International Journal of u- and e- Service, Science and Technology
Vol.9, No. 6 (2016), pp.243-252
http://dx.doi.org/10.14257/ijunesst.2016.9.6.23

Rights vs. Efficiency of Government Information: NEIS Case in Korea[1]

Choong-Sik Chung[2] and Dongwook Kim[3]

Abstract

As the Korean government implements an e-Government which can provide electronic service delivery to the citizens through the Internet, privacy has become one of Korean's most important civil rights. The National Education Information System (NEIS) case shows that e-service delivery initiatives in many countries have been more and more faced with the difficult task of balancing personal privacy and efficiency in government information administration. The lesson from the NEIS case is that it is very difficult to implement government information initiatives without consideration of information privacy rights. Therefore, it is requested that the right to participate in the whole process of government information initiatives should be given to the information subject. Therefore, each government agency's information initiatives should be supervised by independent authority with strong privacy policies.

Keywords*: Privacy Rights, Personal Information Protection, Surveillance by Government, Trust between Government and Citizens. Electronic Government*

1. Introduction

Current technological advances have also created new opportunities for many governments wishing to implement e-Government which can provide electronic service delivery to the citizens. After going through continuous efforts in e-Government and national informatization, Korea has become one of the global E-government leaders - obtaining the highest scores in 'E-government Development Index' and 'E-participation Index'. Korea's E-government Development Index ranking assessed by the United Nations improved from 15th in 2001 to the top in 2010 out of 192 countries worldwide, and its E-participation Index ranking was also ranked 1st in 2010, 2012 & 2014 [1-3]. In addition, many of Korea's E-government practices until now have been introduced to the world as the best cases and received worldwide acknowledgement.

On November 13, 2002, in Korea, President Kim, Dae-jung announced that the 11 major e-Government initiatives were successfully executed and declared the opening of full-scale e-Government services [4]. However, because of e-Government initiatives, for all Koreans, 2003 had been a chaos year of struggle after struggle. Throughout 2003, the whole country was plunged into confusion by The National Education Information System (NEIS).

From a government point of view, NEIS is an integrated and efficient system for academic and administrative operations. However, from a teacher's standpoint, NEIS is a giant and central database system to collect private information from students, parents and teachers, and will be under the control of the government. NEIS which is one of the 11 e-Government initiatives in Korea has not properly operated until 2003.

[1] This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (NRF-2014S1A3A2044645)
[2] Dept. of Public Administration, Kyungsung University. Daeyeon-dong, Nam-gu, Busan, 608-736. Korea. cschung@ks.ac.kr
[3] Dean, Graduate School of Public Administration, Seoul National University. 1 Gwanak-ro, Gwanak-gu, Seoul. 151-742, Korea

ISSN: 2005-4246 IJUNESST

Because of the implementation of NEIS in Korea, new information technology using integrated database networks is necessarily viewed as a threat to personal privacy. The NEIS case shows that e-service delivery initiatives in many countries have been more and more faced with the difficult task of balancing personal privacy and efficiency in government information administration.

Therefore, the main object of this paper is to introduce that implementation of NEIS in Korea was affected by concerns over privacy rights. Key issues to be discussed include: (1) the debate concerning privacy rights vs. efficiency in government information initiatives; (2) the availability of government information using integrated databases vs. the possibility of individual information infringement; (3) building trust between the governments and citizens with privacy policies.

2. What is NEIS? – Government Perspective

2.1. Concept of NEIS

NEIS is a system that connects government agencies and administrations with more than 10,000 elementary and secondary schools, 16 provincial offices of education and their sub-agencies, and the Ministry of Education & Human Resources Development (MOE&HRD) into one network through the Internet [5]. Teachers, students, parents and school administrators will have access to education-related information which will be shared using an integrated database across the nation.

NEIS offers a service where 27 education administration duties such as school affairs that school administrators and civil servants must coordinate and process, social welfare for students, human resource management, budget allocations, and real estate holdings will be electronically processed.

