A Study on the Protection of Biometric Information against Facial Recognition Technology

Min Woo Kim[1], Il Hwan Kim[2], Jaehyoun Kim[3], Jeong Ha Oh[4], Jinsook Chang[5] and Sangdon Park[6]

[1]Research Center, Korea Social Security Information Service, Helath&Welfare Admistration Complex B/D,
400 Neundong-ro, Gwangjun-gu, Seoul (04933), Republic of Korea
[e-mail: mwkim@ssis.or.kr]
[2]Sungkyunkwan University Law School, 25-2 Sungkyunkwan-ro, Jongno-gu, Seoul (03063), Republic of Korea
[e-mail: ilhwhan@skku.ac.kr]
[3]Department of Computer Education, Sungkyunkwan University, 25-2 Sungkyunkwan-ro, Jongno-gu,
Seoul (03063), Republic of Korea
[e-mail: jaekim@skku.edu]
[4]Sungkyunkwan University Law School, 25-2 Sungkyunkwan-ro, Jongno-gu, Seoul (03063), Republic of Korea
[e-mail: odh0524@naver.com]
[5]Software Business School, Kyonggi University, 154-42 Gwanggoysan-Ro, Yeongtong-Gu, Suwon-Si,
Gyeoggi-Do(16227), Republic of Korea
[e-mail: jinmaria@kyonggi.ac.kr]
[6]National Security Policy Research Section, National Security Research Institute,
P.O. Box 1, Yuseong, Daejeon (30147), Republic of Korea
[e-mail: sdpark@nsr.re.kr]
* Corresponding author: Sangdon Park

*Received May 4, 2023; revised June 27, 2023; accepted July 16, 2023;
published August 31, 2023*

Abstract

In this article, the authors focus on the use of smart CCTV, a combnation of biometric recognition technology and AI algorithms. In fact, the advancements in relevant technologies brought a significant increase in the use of biometric information – fingerprint, retina, iris or facial recognition – across diverse sectors. Both the public and private sectors, with the developments of biometric technology, widely adopt and use an individual’s biometric information for different reasons. For instance, smartphone users highly count on biometric technolgies for the purpose of security. Public and private orgazanitions control an access to confidential information-controlling facilities with biometric technology.

Biometric infomration is known to be unique and immutable in the course of one’s life. Given the uniquness and immutability, it turned out to be as reliable means for the purpose of authentication and verification. However, the use of biometric information comes with cost, posing a privacy issue. Once it is leaked, there is little chance to recover damages resulting from unauthorized uses.

The governments across the country fully understand the threat to privacy rights with the use of biometric information and AI. The EU and the United States amended their data protection laws to regulate it. South Korea aligned with them. Yet, the authors point out that Korean data

http://doi.org/10.3837/tiis.2023.08.009 **ISSN : 1976-7277**

aprotection law still requires more improvements to minimize a concern over privacy rights arising from the wide use of biometric information. In particular, the authors stress that it is necessary to amend Section (2) of Article 23 of PIPA to reflect the concern by changing the basis for permitting the processing of sensitive information from ‘the Statutes’ to ‘the Acts’.

Keywords: Biometric Information, Biometirc Technology, Protection of Biometric Information, Widening the scope of sensitive information, Biometric Privacy

1. Introduction

The advancements in relevant technologies brought a significant increase in the use of biometric information – fingerprint, retina, iris or facial recognition – across diverse sectors. Both in the public and private sectors, with the developments of biometric technology, widely adopt and use an individual’s biometric information for different reasons. For instance, law enforcements heavily relied on biometric information to do policing for many years. In some cases, biometric information is used for controlling an access to buildings or facilities under strict restrictions. The demand of biometric technology has resulted in significant expansion amid the COVID-19. Some governments, South Korea and China, used CCTV (closed circuit television) to carry out quarantine measures during the pandemic.

Globally, new technologies like artificial intelligence, big data, and internet of things are collecting a huge attention. Those technologies would enable the expansion of using biometric information. In the future, smart cities equipped with innovative sensors and surveillance cameras will recognize face and behaviors of the citizens in real time. Those collected biometric information, which mostly falls into the scope of personal information, will be transmitted to others, and shared for various purposes. In addition, autonomous vehicles would use biometric technology. Fingerprint scanners could replace traditional keys as to management of who can lock or unlock the car. Thus, it would be no surprise that biometric market size is expected to grow significantly. Following the wide use of biometric information, the protection of biometric information would become an important task in the digital age.

The use of biometric information seems to be irresistible across sectors. While it gives many advantages, posing a privacy risk resulting from the misuse or overuse of biometric information seems to be inevitable. Following the discussions, this article starts by reviewing the data protection laws of selected jurisdictions governing the protection and use of biometric information. The comparative review will include the Personal Information Protection Act of Korea, EU General Data Protection Regulation and US privacy laws. Additionally, this article will evaluate how relevant Korean laws govern biometric information and deliver an argument to urge a new strong legislation to protect the right of privacy arising from the increased use of biometric information.

