand (official #8).*

Since the National Basic Livelihood Security prioritises the obligation of immediate family members (i.e. parents and children) for taking care of people in poverty before seeking public assistance, the government has also investigated personal data of immediate families of recipients, such as their level of assets and income. On top of that, because recipients could make excuses for disconnecting with their immediate family, the government has inspected recipients' bank account transfer history or call history. The investigations are separately taken place in addition to the regular confirmation investigations stipulated in the National Basic Livelihood Security Act. The regular and irregular examinations of recipients' data can be an excessive violation of the privacy of recipients and their families. Nevertheless, like a welfare official's remark below, the government strengthens dataveillance without clear principles. Arbitrary dataveillance as such cannot only endanger a recipient's privacy but also their right to welfare.

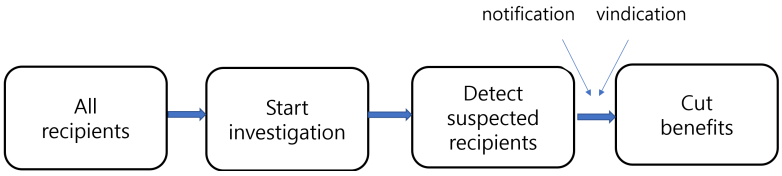
There is no distinction between the data in the investigation and the data that should be not. A few years ago, we collected recipients' call history too, but now we do not. As to bank account history, we still receive a year's worth of history. In the past, although there was only one transaction from an immediate family member, we would view it as substantial financial support. But, nowadays, the government tends to ease the standard after claimants. So, even if there is a transaction history, we don't admit it as an income transfer. But the criteria are uneven. This can change someday (official #5).

Second, the dataveillance conducted on all recipients unconsciously also violates their privacy. <Figure 1> compares the welfare fraud detection process in the analogue and digital eras. In the analogue period, when a person was suspected of welfare fraud, only the data of the very person was reviewed, and their benefits were reduced or suspended after the evidence of welfare fraud was discovered. However, dataveillance through an information system departs from a presumption of guilt on all recipients. In other words, with unconfirmed 'generalised suspicion' (Clarke, 1988: 503), the government steps a reversed process in which data on the entire population of recipients are reviewed and then fraudulent recipients are detected. As such, dataveillance has a problem in its premise by assuming all recipients as potentially fraudulent recipients.

[Analogue Period]



[Digital Period]



<Figure 1> Detection process of welfare fraud in analogue and digital era

However, the more significant matter is that the dataveillance is being carried out while the recipients are unaware of it. As explained by welfare officials below, when there was no information system, officials could directly listen to suspected recipients' stories and reflect on the investigation result. If a public servant was convinced by a recipient's difficult circumstances, the official could not confiscate the recipient's entitlement using discretion. Nevertheless, under the mass dataveillance system, recipients are first investigated automatically by the system and then notified only after being detected as fraudulent recipients, leaving no time to express their circumstances during the investigation. Now, the information system does not allow the discretion of officials.

There are people who are really pitiful among those detected as fraudulent recipients. They come to me appealing "please, save me." Yet we must process it as a welfare fraud regardless of how pathetic the situation is (official #4).

Recipients are unaware of anything before the results of the confirmation investigation come out. We only report to those whose entitlement statuses change once the investigation is finished. We send them a notification letter (official #8).

Of course, recipients who have been identified as fraudulent recipients are given a 60-day vindication period. Yet, because recipients have to establish their innocence by themselves when they are sorted out guilty, they are under pressure to reveal more private information. The information they bring to recuperate their welfare right is usually their 'private life' itself that cannot simply be abbreviated into 'public data.' The following are a few cases in which so-called fraudulent recipients recovered their right to receive benefits through vindication after being classified as illegal.

(Acknowledge that the recipient's child is not a biological child) *Although it has been detected that an elder living alone has a daughter on the family registry, the case was able to continue the benefit entitlement by clarifying that she is not a biological child.*

(Refusal of obligatory support due to mother's mental illness) *A disabled couple's benefit was suspended due to their daughter's income. But it has been confirmed that the family troubles became worse due to the female recipient's mental illness, especially after the daughter performed a kidney transplant and her health deteriorated. Through an investigation, the break in the family relationship was confirmed, and benefit provision remained.*

(Adopted son's refusal of obligatory support) *Although a recipient adopted a child and raised him until his adulthood, the son refused to keep in touch with his parents after marriage. The refusal to obligatory support was verified, and benefit protection remained (MOHW, 2011: 7).*

Although the above cases are summarised in only a few sentences, heart-breaking family stories are hidden between the lines. Suspected recipients are doomed to get emotionally hurt because they need to reveal their private stories such as family conflicts or the secret of birth, which they wanted to keep hiding, to reclaim their entitlement to welfare. They have to prove their misfortune to the state in order to receive benefits. The shame and wounds accompanied are also solely up to the recipients. The explanations by officials below indirectly show the stresses and pains recipients have to bear over the vindication process.

It is very pitiful. If recipients want to recover their benefit entitlements, they have to tell us that their family refuses the obligatory support. It may be difficult to acknowledge their family situation publicly. But they have to do it unavoidably (official #5).

I know a recipient whose relationship with her son was broken. For the objection to the dataveillance result, her son formally confirmed that he does not want to take care

of her smother. She finally got back her benefits but left lament in her mind; she told me, "Do I really have to do this to protect my benefits" (official #8).

The vindication procedures are very stressful, with recipients re-submitting various documents. The confirmation investigation ties up recipients with the dense network of data. They can never lie (official #2).

The pre-detecting function of the SSIS further violates the privacy of marginalised populations. As the criticisms that the SSIS was only utilised to cut off the number of recipients had popped up every so often, the government eventually set up a plan to add a function of pre-emptively searching for marginalised groups who can become potential recipients in 2015(MOHW, 2014b). The pre-detecting function of potential recipients can be viewed as active protection of welfare rights. However, when it comes to privacy, there is a higher risk of privacy invasion. In detail, the investigations for welfare frauds only target the present recipients who agreed to the provision of personal data. Yet, to find out the blind spots of welfare provision, the data of non-recipients are necessarily monitored without explicit consent. The data used to find potential recipients contains numerous sensitive details as presented in <Table 2> - such as a list of utility bills, social insurance delinquents, monthly rents and deposits, or suicide attempters of invasion of privacy.