2.2. Expected Effect of NEIS

The objectives of NEIS are to reduce the burden of administrative tasks on teachers by introducing new Internet and database technologies. Moreover, NEIS will provide academic reports regarding the current status and outcomes of students to their parents, to enhance the satisfaction levels of citizens towards the government by improving government services, and to make education administrative duties more efficient and transparent.

With the development of NEIS completed, the processing time is expected to be reduced by 20-50% and the volume of paper documents by 30%. Teachers are expected to concentrate their abilities on teaching without the distractions of administrative routines[4] and their operational productivity will rise by more than 25%. For parents, issuance of transcripts, certificates of registration or graduation from any schools in the country will become much easier. The general public will also be able to access students' records via the Internet, which will then serve as a point of interaction between schools and homes.

3. History of NEIS - Emerging as a National Issue

In Korea, the first School Information Management System began in 1997. This project was successfully achieved through the implementation of Client and Server System (C/S system) by December 2001. The C/S system was an integrated and efficient system for academic and administrative operations. Therefore, from the schools teacher's perspective,

[4] When students enroll in middle school or high school from elementary or middle school respectively, they must to fill out a personal information form. However, using NEIS, once a student fills in a personal information form in elementary school, that information will be stored in the national education database servers, students will no longer have to perform redundant processes. Each student's personal information will be sent electronically to the student's new school.

there was no reason to change the C/S system. In 2001, the completion of C/S system implementation, every teacher was given a PC for use at school and PCs were allocated to every eighth student. In the same year, equipment for the advancement of school facilities and web-based school LANs were provided to all of the 10,064 schools (222,146 classrooms) across the nation.

Meanwhile, in line with rapidly growing Internet technology, MOE&HRD wanted to enhance the C/S system, which was just connected to each school's LAN based system, to include a nationwide Internet based network system. In 2000, an Information Strategy Planning (ISP) was drawn up to establish NEIS.

The NEIS project was chosen as one of the 11 major e-Government initiatives by the Special Committee for e-Government on May 2001. Subsequently, the NEIS project officially started on October 2001. The most important thing is that the NEIS completion target date was decided as on October 2002 in accordance with the other 10 major initiatives. Therefore, NEIS implementation was pressed for time. Many problems arose from the short timeframes for meeting specific target dates. The timeframe of initiatives need to be realistic, as there can be considerable lags before benefits accrue. In reality, the NEIS implementation target date was decided based on the Korea political situation without consideration of student and teacher's demand.

Moreover, it is necessary that an understanding of user demand and preferences should be gathered in the initial stages of system implementation. In the NEIS implementation, the MOE&HRD focused on administrative operational efficiency using an integrated database and Internet network instead of student's human rights. As a matter of fact, in the system design process of NEIS initiatives, user's requirements were not gathered, and privacy issues were not a concern at all. These government centric and top down strategies were faced with resistance by students and teachers.

The development of NEIS software for managing school affairs, undergraduate courses, school entrance exams, student health insurance and other administrative tasks was completed in August 2002. This system was to be launched in time for the beginning of the second academic semester of 2002. In September 2002, in the process of pilot test, the Korean Teachers and Educational Workers Union (KTU) brought up the student privacy issue and requested further testing of the application before NEIS implementation.

However, NEIS was partially launched in November 2002 with only a general administrative services subsystem which included personnel management, budgeting, and accounting carried out by educational administration agencies because of political considerations[5]. In December 2002, 13 government services were made available on NEIS. The pilot test, which included school affairs-related areas, was extended until February 2003 and NEIS full service across the nation was delayed on March 2003.

In early 2003, the KTU carried out a movement to disobey the implementation of NEIS because NEIS will not only keep the teachers under government's control, but it is also an unconstitutional database system that violates the student's human rights. The given reason why the KTU started the movement against the implementation of NEIS was the possibility of students' basic human rights infringement. The KTU had emphasized that three key parts of NEIS – schools' administration, health and admission affairs, which contain students' personal records on their state of health, school work and grades, and school entrance and transfers – infringes on students' basic human rights including privacy.