2. The Increased Use and Importance of Protection of Biometric Information

Technological advancements are driving the use of facial recognition and its expansion is likely to be inevitable in the near future for various purposes. As discussed below briefly, biometric recognition equipped with artificial intelligence is rising. It covers not only the private sector but also to the public sector. The COVID-19 pandemic, for instance, enabled to use biometric recognition technology by replacing manual body temperature measurements.[1] This would be the beginning of the wide use of biometric recognition technology, and its use could be expanded across the sectors by the government.[2] Biometric recognitions definitely bring advantages. However, the wide use of artificial recognition may bring a concern over the rise of “Big Brother” as well as a proper balance between the public good and the possible violation of privacy rights.[3]

2.1 The Increased Use of Biometric Information

Biometric information is a type of personal information resulting from specific technical processing of data relating to the physical, physiological or behavioral characteristics of an individual for the purpose of uniquely identifying that individual, including but not limited to, retina, fingerprint, facial recognition, voice, hand geometry, vein, and keyboard and signature dynamics.[4] The scope of biometric information is expandable following the advancements in recognition technology.

Recently, biometric information turned out to be a reliable mean for security. It popularly replaces traditional password system, generally comprised of 8 to 20 alphabets letters, numbers and special characters. There are two distinctions enabling the wide use of biometric information across sectors. First, it is unique to an individual. For instance, regarding fingerprints, even identical twins sharing a very similar appearance and the same DNA sequence have different fingerprints. Second, biometric information is unlikely to be changed through the course of one’s life unless physical loss occurs to that person. These characteristics apply regardless of people’s age, race and gender. However, not all of biometric information is useable despite it is unique and unchangeable through one’s life. To be used widely, it is necessary to have following features; Universality, Distinctiveness, Permanence, Collectability, Performance, Acceptability, and Circumvention.[5]

At present, both public and private sectors widely adopted biometric recognitions for identification or authentication purposes. For instance, smartphone manufacturers like Samsung or Apple began, in early 2010, to employ biometric scanners. After the release of mobile devices with fingerprint scanners, consumers highly relied on the biometric technology for security purposes. Since then, the smartphone manufacturers expanded the use of biometric information to iris scan and facial recognition. In the private sector, social media companies provide facial recognition systems to enable the registered people to use a menu, so called “tag your friend”. Financial corporations, mostly by apps, frequently offer biometric recognition to make transactions simple and convenient. The e-commerce companies use biometric systems popularly to provide the better shopping experiences from authenticating the customers to completing their purchases. Commercial organizations control an access to classified facilities with biometric recognition technologies. In the public sector, meanwhile, law enforcements had a long history of collecting biometric information for investigation~~s~~, and they are currently putting body cameras in order to improve police officer’s safety, to acquire evidence with good quality, and to minimize their agency liability during the close contact with the suspects. Since the 9·11 terrorist attack, boarder controllers at the airport and seaport collect biometric information in order to identify suspicious travelers and prevent illegal entry to the territory. Recently, public health authorities widely took facial recognition technologies to carry out quarantine measures amid the COVID-19 pandemic responding to one of the highly contagious diseases. It would be no surprise that the growth of smart cities with latest sensors, CCTV (surveillance cameras), algorithms powered by artificial intelligence and internet of things undoubtedly increase the collection of biometric information extensively.

2.2 Importance of Protecting Biometric Information

Biometric information is a type of personal information resulting from specific technical processing of data relating to the physical, physiological or behavioral characteristics of an individual for the purpose of uniquely identifying that individual. Given that biometric information itself represents data subject, unlike general types of personal information, its protection is crucial in the digital age.[6]

As newest technologies such as artificial intelligence and big data~~,~~ are integrated with things and services, the volume of biometric information collection is increasing. However, using biometric information comes with dark sides. More collection of biometric information could produce a series of data breaches or privacy invasion. For instance, in 2015, the United States Office of Personnel Management officially reported that the 5.6 million fingerprint records of the federal employees have been stolen by the cyber-attack.[7] This incident is not the only case that put threats on biometric privacy.

The fact that biometric information cannot be changed voluntarily is crucial.[8] In general, passwords comprised of numbers, alphabets and special characters are changeable. Unlike the password, one's biometric information is hardly changeable. Thus, if it is leaked by inside data processors, or it is accessed by unauthorized parties via hacking, damages resulting from data breach cases would be massive.

Biometric information currently plays a vital role for security purposes. Technological advancements allowed us to use it with a reasonable cost. Using biometric information definitely provides easiness and convenience across sectors. In spite of the wide use, protecting individuals' biometric privacy should be highlighted in the digital era given. Data protection laws are required to respond to the changing environments driven by evolving biometric technologies.

2.2.1 South Korean Government's Use of Facial Recognition for AI-Based Immigration Systems

In 2020, the Ministry of Justice of South Korea ("MOJ") launched an audacious research project to improve airport immigration systems powered by AI-based facial recognition technologies. Its purpose was to screen suspicious activities of air travelers with CCTV cameras. The MOJ and the Ministry of Science and ICT agreed to make a special lab for private AI companies for research purposes.