Pre-spotting potential recipients with the SSIS underlies the premise that low-income groups are normally ignorant of public welfare services and will be delighted to hear that they can become recipients by any process. However, according to the Ministry of Health and Welfare (2009), 60% of those who did not apply for welfare benefits responded that they did not apply because they thought their applications would be disapproved, not because they were ignorant of welfare services' but because of 'strict means-tests' to them and their families. As a matter of fact, the mother and daughters of Songpa district, who killed themselves in poverty, had a history of being rejected after applying for public assistance. Although the eldest daughter had severe diabetes and high blood pressure, the younger daughter was a credit delinquent and cartoon artist, and the mother had to quit a restaurant waitress job because of a serious back injury, the two daughters were considered capable of working during the qualification examination. The key reason they were socially excluded was not the absence of welfare information, but institutional obstacles. This fact provides significant implications for reducing people excluded from social welfare. South Korea's public assistance conducts very exacting and picky means-tests and work capacity tests on individual applicants and their immediate families. No matter how precisely data mining of the SSIS can dig out low-income households, many applications of the households are to be later declined by the strict screening. Imagine a person, who attempted suicide due to poverty. After being detected through the SSIS and guided for public assistance, he applies for welfare benefits with last hope. But there is no guarantee that he will finally pass the selection process. He could fail to obtain the welfare right because his elderly parents are above the median income. In that case, the disappointment will be much greater than before.

Also, even though low-income groups come to know the fact that they can be a recipient, not all of them are pleased and grateful. As described below, welfare officials often meet people who express their anger at the government for examining their information without prior consent. Some even relinquish their welfare rights, reluctant to let others know about their desperate situations. Thus, some frontline welfare officials, who actually visited pre-detected potential recipients, took a sceptical stance regarding the pre-spotting function of the SSIS as it can hurt self-respect and dignity.

When we try to visit them, they show discomfort most of the time. Nowadays, there are very few people ignorant of welfare services. Some of those who do not apply is with very great pride. They hate us when we call. They ask, "what do you call me for? how come you know my number and information?" Do I confess we surveil their data? This answer might lead to even greater antagonism (official #7).

Of course, the poverty of disadvantaged groups should not be overlooked to protect their human rights. However, the point is that there is a social climate which stigmatises welfare reception and violates recipients' self-esteem. Rather than trying to find blind spots through dataveillance, the government need to make more efforts to improve the social atmosphere.

2. Accuracy: Is the investigation through the information system accurate?

The SSIS enabled more objective asset investigation compared to that of in the analogue era. As in the recollection of a welfare official below, before the information system, means-test largely depended "on applicants' statements" (welfare official #5). Even one could obtain an entitlement to welfare benefits if he/she talked well" to welfare officials (welfare official #7). Yet, after income and assets are tracked down using an information system, distinguishing between appropriate and fraudulent recipients comes to be done based on more objective evidence.

Before the National Basic Livelihood Security Act was enforced, proper and standardised investigations were made. Many elderly recipients still believe that front-line officials at community service centres could select recipients. They tend to speak emotionally. They want to express how difficult they are. Yet, now, we cannot decide based on their statements. The objective data from the information system is being used for recipient selection (official #5).

Nevertheless, dataveillance through the SSIS has several drawbacks in relevance to the accuracy of the data since not all the data managed by the information system are 100% accurate. Like the cases below, since the implementation of the SSIS, various computational errors have frequently occurred, such as death/birth reports not being updated on time, income from the past being summed to the current income, and some financial assets being omitted. Therefore, front-line officials used to find errors one by one and manually correct them.

The SSIS was incorrect a lot of times. There were not a few times when a dead person was reported 'alive' in the SSIS. When we called a recipient's house, her daughter answered, "no, grandmother was dead" (official #1).

Once the new income data is updated, the old one should be deleted. Yet, there are times in which both are added together. Then, this person exceeds the asset requirement (official #6).

Although not many now, there had been many significant errors with the updating functions of income and assets, such as the recipients' incomes were all shown 0 or some data remaining there even after being deleted (official #8).

Of course, it has been more than a decade since the inception of the welfare information system in South Korea, and thus the system's errors have been unrecognisably corrected. But, it isn't easy to 100% guarantee the accuracy of the data in the SSIS because the time difference still exists in data updates. To identify welfare frauds, the Ministry of Health and Welfare conducts a confirmation investigation in which they update all recipients' asset information and review all data. Nonetheless, like the complaints by welfare officials described below, there are many times in which the updated data are outdated. For instance, the aggregate incomes, such as income from daily work or irregular work, cannot be updated so quickly. So, we find that some recipients, who tend to take unstable labour, are not working and have no income at the time the previous payment is reflected on the SSIS.

> *The SSIS is updating public data with the latest information. However, there are times when we have to work again because the recent data is actually too old. For example, because income from daily work is updated later, we do cumbersome manual work to find and correct imprecise information one by one. A recipient needs to get a certificate stating that one is not working, and then we need to scan it as an attachment and input '0 won' by hand (official #5).*

Welfare officials and recipients take all the responsibility for the inaccurate data. Borrowing the words of welfare official #5, as stated above, it is quite common for them to work all night doing "manual work in which they find imprecise data and correcting one by one." Recipients also have to go through the annoying process of vindication because the SSIS has classified them as fraudulent recipients due to inexact data. The noteworthy point is that, as explained by the welfare officials below, about 80~90% of those labelled as fraudulent recipients are going through the process of vindication as they raise complaints that their data are inaccurate. As a result, there are only "less than 10% at the most" who are finally judged as fraudulent recipients after going through the vindication process.

> *After the system detects welfare frauds, 90% of 100 detected cases, roughly speaking, submit complaints. If they go through the relief of rights because they have usually lost contact with their adult children and are not aware of how much the grown children earn. 80% to 90% tend to recover their entitlement (official #6).*

> *Although cases may differ, only 20 instances seem eventually determined as welfare frauds if the SSIS detects 1,000 cases in the beginning. As for the last cases, officials and recipients undergo the relief of rights, which are additional workloads for officials (official #8).*

Indeed, if less than 10% of welfare frauds can be found with dataveillance, the effectiveness of the SSIS seems to be exaggerated. As a matter of fact, there are not a lot of cases where recipients intentionally embezzle the benefits. As stated by welfare official #5, "a lot of those who have been declined for welfare benefits fall back to the poverty line. They are disapproved not because they are substantially well-off but because their income level detected by the SSIS increased slightly above the poverty line. So nearly 80% of them reapply [for benefits]."