On February 14, 2003, the KTU filed a complaint with the criminal court against the minister, deputy minister, and the director in charge of NEIS in the MOE&HRD for the crimes of misfeasance and illegal enforcement. Moreover, fourteen civil society

[5] In Korea, e-Government initiatives were selected as a remarkable presidential achievement within the remainder of Kim, Dae-jung's term of office. Therefore, 11 e-Government initiatives should be completed within 2002 which was Kim's administration's last year. Special Committee for e-Government. *E-Government White Paper*, Seoul: Korea, January 29, 2003

organizations and students groups established a coalition to struggle against NEIS and have carried out many activities to demand the abolishment of NEIS, for example, statements/press releases, online & offline demonstrations and lawsuits to the court.

They have persisted that NEIS is illegal and unconstitutional, and actually ignores many international conventions such as Universal Declaration of Human Rights, UN Guidelines on individual information[6] and even the OECD Guidelines on Privacy (the rights of self-decision, self-control on his/her own private information).

On February 19, 2003, 24 civic groups filed a suit against NEIS to be implemented by the MOE&HRD with the National Human Rights Commission (NHRC) as it may encroach upon people's information rights.

On March 10, 2003, the minister of the MOE&HRD, who was newly designated by the new administration, announced that NEIS implementation will be stopped, and return back to the C/S system. However, this address instantly faced severe opposition from the officials of the MOE&HRD. Therefore, the minister of MOE&HRD stood back a step. The minister said that the MOE&HRD will be await the decision of the NHRC and will follow it.

4. Recommendation of the NHRC - a Turning Point

The NHRC collected material on information and human rights and held a hearing over three months. On May 17, 2003, the NHRC sent its resolution on NEIS, decided by the NHRC Plenary Committee on May 12, to the MOE&HRD as follows, 1) The NHRC concluded it was necessary to closely examine the following points: (i) if the NEIS system limits basic rights, (ii) if it does limit basic rights, further investigation of constitutional grounds for limitation of basic rights, (iii) even if there is a constitutional basis for limiting basic rights, the need to examine whether the goal of the system is clear, if potential damage will be minimized, if the legal benefits are balanced, appropriateness of the means, and appropriateness of the method.

2) The NHRC examined the question of whether NEIS violates human rights based on Article 10 (right to pursue happiness), Article 17 (freedom of privacy and secrecy), Article 31 (right and duty to receive an education), and Article 37 (respect of freedoms and rights of citizens) of the Constitution; Article 12 of the UN Declaration on Human Rights; Article 17 of the International Convention on Civil and Political Rights; Article 16 of the International Convention on the Rights of the Child; OECD Guidelines on the International Circulation of Private Data and Protection of Privacy; UN Guidelines for Regulations on Electronic Personal Information; and the Act on the Protection of Personal Information Maintained by Public Agencies.

3) The NHRC decided to recommend the ministry of education and human resources development amend 'regulations on personnel administration of public educational officials by excluding the area of school management/further education and admission/health care among the 27 areas of NEIS because it could potentially violate human rights such as the right to privacy; maintain the existing C/S system in school management/further education and admission/health care area and improving the security of the C/S system; and exclude items in the separate paper of instructor personnel records that could potentially violate human rights such as the right to privacy.

[6] United Nations Guidelines Concerning Computerized Personal Data Files was adopted by the General Assembly on 14 December 1990 as follows; 1. Principle of Lawfulness and Fairness. 2. Principle of Accuracy, 3. Principle of the Purpose-Specification, 4. Principle of Interested-Person Access, 5. Principle of Non-Discrimination, 6. Power to make Exceptions, 7. Principle of Security, 8. Supervision and Sanctions, 9. Transborder Data Flows, 10. Field of Application.

5. Progress in Resolution of Dispute – a Long Journey to a Statement of Mutual Agreement

After the NHRC decision, the tide was turning. The NHRC emphasized in its report that each student's academic, transfer and medical records should not be saved on a central database and should not be available online. It also said that the teachers' information, which includes blood type, property holdings and military service records, is personal and should not be saved in the system. Therefore, on May 26, the MOE&HRD and KTU arrived at a mutual agreement on NEIS as follows:

Three key parts of the NEIS – schools' administration, health and admission affairs, which contain students' personal records on their state of health, school work and grades, and school entrance and transfers - except those of 3rd grade high school students are excluded from NEIS. The Committee for Educational Informatization which is composed of experts of various area and teachers would be established to examine the problem of NEIS and recommend the solution.