A large amount of personal information was provided to the companies. It includes not only passport number, nationality, date of birth and gender information but also approximately 57.6 million photos of Korean nationals and 120 million photos of foreign nationals, without acquiring consents. Civil activists and NGOs raised a criticism over the fact that those facial images were handed over to private companies with no consents from the data subjects. The Personal Information Protection Commission ("PIPC"), a South Korean data protection authority, ran an investigation against the MOJ. The PIPC reached to a conclusion that the MOJ's project was legitimate because the Immigration Act provided a provision to process one's biometric information without acquiring a consent.[9]

2.2.2 South Korean City Government's Use of Facial Recognition for Child Care Teacher's Attendance Check

In 2022, the Goyang city government in Geoynggi Province decided to install a facial scanner against teachers and employees working at the publicly funded childcare center in order for the attendance check purposes. Before the facial scanner, a hand-written attendance tracker and fingerprint readers were adopted. However, those were inaccurate and insufficient. The city government found actual cases regarding overtime pay frauds.

Concerning the use of facial scanner, the National Human Rights Commission of Korea ("NHRCK") released a decision, suggesting that the Goyang city government is necessary to provide alternative means for employees' attendance check.[10] The NHRCK pointed out that facial recognition technologies are prone to mass surveillance against individuals by the government, and biometric data breaches are inevitable despite many sectors adopt facial scanner for identification or authentication.

2.2.3. South Korean City Government's Use of Facial Recognition to Prevent Child Abuse

In 2021, the city government of An-san, Geyonggi Province, announced to install surveillance cameras powered by AI recognition technologies to prevent child abuse cases in childcare centers.[11] The AI-based surveillance cameras are designed to spot suspicious activities or expressions of negative motions to a child with the use of real-time algorithms.

Following the city government's statement, a severe privacy concern was raised by parents and civil activists. First, to develop a sophisticated algorithm, children's facial images are necessary to be provided. Second, some parents concerned that determining whether a child abuse occurred by watching children's suspicious activities or expressions of negative emotion is hardly achievable. After discussions following the raised concerns, the city council finally cut down the entire budget requesting for AI-powered cameras.

2.3. Guideline for Human Rights concerning the Development and Use of Artificial Intelligence

In April of 2022, the National Human Rights Commission of Korea released a publication called the Guideline for Human Rights concerning the Development and Use of Artificial Intelligence. The background of the guideline came from the advancements in latest technologies. Its impact currently covers all sectors, including but not limited to, employment, finance, public service, and social welfare. For instance, Chat GPT introduced by Microsoft significantly gathers interests and concerns at present. Needless to say, artificial intelligence could improve one's quality of life. In the meantime, facial recognitions equipped with artificial intelligence are able to result in privacy invasion and discrimination. Given that the society is being reshaped by artificial intelligence, it is crucial to set up a foundation to resolve social matters arising from the use of a new technology and provide properly designed measures regarding the right to privacy. In this regard, the guideline may play a constructive role in the age of AI.

The Guideline provides core principles with the use of artificial intelligence. First, it is about dignity. The right to dignity is guaranteed by the Korean Constitution, and it is inalienable. Second, transparency is required. It is necessary to explain clearly to individuals when artificial intelligence is involved as it could put serious impact on one’s fundamental rights. In addition, all individuals should have a right to intervention regarding automotive decision-making process. Third, the right to control his or her personal data should be guaranteed. This must be provided with the principle of data minimization and the principle of data quality. Fourth, no discrimination should be made. Artificial intelligence is imperfect as many actual cases have proved that. Whenever artificial intelligence is involved, one’s information that is highly associated with privacy and human rights should be treated carefully. Fifth, the guideline urges to introduce AI and human rights assessment. With the assessment, we should analyze whether artificial intelligence is aligned with globally recognized legal principles and provide a preventive measure not to produce bias or negative results. Lastly, the government should complete legislations with regard to the use of artificial intelligence. This includes governance and structures to regulate it. In this regard, the right to remedies for individuals suffered from wrongly used artificial intelligence should be provided.

3. Biometric Information Legislations of Selected Jurisdictions

A way of identifying and verifying people with analyzing biological characteristics became common following recent technological developments. There were notable drivers that enabled the increased use of biometric information. Smartphone makers like Samsung or Apple provided biometric recognition to consumers for security purposes. Speakers equipped with smart technologies in order to respond to users such as Alexa, Echo or Siri, are currently available in the market. The COVID-19 pandemic played a significant role to adopt facial recognition as a method for contactless quarantines.