Ironically, those who commit intentional welfare fraud are rarely caught through the dataveillance system. Premeditated fraudulent recipients tend to grasp the means-test's loopholes and illegally use other people's bank accounts or hide their assets to avoid dataveillance. Because they are poor on data, the

system automatically classifies them as legitimate recipients. But, the data within an information system is only accurate 'within the system,' and does not fully reflect reality. As the below explanations by the officials, those who are wealthy yet do not have any income or asset under one's name can become a recipient, while those who have a shabby car or house under one's name cannot have the right to welfare, no matter how poor they are.

> *We can see all the publicly available data of recipients, such as how much money is at a bank and how much income they earn. Yet, think about it on the other side. The SSIS cannot detect when people store their assets under different names unless we see it directly since we receive information under the individual's name (official #1).*

> *It is tough to find cases with intentions, such as saving or buying an estate with a relative's name or getting an income from daily work by borrowing someone else's name. The police should investigate these parts; we administrative officials cannot figure it out well (official #8).*

Because of these reasons, intentional welfare frauds are usually found through neighbour's reports rather than the 'precise' information system.

> *It isn't easy to find out the substantive truth with public data. Most intentional frauds are disclosed by neighbour's reports rather than the dataveillance with administrative data (official #8).*

Lastly, dataveillance has a more significant defect concerning finding welfare blind spots. Theoretically, the most needed data to find potential recipients is an individual's income and assets and whether the individual has immediate family members above a certain income level. However, these data cannot be viewed unless the individual consents to disclose their financial information. As a result, the government has been tracking blind spots by using peripheral data, such as power and water outages, a list of those who did not pay their health insurance, or a list of tenants who pay very little rent. Yet, data mining using peripheral information turns out to be a waste of time because these instances do not directly imply the situations of poverty.

> *Some might assume the power is out and the water is cut because a person could not afford it. However, only 1 out of 100 households' water is cut off due to poverty. When you visit in person, many houses are empty ones where people don't live. It is a waste of administrative power to go through 99 households one by one to find just out one family in need. It is good to find out one desperate case, but it is also a very frustrating procedure (official #6).*

> *They are many people who do not pay their national health insurance, even if they can pay. It would be best if you didn't consider it naively. Some people do not pay on purpose. Some delude themselves, thinking that the government might raise the insurance premium once they regularly pay on time. But, the information system doesn't identify the behind intention and classifies them as those who need urgent intervention and help! (official #7)*

The Next-Generation SSIS is acclaimed for connecting vast amounts of data and predicting those likely to be under the poverty line with advanced statistical analysis. Nevertheless, the big data used in the statistical analysis only provides superficial information to guess individuals' financial conditions indirectly. Moreover, there are no data to predict the absence/presence of an obligatory provider (immediate family members above median income), which is an essential requirement for public assistance entitlement. Due to these aspects, many welfare officials are sceptical about the prospects of the Next-Generation SSIS and its possibility to revolutionise the current imperfect method of finding potential recipients. Some welfare officials even worry that there will be less time for offline outreach to their villages to uncover marginalised households due to the added computer work for dealing with the new data.

> *I cannot say that the SSIS is useless since some people in need are found through the system. But we (welfare officials) still need to look for them on foot. The data cannot cover all the welfare blind spots! But, if there are more and more data connected to the SSIS, we will not be able to go outreach anymore because we have to spend more time sticking to those data analyses to report to the superior institutions anyhow (official #7).*

> *You can mean a lot of things by blind spots. A person who committed self-harm can be viewed as one in a psychological blind spot. However, among those, many people are rich. Since we are looking for those who are in a financial blind spot, self-harm data does not fit well (official #8).*

Like this, dataveillance from an information system cannot be 100% accurate. Mason (1996) thus pointed out that one of the ethical considerations with an information system is providing appropriate compensation to those who suffered due to informational errors. However, the Korean government is only aiming to reinforce the accuracy of the SSIS as if 100% accuracy is ultimately possible. The damages of dataveillance, including the added work of officials due to inaccurate data, and the unnecessary vindication process that recipients have to undergo, are being neglected while the government adhere to the myth of accuracy.

3. Property: Who owns the data of the social welfare information system?

In 『The Age of Access』, Rifkin (2000) saw that the modern concept of *possession,* which refers to 'exclusive ownership over material properties,' became invalid in an information society. Non-material resources, such as data, information, and knowledge, have emerged as important assets in the informational age. Yet, exclusive possession of these is fundamentally impossible since they are easily reproducible. This is why disputes over intellectual property rights, patents, and plagiarism are never-ending. Like the ownership of intellectual property rights, the ownership of SSIS data can be controversial. Welfare benefit users submit consent forms to allow the provision of personal data for social services and benefits. However, the term 'provision' is a very ambiguous term. From a recipient's perspective, the personal data is only 'provided,' not taken away. Yet, the information is replicated and practically 'owned' by the government. The general meaning of 'ownership' involves not only the possession of tangible or intangible assets but also the right to utilise, distribute and delete (Lee, 2004).

Similarly, by being provided with personal data, the government has the de facto right to use, distribute, and dispose of personal data in the future, regardless of the information providers' (here, welfare users and citizens) intentions.

One of the first matters regarding the data property is the utilisation and distribution of data. As discussed before, a state possesses vast person data about citizens, such as birth, death, residence, military service, family relations, and income and asset data. During the analogue era of public administration, the distribution and utilisation of public data by government institutions would be difficult because they were stored as paper documents at each public administrative office which first collected them. However, as each institution's data were computerised and connected through the online information system, the data distribution to third-party institutions has become far more straightforward. As digitalisation advanced, the amount of data interconnected among institutions rapidly increased. The amount of data linked to the SSIS also increased 5.4 times from 2000 to 2000– from 218 data types in 27 public institutions to 1,183 data types in 45 public institutions in South Korea. Nevertheless, most of citizens are underinformed that their data are being transferred among public institutions and are used to detect welfare frauds and blind spots. For instance, as shown in <Table 2>, the Ministry of Health and Welfare brings diverse data sets from different institutions. It brings the list of households with power outages from the Korea Electric Power Cooperation (KEPCO), deposits and monthly rents from the Ministry of Land, Infrastructure and Transport, the users of home health care check-ups and suicidal attempters from public health centres, for potential recipient detection. Nonetheless, as explained by public officials below, those reported as houses without power, tenants, or suicide-risk groups are ignorant that their data is being transferred to the Ministry of Health and Welfare for detecting potential recipients.