However, this agreement brought another backlash from MOE&HRD officials and conservative teacher groups who claim that about 97 percent of schools are already implementing the more convenient NEIS and cannot go back to the old C/S system. In a massive counterattack against the ministry's decision to reconsider the implementation of NEIS, the nation's conservative forces united to attack the government, which they claimed yielded to some interest groups' illegal collective actions.

The main opposition Grand National Party called upon the minister of MOE&HRD to resign immediately, otherwise he would be forced to. Therefore, during a National Assembly Education Committee meeting on May 27, the minister of MOE&HRD said:

"I believe the NEIS has a much better security system than the C/S system. I only meant to suspend the NEIS for six months. This does not mean returning to the C/S system from next year. We will come up with a democratic and systematic way to operate the NEIS before a decision is made".

On June 1, the MOE&HRD broke the agreement by announcing that it will allow each school to choose it's own management system, which means some schools could adopt NEIS. Though it also announced some private information of students would be deleted from NEIS.

On June 18, nine human rights activists started a hunger strike struggle in front of Myungdong Cathedral. They criticized the government for breaking the agreement and asserted to stop the implementation of NEIS. On June 20, the human rights activists visited the MOE&HRD to request as follows; (i) stop the implementation of NEIS, (ii) delete the sections of private information of students, parents and teachers, (iii) review the educational informatization process at all levels.

The KTU also announced that it would hold a national-wide massive strike with a large demonstration on June 21.[7] On June 23, they joined a press conference to announce 'special week of Big Brother' (June 23rd to 29th), which was commonly held by 52 civil society and human rights organizations.

Under the continuous nationwide anti-NEIS demonstration, the MOE&HRD could not resolve the NEIS situations any more. Therefore, Korean government composed the Committee for Educational Informatization (CEI) under the Office of Prime Minister on June 2003. The government held the first meeting of CEI on July 7. After that, CEI held a council from July to December on a monthly basis. Finally, with a seventh meeting on December 15, 2003, mutual agreement was reached as follows:

(1) The database of three areas – schools' administration, health, and admission affairs – should be physically separated from existing NEIS, and operated in the independent servers under the 16 provincial offices of education. The independent supervisory

[7] More than 15,000 teachers out of the 92,000 KTU members took part in the strike as a collective leave from school to protest the implementation of NEIS on June 21.

authorities should be established as 16 provincial offices of education level. (2) The supervisory authority empowered the principals to collect, manage information, and develope appropriate measures to enhance human rights. (3) Long term basis, it is a basic direction to make maximum efforts to respect the autonomy of each school in the selection of information system. Under the current stage, each school can operate a server separately or on a group basis.

After a mutual consent between the government and anti-NEIS civic groups, the minister of MOE&HRD who has not coped with the NEIS situation properly was reshuffled as of December 17, 2003. This agreement statement was confirmed by a minister meeting on NEIS led by the Prime Minister on March 3, 2004. Therefore, a heated and long pending controversy on NEIS was officially settled.

6. Lessons from NEIS Case

There are a number of key lessons from the NEIS case can be set out below: a) information human rights, b) building trust, and c) legislation for privacy.

6.1. Information Human Rights - Cope with the Coming Surveillance Society

Privacy is one of the fundamental rights from which all other human rights are derived. Recently, the notion of privacy has evolved into several different doctrinal concerns: autonomy, intrusion, and information privacy [6].

At the end of the 19th century, Warren and Brandeis couldn't have conceived how technology could threaten human privacy at such a fundamental level. Since then, there has been a tendency to broaden the traditional concept of privacy (the right to be left alone) and to identify a more complex synthesis of interests which can perhaps more correctly be termed personal information privacy. The NEIS case shows well the importance of information human rights which includes information self-determination[8].