Considering the wave of biometric technologies, governments across the globe recognized threats resulting from the wide use of biometric information. Some countries like EU and US changed their legislation to protect biometric privacy. A compelling background protecting biometric privacy is that biometric information is different from types of personal information such as name, address or phone number. Generally speaking, biometric information cannot be changed by data subjects. Moreover, data processors including governments are easily able to collect biometric information from data subjects with latest devices like highly advanced surveillance camera and are able to share biometric information with law enforcements, resulting concerns the right of privacy and digital big brother.[12] This view has been supported by the Constitutional Court of Korea, pointing out that “Even if the collected fingerprint information is disposed of or its use is discontinued, the leaked biometric information can continue to be used for the purpose of verifying the individual's identity, and in turn, resulting damages can occur extensively throughout one’s lifetime”.[13] In addition, the leaked biometric information, considering the intrinsic privacy-relations, could be a bridge to analyze an individual's private life. Thus, biometric information should be treated carefully, and should require a strong protection by laws.[14] This chapter would review and analyze biometric legislations of selected jurisdictions.

3.1 EU

In 2016, the European Union enacted the EU General Data Protection Regulation ("EU GDPR"). EU GDPR replaces the outdated data protection law, EU Data Protection Directive, 95/46/EC. The reason to enact a new data protection law was to harmonize data protection laws across all member countries. It also aimed to provide a greater protection and rights given to individuals. The Directive, in fact, lacked power to enforce its principles and contents to the member countries. It only played a guideline role under the EU legal system. Eventually, a disparity in terms of legal binding power between directives and regulations produced a loophole. Unlike the Directive, EU GDPR holding a legal binding power across the member states is expected to serve as a new global data protection standard with general principles and rules in processing personal information.[15]

EU GDPR defines that biometric information is related to the physical, physiological or behavioral characteristics of a natural person, which can make an identification of that natural person. In fact, this is a huge change following the fast-evolving data environment since the Directive enacted in 1995 lacked provisions with respect to the regulation on biometric information. Pursuant to the article 8(1), the Directive only stated the definition, "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life". It may be argued that fingerprints could fall into the scope of data concerning health, but that is insufficient since individual health data just embraces personal medical history or symptoms.

Meanwhile, EU GDPR sits in a different position in that it added the term of biometric data with genetic data and data concerning health or natural person's sexual orientation to the definition. Pursuant to the article 2(14), it stated as the definition, "[p]ersonal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person", which allow or confirm the unique identification of that natural person such as facial images or dactyloscopic data.

To process biometric data, EU GDPR Recital (53) clarified that additional conditions with limitations are necessary, and its process of biometric data, a type of special categories of personal data, is prohibited only with limited exception under the Article 9. Thus, EU GDPR strictly regulates the process of biometric information. This is a reflection of EU GDPR's intention to provide a strong protection regarding the use of biometric information.

3.2 United States

The United States has distinctive data protection legislations if it is compared with South Korea or EU data protection legal system. The US lacks a single universal data protection law that covers all sectors. Therefore, each sector is regulated by different data protection laws, i.e. the Privacy Act of 1974, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and the Children's Online Privacy Protection Act, to name a few. Recently, however, a notable effort is being made in the level of the US Congress. The House put efforts to enact a federal data protection law that covers all sectors comprehensively by introducing the American Data Privacy and Protection Act, H.R. 8152, sponsored by the Energy and Commerce Committee members, Frank Pallone, Jr, the committee chairman, and Cathy McMorris Rogers, the committee ranking member.

Pursuant to the bill, it provides the definition of biometric information. The section 2(3) states that, “any covered data generated from the technological processing of an individual’s unique biological, physical, or physiological characteristics that is linked or reasonably linkable to an individual”. It includes fingerprints, voice prints, iris or retina scans, facial or hand mapping, geometry, or templates and gait or personally identifiable physical movements. However, the scope of biometric information excludes; a digital or physical photograph, an audio or video recording, and data generated from a digital or physical photograph, that cannot be used to identify an individual.

No doubt that congressional efforts to make an American comprehensive data protection law is noteworthy. In spite of the efforts to advance the bill with favorable votes, it reached to a deadlock due to the clause of preemptive application against state data protection laws and the clause recognizing the right of action to individuals.[16]

Besides existing federal data protection laws, some states have completed to make biometric legislations in order to respond to the increased use of biometric information across sectors. In 2008, the state of Illinois enacted a law for biometric information called the Illinois Biometric Information Privacy Act (“BIPA”).

BIPA specified, “biometrics are unlike other unique identifiers that are used to access finances or other sensitive information”. It also defines biometric identifier by stating retina or iris scan, fingerprint, voiceprint or scan of the hand or face geometry, and further stated that biometric information means any information based on an individual’s biometric identifier used to identify an individual. Basically, BIPA makes unlawful when companies use biometric recognition technology without acquiring the data subject’s consent. One thing notable is that BIPA gives the right of action to individuals aggrieved by incompliance. The right of action given to aggrieved data subjects led IT companies to face lawsuits such as cases, i.e. Rosenbach v. Six Flags Entertainment Corp, Patel v. Facebook, Inc. and Bryant v. Compass Group USA. Regarding the private right of action, the Court of Rosenbach v. Six Flags Entertainment Corp. held that actual injury or adverse effect, beyond violation of his or her rights, is unnecessary to constitute the aggrieved person under the Act.[17]

The state of California enacted the California Consumer Privacy Act of 2018 (“CCPA”), effective in January of 2020. This data protection law modeled after EU GDPR. CCPA provides 11 different types of personal information, and biometric information falls into one of those 11 types. Following the definition, CCPA states that biometric information is “an individual’s physiological, biological or behavioral characteristics, including an individual’s deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity”. The Act also provides several examples of biometric information protected by the law. It includes imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template can be extracted (face-print, a minutiae template, voiceprint), and keystroke patterns, gait patterns, and sleep, health, or exercise data that contain identifying information.