> *Information like households with power cuts is brought from KEPCO, but we do not receive consent from those individuals. We are using data premising that permission from the prior institution is enough. So it can be problematic because we are not clearly telling individuals, "we also will use your data" (official #8).*

Private enterprises 'in principle' have more significant limitations when sharing consumers' data with a third party, even when the third party is their own affiliate. However, the data linkage between governmental organisations and public institutions is quickly done without any strict restriction, as if they are a single entity, the state. Of course, it is impossible in reality to go to every individual and ask for permission every time the data is transferred or used for new purposes. As a result, as explained by the above welfare official, receiving consent for the provision of personal data has always been done beforehand and just one time in a first institution. Nevertheless, although receiving consent beforehand is efficient and inevitable, the government must acknowledge that this method can invade the data ownership of citizens and deeply ponder whether the data connection is ethical before the SSIS dataveillance.

However, the government seems to be only interested in acquiring legal grounds to legitimatise dataveillance. It has not paid great attention to devising an ethical solution for protecting the data ownership of people. Article 38 of 「Framework Act on Social Security」 states that no information on any individual shall be held, utilised, or provided without the authority stated under the Act. At an instant glance, dataveillance seems to be carried out under strict principles. Yet, in reverse, it also means that possession, utilisation, and distribution of data are possible as long as it is 'legally stated'. For this excuse,

the Ministry of Health and Welfare (2014b: 5) has continuously added legal provisions within the Acts to allow the linkage and utilisation of relevant data from public institutions to facilitate the detection of welfare frauds and blind spots. But the legal provisions are just formal and perfunctory justification on dataveillance since they are only being mechanically added without many ethical considerations and public disscussion on data ownership. When amending the law provisions, it must be properly announced and elucidated to welfare users and the stakeholders. However, similar to Facebook's case (van Dijck, 2014: 205), the consent terms to provide personal data are being revised without offering the welfare users any public notice.

The second matter regarding data property is about its disposal. Data are intangible and therefore remain forever unless deleted. The vitality of data can be seriously deleterious to those who want to delete their past. Mayer-Schönberger (2009) thus conceptualised 'the right to be forgotten' and maintained 'data expiration date' to be implemented in a digital system, just like how a human memory system is oblivious. A right to be forgotten can be a way to strengthen the information rights of those recipients who wish to cover their complicated family relations, accidents, and former records of welfare frauds. However, there is no expiration date on the SSIS. As described by the official below, recipients do not have the right to delete the data or counselling notes that they provided in the first place. Hence, once offered, recipients' data are not disappeared but cumulated ever since.

> *Recipients can look up their information if they bring a national ID card and asks to check their income data. However, it cannot be deleted. Also, their counselling notes cannot be deleted either. It stays here forever, only being filed up (official #8).*

The absence of data expiration date can be a greater problem when investigating welfare fraud. This is because the record of being identified as a fraudulent recipient remains, and one can tacitly be blacklisted.

> *The histories of a recipient and their families are being saved. For instance, there was a daughter who grew up with a dad who was a recipient. After becoming independent and having a child, the daughter came to apply for childcare benefits. In the process, all the daughter's previous household histories would pop up. Since the father had committed welfare fraud in the past, the information also stayed on too (official #8).*

> *If a recipient's benefits have been suspended due to welfare fraud, that information remains. Although welfare fraud is not like a criminal record, everything is saved in detail on the SSIS's counselling note section. 80% of those classified as fraudulent applicants tend to reapply for benefits. Yet, because of the previous record, we look into them more carefully, scrutinising them twice three times instead of once (official #5).*

As a result, to prevent recipients' stigmatisation and ensure the right to delete the information, there is a need to clarify the period during which the government can keep a recipient's information. However, the current policies tend to suggest storing the data of recipients and low-income groups for as long as possible to investigate welfare frauds and blind spots. For instance, Choi et al. (2012: 105) recommended that the government is allowed to collect data for at least five years from those whose welfare applications was disapproved to find out potential recipients efficiently. Yet, this recommendation

requires careful consideration as requesting information on income, assets, and family relations from those not receiving welfare benefits can increase the possibility of invasion of privacy.

Finally, another question regarding the property of information is about the justification of data utilisation. The state has been using recipients' data without any restraints. Yet, Gert (1998) argued that for an act to acquire moral justification, the Act must be impartial. In other words, it is unreasonable to prosecute a policy that cannot be applied to everyone on particular individuals. Few people in the upper/middle class would allow continuous and meticulous monitoring of their private data, including income, assets, family relations, bank account transfer history, certificate of entry and exit, or call history, in exchange for a small amount of money. But, the state is asking for too much information from low-income groups in exchange for basic living costs. The government tends to take it for granted that marginalised people may and should endure continuous dataveillance since welfare benefits are paid to them. Yet, it cannot be morally justified that one's data can be treated cheaply just because one is poor.

4. Accessibility: Who can access the data of the social welfare information system?

Jonson (1997) believed that undemocratic features are inhering in the structure of an information system. Like a panopticon, individuals whose data is monitored tend not to access the information system, whereas those who conduct dataveillance can access the system and view the data. The same goes for the SSIS. The SSIS contains a tremendous amount of recipients' data, yet, the recipients, the information providers, are not authorised to access the system. As welfare officials below say, the information system can principally be viewed "by officials only" (official 8). Even public officials were strictly restricted from viewing data outside their work areas.

> *We can only access the information system. Not everyone can see it, nor the recipients themselves. We, the officials, can only access it (official #8).*
>
> *It is not that all public officials can access all of the recipients' data. Access to the SSIS sections is restricted even to officials according to the specific tasks in their charge (official #1).*
>
> *There are about 100~200 different sections of data within the SSIS network. We cannot access all that information. I only use the section I am responsible for. Accessing other parts is prohibited (official #1).*
>
> *Each official can access only the information in their responsibility. I never thought we could access excessive personal information (official #6).*

Indeed, as a sub-system of the SSIS, the government has operated a "Constant Monitoring System in Protection of Personal Data" to catch any officials going beyond one's access limit and searching other data sections. Once the monitoring system detects an unauthorised search, it immediately asks the official to explain the reason (MOHW, 2015: 57-58). This monitoring system is supposed to be used to protect the privacy of recipients from public officials. It is 'meta-dataveillance on dataveillance' or, in terms of Orwell (1948), the 'Super-Big Brother' supervising Big Brother. However, having Super-Big Brother is

not the most democratic way to protect recipients' data because recipients are still not given access. The monitoring system is for central government institutions to supervise the conduct of front-line public officials. Local officials are now in a "dreary" work environment because access to information is blocked in many ways. Official feel they are also a target of dataveillance by the SSIS, alongside recipients. It has created an atmosphere of social control all over the field of public welfare administration.