The more serious thing is that this off-line surveillance through CCTV transformed to the cyberspace surveillance through controlling the Internet at break-neck speed. Therefore, now surveillance has become one of the most dangerous threats to human rights and democracy. Moreover, owing to the rapid development of information technologies including the Internet and databases, the governments have the ability to collect and process all kinds of information, as they want. Therefore, protecting human rights and democracy from the surveillance is a very urgent and important task that we have faced.

Like the NEIS case, integrated databases and networks have a fundamental problem. There is no way to guarantee that the information in the database and network is kept safe. Although it is possible to use information technology to protect or enhance privacy, the tendency of information technology advances is to do the reverse. One of the inherent problems with privacy-protecting technology is that it is very difficult to know whether or not the technology is working properly.

To protect human rights and democracy from surveillance, it is requested that the right to participate in designing the information systems and determine the information systems, the right to know and control the information and information systems should be given to the information subject. In particular, the need to allow individuals to make relevant decisions regarding their personal data should be kept according to the OECD guidelines. Finally, technologies should be under the control of the information subjects and the surveillance of governments should be supervised by an independent authority.

[8] This concept was not included in the original OECD guidelines and introduced recently. In 1983, the German Constitutional Court popularized the term "information self-determination" as follows; "The basic right guarantees the ability of the individual, to decide in general for himself the release and use of his own personal data" [7].

6.2. Building Trust – Partnership between the Governments and Citizens

In line with the worldwide e-Government initiatives, convenient e-service delivery through the Internet gave rise to privacy issues in many countries. According to the new research on the American Internet users[9], though Americans value the ease and efficiency of better e-services from government, they also express concerns that dealing with government over the Internet may compromise their privacy.

Like this, it seems that distrust of governments, related to privacy issues, is a universal phenomenon. Moreover, in Korea, the social tendency of distrust between the government and the citizens is excessive. There has been a lot of controversy surrounding securities on NEIS, perhaps justified, perhaps not. Much of the controversy and confusion is due to differences in opinion on the degree of protection against information sharing by the government.

This sharing of information on individuals inevitably raised privacy protection issues [9]. Therefore, the Korean government also established a regulatory process regarding physical, administrative and technical security measures for NEIS to prevent illegal access[10]. However, the more the government officials are looked down upon as unreliable, inefficient, and untrustworthy, the more Koreans worried about the possibility of personal information infringement from NEIS.

Therefore, as long as distrust between the government and citizens exist, a technical oriented approach could not solve the privacy issues properly. The most important thing is to build trust between the government and the citizens. For this, citizen participation is crucial in the whole process of government information management[11].

To ensure that the public and stakeholders will be partners in the government information management effort, it is important to try to build trust in government, because lack of trust by the public can lead to the failure of or serious delay in government e-service delivery initiatives. Especially, citizen participation has a key role to success, from the vision/planning process through implementation, monitoring, and evaluation. Therefore, the government has to treat the citizen not only as a customer but also as a partner in the whole process of government information initiatives.

6.3. Encouraging the Adoption of Privacy Policies – Strong Regulations Also Required

There are many different national approaches to privacy in order to secure effective privacy protection in the government's e-service. There is agreement that there is no single uniform solution. In the United States and many European countries, like the United Kingdom, France, Germany, and Sweden, the 1970s may be described as a period of intensified investigative and legislative activities concerning the protection of privacy

[9] According to the survey, nearly forty-five percent of Americans strongly agree that if they submit personal information about themselves to government Web sites, government will be able provide them with better services. However, nearly the same percentage believes that if they submit personal information to government Web sites, it may risk the security and privacy of their personal information [8].

[10] These technical security strategies included network security through a firewall/intrusion detection system and security technologies such as PKI-based certification. Moreover, encryption technologies to protect the information transaction in the information sharing system were installed.

[11] According to the OECD Guidelines, the Individual Participation Principle is defined as follows; An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him i) within a reasonable time; ii) at a charge, if any, that is not excessive; iii) in a reasonable manner; and iv) in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

with respect to the collection and use of personal data[12]. This means the legislation of privacy protection closely related to the development of democracy.