Unlike BIPA, CCPA does not grant right of action to individuals. However, pursuant to section 1798.155. the state of California is able to bring a lawsuit asking a civil penalty of no more than two thousand five hundred dollars for a violation, or seven thousand five hundred dollars for an intentional violation. These penalties are assessed and recovered in a civil action brought by the name of the California Attorney General. The penalties assessed in a civil action or settlements are designed to deposit in the Consumer Privacy Fund.

In November of 2020, the state of California passed the California Privacy Rights Act of 2020 (“CPRA”) which took effect on January 1, 2023. This law was passed by the voters in California. Although CPRA seems to be different from CCPA, CPRA was built on CCPA. The main difference between two Acts is that CPRA emphasizes the right of privacy and put more obligations to data processors.

CPRA defines sensitive information, which is divided into two different categories. One is direct identifiers while the other is highly private information. The scope of highly private information includes not only biometric information but also precise geo-location, ethnicity, religion, genetic and biometric information, sexual orientation, and the contents of email and text messages unless those messages were sent to the business in question. Pursuant to section 1798.140 of CPRA, it defines biometric information, “an individual’s physiological, biological or behavioral characteristics, including an individual’s deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity”.

3.3 South Korea

Data protection laws of South Korea lacked provisions to protect biometric information before 2020. However, with a series of discussions, the National Assembly of South Korea significantly changed the Personal Information Protection Act (“PIPA”) in 2020, serving as a general law, along with the Act on Promotion of Information and Communication Network Utilization and Information Protection and the Credit Information Use and Protection Act, which are special laws applicable to specific business areas. The compelling background for the amendment was to respond to the emerging of newest data technologies such as Artificial Intelligence, Big Data, Internet of Things and Clouds. Those new data technologies are mainly designed to collect and store a huge amount of personal information. Eventually, it is expected to raise a serious concern over the right to privacy given that the excessive use of personal information by the government and corporations is undisputable. By amending the data protection laws, South Korea could align with global legislations.

PIPA contains a provision with regard to biometric information. Pursuant to the article 18 of the Enforcement Decree of PIPA, it provides a definition of biometric information, “Personal information resulting from specific technical processing of data relating to the physical, physiological or behavioral characteristics of an individual for the purpose of uniquely identifying that individual”. Following the article 23 of PIPA, Decree specifies the limitation of the processing biometric information which falls into the scope of sensitive information. Data processors are only allowed to process biometric information when (1) they acquired consent from data subject or (2) other statutes require or permit the processing of one’s sensitive information. South Korea put efforts to amend their data protection laws following the technological developments regarding biometric information. However, rather than putting the definition of biometric information such as what biometric information exactly means in the Clause, which is easily found in the EU GDPR, the PIPA merely contains the legal-conceptual explanation of biometric information that may result in difficulties in understanding it for general individuals.[18]

3.4 Summary

As discussed above, data protection laws across the globe have been amended or have been newly enacted in order to respond to the wide use of biometric information. A common approach between governments is that biometric information falls into the scope of sensitive information in many cases. The table below is a brief comparison of relevant data protection laws of selected jurisdictions. **(*See Table 1*)**

Table 1. Comparison of Biometric Legislation between Selected Jurisdictions

Name of Law		**Definition**
EU	GDPR	Personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or fingerprint data
US	ADPPA (H.R. 8152)	Any covered data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that is linked or reasonably linkable to an individual
	BIPA (Illinois)	any information based on an individual's biometric identifier (a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry) used to identify an individual
	CCPA (California)	An individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity
	CPRA (California)	An individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity
South Korea	PIPA Enforcement Decree	Personal information resulting from specific technical processing of data relating to the physical, physiological or behavioral characteristics of an individual for the purpose of uniquely identifying that individual

4. Public Survey on the Use of Biometric Technology (Intelligent CCTV)

A public survey cited in this paper, a part of research paper published by the National Human Rights Commission of Korea, was conducted by a private consulting firm in 2021. The public survey was conducted with 1,000 adults over 17 years old. Those 1,000 respondents were selected by gender, age and region.[19]

The survey aims to collect and analyze; (1) public perception in smart CCTV (2) whether the respondents agree or disagree with installing intelligent CCTV and (3) concerns such as privacy invasion or behavioral effects resulting from intelligent CCTV. Before diving into the result of public survey, a notable difference between traditional CCTV and intelligent CCTV should be addressed. The intelligent CCTV is a surveillance camera equipped with software and algorithms powered by artificial intelligence while the traditional CCTV lacks those modern technologies so it remains to a passive recording role.