> *If I look at the information I am not accessible; a pop-up will suddenly appear on the screen, asking me to explain. While working at a village community service centre, An applicant came to apply for disability benefits. He said he also worked at a village community service centre. So, I looked up the applicant on the staff list of the SSIS. But, as soon as I looked up, a tab appeared on the network, asking why I searched the person. So, I had to explain why I did it. It freaked me a bit, like "How on earth did they know?" (official #7).*

> *Not only recipients are monitored, but we, officials, are also monitored. The work atmosphere is a bit dreary. I cannot help any of my peer's work. Because we log on to the network using our own certificate ID, I cannot log in at a different seat. If I access the SSIS with a different computer, the tab immediately appears, asking me to justify the reason since one person cannot be at two places once (official #8).*

As shown above, dataveillance using the SSIS has significant limitations. Regardless of the purpose, investigating welfare frauds and blind spots through the information system invades the privacy of low-income groups, and inaccurate data can harm them. Furthermore, recipients are not guaranteed ownership and accessibility of their data within the information system. Nevertheless, ethical dilemmas around dataveillance are rarely resolved by lessening the privacy invasion, increasing data accuracy, and administratively ensuring data property and access rights. The aforementioned limitations are inherently related to the more fundamental topic of "What social welfare should pursue in the age of information?" Hence, the following section will briefly examine ethical dilemmas around social welfare digitalisation. The discussion will firstly be on the roles of social welfare workers, the grounds of social welfare practice, and lastly, the orientation of social welfare.

Three Fundamental Dilemmas of Social Welfare Information System

1. Assessment vs. Analysis: What are the roles of social workers in the digital age?

First, social workers now have to navigate increasingly complex role conflicts compared to before. They must decide whether to evaluate based on the judgement of values or through analysis by the information system. Traditionally, the roles of social workers would involve both evaluating the demands of individuals and the scientific analysis for service provision. Therefore, as Choi (2014) highlighted, practising social welfare in the real settings is fundamentally fluctuating, complex, and unpredictable. It has therefore been assumed that social workers cannot solely adhere to manuals and rules, but must also rely on their reflective thinking and judgement of values. In the same vein, Kim (2005) argued that social workers are ‘value-grounded’ professionals.

> *Regardless of what the social welfare sector one works in, in order to solve a problem, social welfare workers must base their approach on 'values', rather than solely on 'science.' Moving beyond neutrality and objectivity, practising social welfare work involves identifying what is right and worthy through normative judgement and consensus (Kim, 2005: 124).*

However, with the ongoing advancement of digitalisation, the judgement of values, traditionally performed by social welfare workers, runs a high risk of being supplanted by computer system analysis. The Korea government has announced plans to adopt the "convenient and smart system," Next-Generation SSIS, over reliance on the "experience and knowledge of social welfare officials" (MOHW, 2015: 17). Objective computer analysis, conducted without subjective judgement or humanistic intervention, are seen more useful than human decisions. Nevertheless, the reason for employing social welfare officials separately from other public officials lies in the unique aspects of their roles – direct interaction with welfare recipients and the provision of services with flexibility. If the roles of social welfare officials become confined to merely verifying cases predetermined by the information system, the core principles of social welfare – reflective judgement and human interaction – risk being eroded.

Some people may think it is a distant future scenario. But if the role of social welfare workers continues to be marginalised by the information system, social welfare administration can be completely replaced by 'artificial intelligence' in some points in the future. As futurists predict, with the progression of digitalisation, the majority of human tasks will be performed by machines. In fact, in collaboration with major hospitals, IBM is currently developing an artificial intelligence, 'Dr. Watson,' capable of diagnosing and treating patients (Brynjjolfsson and McAfee, 2014: 120). Given the Next-Generation SSIS's emphasis on being a 'smart information system,' there is no assurance that a Social Worker Watson will not be trialled in the future. Additionally, alongside 'fairness,' the value of 'efficiency' is gaining importance in social welfare policies. The active adoption of IT in the American medical system, such as Dr. Watson, stems from a belief in its potential to enhance hospital profitability and efficiency (McKinsey, 2011). If commercialisation of social welfare intensifies and efficiency emerges as the dominant value in the Korean social welfare fields, there will be an increased demand for the adoption of superior and more recent IT technologies. As a result, with digitalisation becoming an unstoppable trend, social welfare workers – whether in the public or private sector – will lose their intrinsic roles.

Brynjolfsson and McAfee (2014: 241) from MIT, who forecasted The Second Machine Age, acknowledge that there are specific activities computers cannot perform – that are 'critique and reflection' and 'art and creation'. Although computers can reorganise and analyse existing data, they are incapable of making value judgements and creatively generating new ideas. This delineates the renewed roles of social welfare workers. As digitalisation progresses, social welfare workers should critically assess field issues and offer creative solutions. The role of social workers extends beyond accurately calculating benefits and providing services. If only these functions are emphasised, social welfare workers might have to cede their positions to a computer system capable of performing these tasks more efficiently.

2. Data vs. Reality: What should social welfare be based on in the age of information?

Secondly, when practising social work in the age of information, one can become confused about whether to prioritize 'data' or 'reality' as a primary criterion for judgement. van Dijck (2014) indicated that datafication has become a dominating paradigm in modern society. Indeed, human behaviours and

social activities are swiftly being transformed into quantifiable online data. Specifically, with the introduction of Web 2.0, aspects that could not previously be expressed in numbers, such as emotions, relationships, conversations, and symbols, began to be codified. As the simplest example, Facebook converts human relations, such as emotions like 'Like,' or making friends, into an algorithm. This datafication is based on certain ontological and epistemological beliefs that almost all human reality can be datafied. Echoing van Dijck's comment (2014: 199), these beliefs have created the myth of dataism, meaning that data can represent all human activities. People, devoted to dataism, are prone to feel despair and rejected when their number of Facebook's 'Likes' is low.