It is a common practice in continental Europe to talk about "data laws" or "data protection laws" whereas in English speaking countries they are usually known as "privacy protection laws". Moreover, it is generally known that the European countries have stressed the need of privacy protection legislation while the United States has focused on self-regulatory approaches[13]. However, it seems that it is not important for Koreans to select which approach the government uses.

OECD recommended effective solutions as a mix of regulatory and self-regulatory approaches blending legal, technical, and educational solutions comprised of the legal, cultural, and societal contexts [11]. OECD member countries should establish legal, administrative or other procedures for the protection of privacy and individual liberties in respect of personal data[14].

Korea became a member of OECD on December 12, 1996. However, in relation to the privacy protection legislation, it still has a long way to go to meet OECD guidelines. According to the map of data protection laws around the world by Privacy International, Korea is ranked as a legislation pending country.

The Constitution of Korea stipulates that every citizen shall not have their rights to confidentiality and freedom of privacy (Article 17) and freedom of communication (Article 18) infringed. On January 7, 1994, *The Protection of Personal Information by Public Organizations Act* was legislated. This act governs the protection of personal information in the public sector only. Moreover, this act has no concrete punishment article in case of personal data reveal.

There are no private sector self-regulatory initiatives in Korea at the present time. The approach to privacy in the private sector is partially done by other laws with privacy provisions15. For example, medical records are sensitive personal information. Many people think it's illegal to release medical records. However, in Korea, there is no national law criminalizing the improper release of medical records. Such laws are clearly needed, because unauthorized releases are very widespread.

In the same way, in Korea, there is no law criminalizing the improper release of student records. In the United States, all schools receiving federal funds must comply with the

[12] In the United States, the *Privacy Act* was legislated in 1974. Even though the UK has had legislation in place since 1984, the *Data Protection Act of 1984*, it has just completed a revision of its law that brings the nation into full compliance with the regional standards of the European Union. In 1976, the Council of Europe established a Committee of Experts on Data Protection that reported its findings in early 1979 and the result was the Council of Europe's *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* [10].

[13] The United States does not have federal comprehensive legislation or mandatory "baseline" privacy requirement. Instead, the United States relies on a combination of self-regulation, sector-specific legislation, educational outreach, and enforcement authority. The use of personal information held by federal government agencies is regulated by the *Privacy Act* (1974) which establishes fair information principles for handling personal data. The Office of Management and Budget (OMB) is responsible for overseeing the Act. The Privacy Act provides data subjects with a civil right of action which may result in monetary damage and/or injunctive relief. The Act also provide criminal penalties for knowing violations of the Act.

[14] Member countries should in particular endeavor to: a) adopt appropriate domestic legislation; b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise; c) provide for reasonable means for individuals to exercise their rights; d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles: and e) ensure that there is no unfair discrimination against data subjects.

[15] *The Use and Protection of Credit Information Act* focuses on the protection of personal data in financial transactions. For example, the Act prohibits a financial institution from revealing or sharing personal/financial data without the data subject's written consent. Korea also has an Act on the Protection of Confidentiality in Communications. *The Telecommunications Network Use Proliferation Act* was amended in January 1999 to institutionalize the protection of personal data in the private sector, reflecting the principles in the OECD Guidelines. The revised Act, which was in effect as of January 2000, authorized government to place specified restrictions on information and telecommunications service provider in case they abuse or misuse an individual's personal data.

1974 federal *Family Educational Privacy Rights Act* (FERPA). In general, FERPA prohibits schools from releasing education records or personally identifiable information[16] other than directory information without having parental consent.

As far as the legal problems of NEIS are concerned, the protection of privacy and the possibility of individual information infringement constitute perhaps the most widely debated aspects. Therefore, in view of the inadequacy of existing laws relating to the processing of student data and individual rights, it is urgently requested that comprehensive privacy laws should be legislated.

However, this legislation can set a safe minimum for privacy. Because more and more digitalization of information and networking of government information is carried out rapidly in the various agencies, a single privacy act may have to many limitations. Like the NEIS case, it is possible that violating citizen's privacy may be happen in other countries because many governments have implemented e-Government initiatives through integrated databases [13]. Therefore, along with comprehensive privacy laws, strong and detailed regulations are also required when implementing government information initiatives.