The public survey approaches to two different groups such as the respondents who are aware of smart CCTV accounting for 510 individuals and the rest of the respondents accounting for 490 individuals who are not aware of smart CCTV. Both were provided with the same questions during the survey.

4.1 Relationship between intelligent CCTV and safety

First of all, the public revealed an overwhelmingly positive view that intelligent CCTV provides safety. This has no exception whether the respondents lack knowledge or perception regarding intelligent CCTV or not. **(*See Table 2*)** More than 80% of the respondents agreed that intelligent CCTV would bring safety.

This positive view is shared with the respondents living in both urban area and rural area. A favorable response to intelligent CCTV and safety account for more than 80%. Small number of the entire respondents disclosed that intelligent CCTV has no relevance to safety.

Table 2. Relationship between intelligent CCTV and safety

		Agree	**Neutral**	**Disagree**	**Don't know**	**Total**
510 out of 1,000	Male	80.8%	14.4%	4.1%	0.7%	100%
	Female	83.4%	14.4%	1.4%	0.8%	100%
	Urban	82.0%	14.4%	3.2%	0.4%	100%
	Rural	80.2%	15.1%	0.4%	0.7%	100%
490 out of 1,000	Male	73.4%	18.4%	3.8%	4.4%	100%
	Female	70.9%	17.3%	7.6%	4.2%	100%
	Urban	73.0%	18.2%	5.0%	3.8%	100%
	Rural	67.3%	15.3%	9.7%	7.7%	100%

4.2 Relationship between intelligent CCTV and privacy concern

Despite smart CCTV could enhance safety, the public revealed a concern over the use of latest surveillance system with facial recognition technology. Approximately, the half of the respondents by gender stands align with the view that intelligent CCTV could infringe the right to privacy and bring possible damages caused by data breaches. **(*See Table 3*)** However, the respondents living in rural area less concerned about the issue of privacy and data breach than the respondents in urban area.

Table 3. Relationship between smart CCTV and privacy concern

		Agree	**Neutral**	**Disagree**	**Don't know**	**Total**
510 out of 1,000	Male	52.2%	32.5%	14.3%	1.0%	100%
	Female	52.5%	34.1%	12.5%	0.9%	100%
	Urban	53.4%	33.0%	12.9%	0.6%	100%
	Rural	39.3%	34.8%	21.3%	4.7%	100%
490 out of 1,000	Male	45.4%	40.0%	12.6%	2.0%	100%
	Female	46.3%	35.9%	14.3%	3.5%	100%
	Urban	48.3%	36.6%	12.7%	2.4%	100%
	Rural	32.4%	42.5%	18.9%	6.2%	100%

4.3 The sequential concerns over intelligent CCTV

The public survey provided that the biggest concern over the installation of intelligent CCTV is as to privacy invasion. (***See Table 4***) The respondents, regardless of their gender or the area of residency, expressed as the first concern that the right of privacy could be compromised by smart monitoring system of intelligent CCTV.

The other concern was the unauthorized processing of personal data recorded by the camera powered by artificial intelligence. It was followed by the concern over behavioral effects, i.e. chilling effect due to the pervasiveness of intelligent CCTV. Some of the respondents worried about cybersecurity issues such as insider threat or hacking with malicious intentions.

Table 4. The most concerns over smart CCTV

		Privacy invasion	**Unauthorized processing**	**Behavioral effects**	**Cybersecurity weakness**	**Etc.**	**Total**
510 out of 1,000	Male	47.2%	19.9%	11.3%	6.9%	14.7%	100%
	Female	46.0%	20.6^	9.5%	8.1%	15.8%	100%
	Urban	47.8%	20.6%	10.0%	7.2%	14.4%	100%
	Rural	32.9%	15.8%	16.9%	10.4%	23.9%	100%
490 out of 1,000	Male	47.0%	22.0%	7.3%	7.3%	14.4%	100%
	Female	45.7%	22.7%	9.4%	9.7%	13.1%	100%
	Urban	47.8%	23.3%	8.0%	8.8%	12.0%	100%
	Rural	41.6%	14.4%	11.2%	8.6%	24.1%	100%

4.4 Whether intelligent CCTV should be used in caution

With respect to the use of intelligent CCTV, the public survey asked the respondents as to whether the respondents agree or disagree with the following statement; Facial recognition surveillance cameras should be used carefully since the human rights including the right of privacy are most likely to be invaded. (***See Table 5***)

The result shows that the about two-third respondents, at least, disclosed their opinion expressing concerns over the association between intelligent CCTV and privacy. Only small number of the respondents disagreed so that the use of intelligent CCTV has nothing to do with the human rights.

Table 5. Should intelligent CCTV need to be used in caution?