However, there is indeed a great gap between offline reality and online data. As mentioned earlier, not only is the accuracy of data managed by the SSIS unguaranteed, but it cannot fully represent the recipient's real situation either. A human's life is full of 'informal stories' that cannot be codified. Although the information system can provide relatively precise financial information, such as income and assets, reproducing informal descriptions behind the income and assets is nearly impossible. However, borrowing the cocepts of Parton (2008), the information system replaces 'social knowledge', such as the recipient's life and human relations, with 'informational knowledge', codified numbers. Instead of reflecting the recipient's in-depth psychological and environmental circumstances, informational knowledge represented in a series of numbers is only superficial and phenomenal. Nonetheless, the social welfare administration now heavily relies on numeric data provided by the information system. This causes social welfare administration to be based on data rather than the actual reality in which recipients live their lives. Social workers have learned that when practising social welfare, a client needs to be recognised as a 'person-in-environment'. The person-in-environment perspective requires a comprehensive understanding of the surrounding environments of people. The practitioners of social work should focus on the actual environments of recipients, not on tangible data. This value of social welfare should remain unchanged in the age of information.

3. Social Control vs. Social Solidarity: What should social welfare promote in the age of digitalisation?

Lastly, in the information age, social welfare is bound to make a pendulum movement between two natures: social control vs. social care. The nature of social control pursued in modern social welfare has been steadily criticized by scholars. For instance, Day (1981) demonstrated that social welfare has the function of controlling deviant behaviours of minority population, and Raynor (1985) indicated that social welfare serves the role of correcting crimes of social minorities in a less coercive way than judicial punishment. Garland (1985) also viewed social welfare as a component of the penal-welfare complex that controls deviance and crimes. Going beyond the micro-level social work practices, neo-Marxists have criticized that the welfare states possess the quality of social control as they address the labourer's complaints and have them comply with the capitalist order (Ginsburg, 1979; O'Connor, 1973).

However, social welfare policies, which originally aim to lessen crimes and social resistance, has created another type of crime – welfare fraud. Viewing welfare frauds from a criminological perspective, Tunely (2011) observed that welfare frauds were more rampant in societies that are aggressive towards people under poverty. In his view, excessive dataveillance over recipients is an expression of the aggressiveness. If the standards are too intensive, even a small mistake can be seen a welfare fraud.

Indeed, as categorized by van Stolk and Tesluic (2010:3), so-called welfare frauds include not only intentional fraud but also unintentional customer error, official error, and corruption committed by administrative officials. Thus, it is a wrongful attitude to assume that all welfare frauds occur due to the recipient's immoral conduct. This attitude will only aggravate stigma and prejudice against recipients.

Of course, even so, inappropriate welfare allocations anyway should be reduced whether the actual intention is fraud or error. Nonetheless, dataveillance is not the only solution for welfare fraud reduction. According to Martin and his colleagues (2009), the deterioration of societal structures, such as growth in unemployment and poverty rates, is the reason behind the increase in welfare frauds. Furthermore, excessively stringent investigation of assets can be another reason. The reason why there are many fraudulent recipients in countries such as the U.S., U.K., and South Korea is that the screening process for social assistance is too thorough and intricate. As such, welfare frauds caused by structural and institutional factors would not decrease, no matter how intensive dataveillance are conducted. Rather, if dataveillance is intensified, fraudulent recipients would increase since the data system will spot even the smallest increase in income and detect more minor income and assets discrepancies.

At this point, we need to recall another feature of social welfare – social solidarity. Social welfare was not implemented solely to control the poor population. Traditionally, social welfare was established and developed for the recovery of social solidarity and community (Titmuss, 1963). For social solidarity, the public has agreed to pay taxes for welfare policy and to join social insurance for liability and redistribution of income. In fact, the reason why many citizens, including conservatives, are enraged with welfare fraud is that they believe it threatens the social community built on trust (Haidt, 2012). Similarly, the reason the poor population, who have been pushed into blind spots, cannot be ignored is that they are part of the social community as well. If it is agreed that social solidarity is another aim of social welfare, the direction of SSIS should be readjusted towards a way that protects social trust. Overly stringent investigation on assets and income also need to be ameliorated if it rather undermines social trust and community building. Without such considerations, it would be difficult for the government to avoid criticisms that the SSIS only serves the purpose of social control, not social solidarity.

Conclusion

So far, ethical issues that social welfare has confronted in the informational age, specifically around dataveillance using SSIS, have been discussed. This paper is an introductory study on social welfare information ethics and is insufficient to provide specific policy implications. Hence, the conclusion will be substituted by briefly suggesting the policy directions that social welfare digitalisation could take in the future. First of all, there is a need for cooperation between engineering and social welfare when developing the SSIS. Big data system in social welfare should be developed by considering not only "What is technically possible?" but also "What is ethically appropriate?" Recently, the integration of natural science and social science has been trending. IT enterprises are requiring employees to adopt not only engineering knowledge but a humanistic imagination as well. However, there is still a great gap between those two worlds in the field of public administration in South Korea. In this situation, it is hard to anticipate the establishment of SSIS with a balance of ethics and technology. If there are no experts with both technical and ethical perspectives, there is a need for experts from each field to get together and cooperate. The Ministry of Health and Welfare, which is overseeing the development of the information

system, should be more active in reconciling the two areas. It must be kept in mind that the development of big data system in social welfare is not a task to be dealt quickly with as a yearly 'project,' but rather an important 'responsibility' that lays the foundation for the future generation of social welfare.

Secondly, the ethical responsibility of all those who engage in SSIS should be reinforced. Dataveillance through SSIS has closely related to the classic ethical dilemma regarding "Can the purpose justify the means?" As observed earlier, although dataveillance is being used for the 'right purpose,' identifying blind spots and welfare frauds, dataveillance is the 'means' that implies the invasion of privacy. In 『The Prince』, Machiavelli (2015) stated that if the use of means is unavoidable in re-establishing social order, the means can be justified. However, even though the use of means is inevitable, there is still the responsibility to compensate for the damage arising from the use of means. The responsibility for the side effects needs to be deal with separately. In 『Politics as a Vocation』, Weber (2007) asserts that every human behaviour is performed according to two principles: the ethics of conviction and the ethics of responsibility. Weber believes that, unlike religious people who follow their absolute beliefs (ethics of conviction) and thus do not dwell on the consequences, administrators and politicians should be aware of human imperfection and flaws, and therefore should predict and take the ethics of responsibility for the consequences that one's decision will bring. This is because the state, which cannot but unavoidably control over the public, also has to take responsibility for the consequences of social control that inevitably leads to harmful side effects.