Like the NEIS case shows well, privacy consciousness in the citizens has enhanced very quickly. However, in the public sectors, especially in the government, understanding of privacy is still insufficient. Therefore, it is necessary that government information projects should be supervised by both the powerful agencies and citizens through strong privacy policies.

7. Conclusion

Generally, privacy rights should be obtained through civil discourse and legislation rather than through a sharp conflict between government and privacy activists. However, owing to the struggles against NEIS, the Korean government recognized the importance of privacy seriously. Therefore, Koreans stand at a crossroad in relation to the evolution of privacy rights, because they have to change their thinking, their laws, and their culture. As more and more citizens realize the importance of privacy, less and less government leadership on the issue will be needed.

The lesson from the NEIS case shows well that it is very difficult to implement e-Government initiatives without consideration of information privacy rights [14]. Therefore, it is requested that the right to participate in the whole process of government information initiatives should be given to the information subject. Moreover, it is important to build trust between the government and citizens. Transparent rules and regulations governing the protection of privacy and personal data and their effective implementation on information networks are key elements to increasing confidence in citizens. Lastly, each government agency's information initiatives should be supervised by an independent authority with strong privacy policies.

[16] Under federal regulations, personally identifiable information includes: the student's name, the name of the student's parent or other family member, the address of the student or the student's family, a personal identifier such as the student's social security number or student number, a list of personal characteristics that would make the student's identity easily traceable, and other information that would make the student's identity easily traceable [12].

References

[1] United Nations (UN).: UN E-Government Survey 2010: Leveraging e-government at a time of financial and economic crisis, **(2010)**.
[2] United Nations (UN).: UN E-Government Survey 2012: E-Government for the people, **(2012)**.
[3] United Nations (UN).: UN E-Government Survey 2014: E-Government for the Future we want, **(2014)**.
[4] Special Committee for e-Government.: E-Government White Paper, Seoul, Korea, **(2003)** January 29.
[5] Ministry of Education & Human Resources Development.: 2003 White Paper: Adapting Education to the Information Age. Seoul: Korea. **(2003)** November 27.
[6] L. Nelson and J. Cost, "Protecting the Common Good: Technology, Objectivity, and Privacy", Public Administration Review, vol. 62, **(2002)** September, pp. 69-73.
[7] V. M.-Schonberger, "Generational Development of Data Protection in Europe", Agre & Rotenberg edited. Technology and Privacy: The New Landscape, The MIT Press, **(1998)**.
[8] The Center for Excellence in Government.: "The New E-Government Equation: Ease, Engagement, Privacy, and Protection", **(2003)** April 17.
[9] Office of Management and Budget, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of **(2003)** September 26.
[10] J. S. Stratford, and J. Stratford, "U.K Data Protection in the Context of European Policy", Journal of Government Information,vol. 55, no. 1, **(1998)**, pp. 89-93.
[11] OECD.: Privacy Online: OECD Guidance on Policy and Practice. Paris: France, **(2003)**.
[12] K. J. Earley, "Where Do Student Privacy Laws Leave Schools?", The Education Digest, **(2004)** January, pp. 18-22.
[13] C.-S. Chung, "The Introduction of e-Government in Korea: Development Journey, Outcomes and Future", Gestion et Management Public, AIRMAP, France, vol. 3, no. 4, **(2015)**, pp. 107-122.
[14] C.-S. Chung, "Why and How the Korea transformed to the global E-Government Leaders? Focus on the United Nations E-Government Survey", Asian Association of Public Administration Conference., China, **(2015)** January 9.

Authors

Choong Sik Chung, Dept. of Public Administration, Kyungsung University**,** Professor**,** e-Government, Information Policy

DongWook Kim, Graduate School of Public Administration, Seoul National University, Dean, Professor, Ph.D. in Public Policy & Management, Informatization Policy, ICT Policy, Policy Analysis & Evaluation.