		Agree	Neutral	Disagree	Don’t know	Total
510 out of 1,000	Male	67.0%	23.7%	8.6%	0.7%	100%
	Female	73.7%	15.8%	9.1%	1.4%	100%
	Urban	70.6%	19.8%	9.1%	0.6%	100%
	Rural	61.4%	27.3%	6.1%	5.2%	100%
490 out of 1,000	Male	64.1%	26.1%	8.9%	1.0%	100%
	Female	64.9%	22.1%	11.0%	2.0%	100%
	Urban	65.0%	24.1%	9.8%	1.2%	100%
	Rural	61.9%	22.2%	11.7%	4.1%	100%

As the survey reveals, many respondents clearly agree that the smart CCTV makes a huge contribution to enhancing public safety. Meanwhile a concern over privacy comes with the use of smart CCTV. The extent of concern over the use of smart CCTV also includes unauthorized processing of recorded data, behavioral effects (chilling effect) and cyber security weakness such as hackings. Due to the probable concerns, many respondents agree that smart technology with facial recognitions should be used with cautions. The wide use of facial recognition is likely to be inevitable as it provides convenience and accuracy, yet it is necessary to protect the right of privacy given to individuals as well. The privacy laws could play a role on that. If the current laws lack proper protections, a new approach regarding regulation taking after the EU and the United States should be taken considering the expansion of biometric technology.

5. Conclusion

The fast-changing environments driven by biometric technologies changed data protection legislations across the globe. EU changed its data protection law, EU GDPR, to protect privacy. Although the US lacks a comprehensive data protection law, some states like Illinois or California enacted their own data protection law to regulate the use of biometric information. Equivalent to EU and the US, South Korean data protection law, PIPA, has been amended in 2020, and it contains a relevant provision regarding biometric information.

The public survey discussed in the above chapter clearly discloses both the bright side and the dark side with regard to the use of biometric information. In the survey, CCTV (surveillance camera) powered by biometric technologies was regarded as a way to enhance public safety. On the other hand, many respondents expressed a concern that those surveillance cameras equipped with latest technologies could put the right of privacy at risk. The risk is not limited, but expandable to unauthorized accesses, the chilling effect and weakness in cybersecurity.

However, it is noteworthy to point out that the 2020 PIPA amendment is likely to be insufficient. Under the Korean data protection law, PIPA, after the amendment in 2020, added the provision to define biometric information. The relevant provision for details for protection is provided by the Enforcement Decree of PIPA, the lower rank of statutes, rather than PIPA itself. The Enforcement Decree has the complementary effect to the law (PIPA), and in turn, its level of protection cannot be effectively guaranteed. Therefore, it is necessary to add in the article 23 of PIPA itself that articulates the scope of sensitive information, rather than regulating by the Enforcement Decree. The clause of biometric information should be added in the article 23 of PIPA.[20] In other words, expanding the scope of sensitive information is necessary by adding 'biometric information' in the article 23 of PIPA.

Moreover, the Article 23 of PIPA specifies legal grounds in order to process sensitive information; (1) consent from the data subject, or (2) where other statutes require or permit the processing of sensitive information. The "statutes" under the Korean legal system embraces not only the "Act" but also the "Enforcement Decree". While the "Act" is required to pass legislative procedures by the legislative body, the National Assembly of Korea, the "Enforcement Decree" is required to pass procedures only by the Administrative Branch. This creates a leeway regarding the data protection level. Thus, it is necessary to amend Section (2) of Article 23 of PIPA as follows; (2) where other Acts require or permit the processing of sensitive information.[21]

Advantages of using biometric information are manifest. Biometric information never gets changed during the course of one's life and unique to all of individuals regardless of age, race or gender. Many sectors – airport security, law enforcements, online banking and mobile shopping – have already adopted biometric information. Given those features and landscapes, the use of biometric information is likely inevitable to increase. Meanwhile, the use of biometric information comes with substantial cost so that it poses a risk to one's privacy. In particular, new technologies like AI, Big Data, Internet of Things and Clouds, would be much stronger drivers in collecting biometric information in the near future. To protect biometric privacy, a properly designed legislation could provide strong protections. Thus, data protection laws should pay attention to the changing data environments.

References

[1] Meredith Van Natta et al, "The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic," *Journal of Law and the Biosciences*, vol. 7 no. 1, pp. 5-6, 2020. Article(CrossRef Link)

[2] Kim Myung Yeop, "A Study on Legal Improvement of Smart City and Information of Facial Recognition," *Ilkam Real Estate Law Review*, Vol 25, pp. 78-79, 2022. Article(CrossRef Link)

[3] Lee Min-Yeong, "Issues on Protecting Personal Image Data managed by Artificial-Intelligent CCTV," *Soongsil Law Review*, vol. 52, pp. 210-214. 2022.