The governments need to reinforce ethical responsibility for dataveillance through social welfare information systems. No developers, administrators, and researchers of the information system are free of ethical responsibility. They must navigate through specific areas of conflict, such as privacy, accuracy, property, and accessibility, rather than simply mechanically developing and activating information systems. They need to consider countermeasures against possible damages. To do this, they can reference international standards such as OECD Privacy Principles (collection limitation principle, data quality principle, purpose specification principle, use limitation principle, security safeguards principle, openness principle, individual participation principle, and accountability principle) to establish ethical standards in South Korea.

Thirdly, a reverse monitoring system carried out by recipients and the public on the dataveillance of SSIS should be built. Currently, the information on SSIS is structured in a way that only select officials can access. Under the excuse of 'protection of personal data,' the information accessibility by recipients and citizens are being suspended and those public officials carrying out the dataveillance are monitored by a superior Super-Big Brother (central government agency). Nevertheless, limitations and suspension of accessibility are not the sole methods to protect personal data. Norwegian criminologist, Mathiesen (1997), highlighted the Synopticon which enables the majority to monitor a small number of people with power. This contrasts with the panopticon, where the minority monitors the majority. Unlike the panopticon, synopticon refers to a reverse monitoring mechanism in which leaders and the public monitor simultaneously (syn). Synopticon is a 'monitoring on monitoring' that starts from the bottom, unlike Super-Big Brother which takes place at the top.

A reverse monitoring mechanism needs to be adopted in the SSIS as well. Firstly, welfare recipients ought to have rights to be informed about how and what personal data are collected and connected within

public organizations. Secondly, in addition to the right to request access, deletion, and revision, the right to refuse data linkage that goes beyond its original purpose of collection should be affirmed. Also, establishing a reverse monitoring committee, which includes recipients and the public, to check whether dataveillance is being ethically operated should be considered. Acknowledging that the distribution rate of high-speed internet (140%) and that of mobile phones (110%) exceed 100%, the government has emphasised that the Next-Generation SSIS should enhance the public's and recipient's accessibility and utilisation of the system (MOHW, 2015: 4). The 'recipient-centred information system,' which is only being described abstractly, should be realised so that the public can participate in the public information system.

Fourthly, it is necessary to recognise that the direction of dataveillance with SSIS should be aimed at community trust and solidarity. As Kim's (2013: 105) criticism highlights, the reason why we are paying attention to distributive justice is not simply because an accurate and reasonable calculation is important between uncorrelated individuals. Distributive justice is based on whether individuals are receiving a reasonable reward when living together as a member of the community. In the same context, the reason why people believe welfare frauds and blind spots are unjust is not only because welfare benefits are not accurately calculated and distributed to each recipient, but also because we believe fraudulent recipients break the social trust as a member of the community. Furthermore, we want to help the poor population because we believe they are also members of the community. It is a very ethical and social motive, not solely economic and rational motive.

Therefore, investigation of welfare frauds and blind spots using dataveillance can only acquire ethical justification once it contributes to the trust and solidarity of the community. As Clarke (1998: 505) pointed out, dataveillance based on unnecessarily strict rules can create hostility within the community. Ricoeur (2006) believed that true justice does not come from duties or rules which ignore certain relations between individuals, but from a cooperative and collective life. We do not feel that we have a good life when the exactly right amount of benefits has been allocated to each individual. Rather, even if material distribution was made a bit imperfectly, people can feel they live a better life when they are in intimate, mutual and reciprocal relationships. Ricoeur (2006: 292) claimed what that holds a good society tightly is 'solicitude,' an ethical virtue, not a norm. In the process of dataveillance through SSIS, an attitude of solicitude towards recipients is also essential. Like Brynjolfsson's and McAfee's (2014) analysis, we are living in the Second Machine Age. However, it is still humans who decide the machine's direction of use. Whether to utilise IT for solicitude or control is up to humans. Practitioners and researchers of social welfare should start reflective thinking to answer ethical dilemmas that social welfare faces in the age of information.

References

Kang, Hye-Gyu, 2010, "Main Contents and Expected Effects of the Social Welfare Integrated Management Network", Issue & Focus, 19: 1-8. (**Korean**)

Kim, Ki-Bok, 2013, "A Teleological Approach to Justice: A Critique and Interpretation of Ricoeur's Critique of Rawls's Theory of Justice", Studies in Contemporary European Philosophy, 33: 97-126. (**Korean**)

Kim, Sang-Bae (Ed.), 2008, Anatomy of Internet Power, Seoul: Hanul. (**Korean**)

Kim, Su-Young & Kim, Yi-Bae, 2014, "The Impact of Public Social Welfare Administration's Informatisation on the Practice of Frontline Social Welfare Bureaucrats: A Critical Review of the Social Welfare Integrated Management Network", Korean Journal of Social Welfare Administration, 16(4): 91-126. (**Korean**)

Kim, Eun-Ha, 2015, "The Potential and Limitations of Identifying Marginalised Groups in Welfare using Information Systems", Proceedings of the 2015 Social Policy Association Joint Conference, 489-501. (**Korean**)

Kim, In-Sook, 2005, "The Identity of Korean Social Welfare Practice: From a Politico-Social Perspective", Situation and Welfare, 20: 119-152. (**Korean**)

Ministry of Health and Welfare, 2009, A Study on the Survey of Welfare Status for Active Welfare Expansion. (**Korean**)

Ministry of Health and Welfare, 2011, "Press Release on the Results of the Livelihood Security Recipients' Supporter Verification Survey".(**Korean**)

Ministry of Health and Welfare, 2014a, Guidelines for the Use of the Social Security Information System. (**Korean**)

Ministry of Health and Welfare, 2014b, Research Task Content for the Study on the Discovery of Welfare Blind Spots using the Social Security Information System. (**Korean**)

Ministry of Health and Welfare, 2015, Request for Proposal for BPR/ISP Consulting for the Construction of the Next-Generation Social Security Information System. (**Korean**)

Choi, Kyun, Hwang, Kyung-Ran, Seo, Byung-Soo, Ryu, Myung-Seok, Kim, Hyun-Jin, & Jang, Jin-Yong, 2012, A Study on the Systematisation of the Discovery of Welfare Blind Spots and the Enhancement of Welfare Information Accessibility, Sejong: Ministry of Health and Welfare & Korea Social Welfare Council. (**Korean**)

Choi, Myung-Min, 2014, "The Essence and Reflectivity of Social Welfare Practice in Fluid Modern Society", Proceedings of the Korean Society for Social Welfare Practice Conference, 189-217. (**Korean**)

Ham, Young-Jin, 2013, "A Preliminary Discussion on the Effects of Welfare Sector Informatisation: Focusing on the Social Welfare Integrated Management Network", Digital Policy Research, 11(8): 11-21. (**Korean**)

Ham, Young-Jin, Lee, Hee-Jong, Park, Gyu-Beom, & Lee, Young-Gle, 2012, A Foundation Study for the Enhancement of Reliability and Efficiency of Happiness e-connect: A Guide for Linked Information for Income and Property Investigation, Osong: Korea Health and Welfare Information Development Institute. (**Korean**)

Hong, Sung-Wook, 2002, Panopticon: The Information Prison of the Information Society, Seoul: Book World. (**Korean**)

Kang, Jung-In & Kim, Kyung-Hee (Trans.), 2015, The Prince, Machiavelli, N., 1532, Il Principe, Seoul: Gachi. (**Korean**)

Oh, Saeng-Keun (Trans.), 2003, Discipline and Punish, Foucault, M., 1979, Discipline and Punish, Seoul: Nanam. (**Korean**)

Lee, Young-Dae, 2004, The Change of the Concept of Ownership and Intellectual Property Rights, Jincheon: Korea Institute of Information and Communication Policy. (**Korean**)

Aronson, J., 1995, “A Pragmatic View of Thematic Analysis”, The Qualitative Report, 2(1): 1-3.

Brynjolfsson, E, and McAfee, A. 2014, The Second Machine Age, London: Curtis Brown.

Clarke, R. A. 1988, “Information Techonology and Dataveillance", Communications of the ACM, 31(5): 498-512.
Davenport, T.H., Harris, J.G., and Morison, R. 2010, Analytics at work: Smarter Decisions, Better Results, Boston: Harvard Business School Press.
Day, P. R., 1981, Social Work & Social Control, London: Tavistock Publications.
Esposti, D. S., 2014, “When big data meets dataveillance: The hidden side of analytics", Surveillance & Society 12(2): 209-225.
Garfinkel, S., 2001, Database Nation: The Death of Privacy in the 21st Century, Sebastopol: O'Reilly Media.
Garland, D., 1985, Punishment and Welfare, Aldershot: Gower.
Gert, B., 1998, Morality: Its Nature and Justification, Oxford: Oxford University Press.
Geoghegan, L., Lever, J., and McGimpsey, I., 2004, ICT for Social Welfare: A toolkit for managers, Bristol: Polity Press.
Giddens, A., 1985, The Nation-State and Violence, London: Polity Press.
Giffords, E. D., 1998, “Social Work on the Internet: An Introduction", Social Work 43(3): 243-251.
Ginsburg, N., 1979, Class, Capital and Social Policy, London: Macmillan.
Haidt, J., 2012, The Righteous Mind, New York: Vintage Books.
Jonson, D., 1997, “Democracy, Technology, and Information Societies”, 5-16, in The Information Society, edited by Goujon, P., Lavelle, S., Duquenoy, P., Kimppa, K., Laurent, V., Belgium: University of Namur.
Kreuger, L. W., Stretch, J. J., and Kelly, M. J., 2006, “Is Computer-Assisted EBP Generating “Fast” Practice?", Journal of Evidence-Based Social Work, 3(3-4): 27-38.
Kusserow, R. P., 1984, “The government needs computer matching to root out waste and fraud", Communications of the ACM, 27(6); 542-545.
Lyon, D., 1993, “An Electronic Panopticon? A Sociological Critique of Surveillance Theory", The Sociological Review, 41: 653-678.
Marlowecan, L. S., 1997, “Social Workers On-Line: A Profile", Computers in Human Services, 14(1): 59-70.
Martin, H., Lackner, M. and Schneider, F.G., 2009, “An empirical analysis of the dynamics of the welfare state: the case of benefit morale", CESinfo Working Paper No. 2641, CESifo Group Munich.
Marx, G. T., and Reichman, N., 1984, “Routinising the discovery of secrets." American Behavioral Science, 27(4): 423-452.
Mason, R.O., 1986, “Four Ethical Issues of the Information Age", Management Information Systems Quarterly, 10(1): 4-12.
Marson, S.M., 1997, “A Selective History of Internet Technology and Social Work”, Computers in Human Services, 14(2): 35-49.
Mathiesen, T., 1997, “The Viewer Society: Micheal Foucault's 'Panopticon' Revisited", Theoretical Criminology, 1: 215-234.
Mayer-Schönberger, V., 2009, Delete: The Virtue of Forgetting in the Digital Age, Princeton: Princeton University Press.
McKinsey, 2011, Big data: The next frontier for innovation, competition, and productivity, McKinsey Global Institute.
Mclaughlin, K., Obsborne, S. P., and Ferlie, E., 2002, New Public Managment, Oxon, Routledge. Mele, N., 2013, The End of Big, New York: St. Martin's Press.

Moor, J., 1985, “What is Computer Ethic?", Metaphilosophy, 16: 266-275.
O'Connor, J. 1973, The First Crisis of the State, New York: St. Marin's.
Orwell, G., 1948, 1984, New York: Penguin Books.
Parton, N., 2008, Changes in the form of knowledge in social work: from the 'social' to the 'informational'?", British Journal of Social Work, 2: 253-269.
Pithouse, A., Hall, C., Peckover, S., and White, S. A, 2009, "Tale of Two CAFs: The Impact of the Electronic Common Assessment Framework", British Journal of Social Work, 39: 599-612.
Raynor, P., 1985, Social Work, Justice and Control,. Oxford: Basil Blackwell.
Rudder, C., 2014, Dataclysm, New York: Crown.
Shattuck, J., 1984, “Computer matching is a serious threat to individual rights", Communications of the ACM, 27(6): 538-541.
Spinello, R., 2006, Cyberethics, Sudbury: Jones and Bartlett.
Titmuss, R. M., 1963, Essays on the Welfare State, Boston: Beacon Press.
Tunley, M., 2011, “Need, greed or opportunity? An examination of who commits benefit fraud and why they do it", Security Journal, 24(4): 302-319.
van Dijck, J., 2014, “Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology", Surveillance & Society, 12(2): 197-208.
van Stolk, C., and Tesliuc, E. D., 2010, “Toolkit on Tackling Error, Fraud and Corruption in Social Protection Programs”, Washington: The World Bank.
Weber, M., 1968, Economy and Society, Berkeley: University of California Press.