[4] Kim Il Hwan, "A Constitutional study on the Bio-information protection," *Human Rights and Justice, Korea Bar Association*, vol. 334, 2005. Article(CrossRef Link)

[5] Anil K. Jain et al, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20, 2004. Article(CrossRef Link)

[6] Kim Il Hwan, "A Study on the Bio-information protection law," *Public Land Law Review*, vol. 33, pp. 355-384, 2016. Article(CrossRef Link)

[7] Andrea Peterson, "OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought," *Washington Post*, 2015. Article(CrossRef Link)

[8] Kim Song-ok, Kwon GeonBo, "The Use of Biometric data by Facial Recognition Technology and Its Limits - Focusing on laws for identification of missing children -," *Korean Constitutional Law Asscciation*, vol. 27 no.1, pp. 115-163, 2021. Article(CrossRef Link)

[9] Personal Information Protection Commission, Letter of Deliberation and Resolution, 2022-07-046, 2022. 4. 27. Article(CrossRef Link)

[10] National Human Rights Commission of Korea, 22Petition0139800, 2022. 9. 16. Article(CorssRef Link)

[11] Cheon Ho Sung, Several local governments in S. Korea are building AIs using CCTV data without subjects' consent, 2021.

[12] Kwon Geonbo et al, “The Information Human Rights in the Age of Intelligent-information Society,” *National Human Rights Commission of Korea*, p. 161, 2022. Article(CrossRef Link)

[13] Constitutional Court 2011Hun-Ma731, May 28, 2015. Article(CrossRef Link)

[14] Cho Kyu-beom, “A Legislative Study on the Protection of Biometric Information,” *Public Law Review*, Vol 37. No. 1-2, pp. 181-200, 2008. Article(CrossRef Link)

[15] Kim In Seok et al, “Research on Developing Strategies for Personal Information Protection in Response to Strengthening International Interoperability and the Era of Intelligent Information Technology,” *Personal Information Protection Commission Research Paper*, p. 5, 2016. Article(CrossRef Link)

[16] Jonathan M. Gaffney, et al, “Overview of the American Data Privacy and Protection Act, H.R. 8152,” *Congressional Research Service Report*, p. 5, 2022. Article(CrossRef Link)

[17] Rosenbach v. Six Flags Entertainment Corp. 2019 IL 123186, Article(CrossRef Link)

[18] Lee Kwon Il, “Eine verfassungsrechtliche Studie zu dem Schutz und der Verwendugn der Biometrischen Daten,” *Institute of Law Studies PUSAN NATIONAL UNIVERSITY*, vol. 61, no. 2, p. 5, 2020. Article(CrossRef Link)

[19] Korea Information Management Assessment, Survey on the current status and improvement measures for the use of intelligent CCTV and facial recognition systems and protection of personal video information, National Human Rights Commission of Korea, 2021. Article(CrossRef Link)

[20] Kim Il Hwan, “A Study on the Legislative Improvement Plan for Protection and Utilization of Biometric Information,” *European Constitution*, vol. 30, pp. 489-529, 2019. Article(CrossRef Link)

[21] Kwon Geonbo et al, “Personal Information Protection Legislation Improvement Plan for Response to Intelligent Information Society,” *Personal Information Protection Commission Research Paper*, p. 177, 2017. Article(CrossRef Link)

Dr. Min Woo Kim is a researcher at Korea Social Security Information Service, one of public institutions under the Ministry of Health and Welfare of South Korea. He received Ph.D. in Law from Sungkyunkwan University. His academic interest area includes data protection laws and privacy rights.

Professor Il hwan Kim is the Dean of Sungkyunkwan University (SKKU) Law School and heads the SKKU Science & Technology Law Institute. He served as the Chairperson of the Personal Information Dispute Mediation Committee. He received his bachelor of laws and master of laws from Sungkyunkwan University and earned his Ph.D. in law degree from the University of Mannheim in Germany. His academic interest area includes constitutional law and data protection law.

Professor Jaehyoun Kim currently serves as an executive vice-president of Sungkyunkwan University (SKKU). He received his B.S. degree in mathematics from SKKU, Seoul, Korea, M.S. degree in computer science from Western Illinois University and Ph.D. degrees in computer science from Illinois Institute of Technology in USA. He served as a Chief Technology Officer at Kookmin Bank in Korea before he joined the Department of Computer Education at Sungkyunkwan University in March 2002. As a professor at Sungkyunkwan University, his research interest areas include software engineering & architecture, e-Learning, SW/AI education and computer-based learning.

Dr. Jung Ha Oh is a researcher at Sungkyunkwan University (SKKU) Science& Technology Law Institute. She received her master of laws degree and Ph.D. in law degree from Sungkyunkwan University. Her academic interest area includes artificial intelligence, algorithm, personal data and constitutional law.

Professor Jinsook Chang is an assistant professor at Software Business School of Kyonggi University and teaches International Economic Law. She received her bachelor of laws, master of laws and Ph.D. degree from Sungkyunkwan University. She also earned LL.M. with a specialization certificate in International Law at American University Washington College of Law, Washington DC, USA. Her overall research is mainly aimed at integrating International Economic Law with Human Rights.

Dr. Sang Don Park is a senior researcher at the National Security Research Institute. He researches about the law and policy. He received his LL.B. LL.M. and Ph.D. in law degree from Sungkyunkwan University. His research interest areas include constitutional law theory, administrative law theory and public laws on ICT and security.