Legal Issues in the Introduction of Compelled Decryption According to Device Unlock Limits

Chohee Bae[1], Sojung Oh[2], Sohyun Joo[1], Jiyeon Joo[2], and KyungLyul Lee[3*]
[1] Department of Law, Sungkyunkwan University, Seoul, Korea
[e-mail: {b55111506, joo.sh91}@gmail.com]
[2] Department of Forensic Sciences, Sungkyunkwan University, Seoul, Korea
[e-mail: mira0809@naver.com, joojiyeon0313@gmail.com]
[3] School of Law, Sungkyunkwan University, Seoul, Korea
[e-mail: klee04@skku.edu]
*Corresponding author: KyungLyul Lee

Received August 14, 2022; revised October 16, 2022; accepted November 20, 2022; published February 28, 2023

Abstract

With the emergence of advanced encryption technologies such as Quantum Cryptography and Full Disk Encryption, an era of strengthening information security has begun. Users respond positively to the advancement of privacy-enhancing technology, on the other hand, investigative agencies have difficulty unveiling the actual truth as they fail to decrypt devices.

In particular, unlike past ciphers, encryption methods using biometric information such as fingerprints, iris, and faces have become common and have faced technical limitations in collecting digital evidence. Accordingly, normative solutions have emerged as a major issue. The United States enacted the CLOUD Act with the legal mechanism of 'Contempt of court' and in 2016, the United Kingdom substantiated the Compelled Decryption through the Investigatory Powers Act (IPA). However, it is difficult to enforce Compelled Decryption on individuals in Korea because Korean is highly sensitive to personal information. Therefore, in this paper, we sought a method of introducing a Compelled Decryption that does not contradict the people's legal sentiment through a perception survey of 95 people on the Compelled Decryption. We tried to compare and review the Budapest Convention with major overseas laws such as the United States and the United Kingdom, and to suggest a direction of legislation acceptable to the people in ways to minimize infringement of privacy. We hope that this study will be an effective legal response plan for law enforcement agencies that can normatively overcome the technical limitations of decoding.

Keywords: Compelled Decryption, Decryption, Encryption, Privilege Against Self-Incrimination, Personal Information Protection

A preliminary version of this paper was presented at APIC-IST 2022, and was selected as an outstanding paper. This version includes the perception survey of the people's legal sentiment about Compelled Decryption. This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea(NRF-2021S1A5A2A03068277).

http://doi.org/10.3837/tiis.2023.02.017 **ISSN : 1976-7277**

1. Introduction

1.1 Research Aims

The Miniaturization and High-Capacity System of devices were fascinating to attract public attention. Therefore, unlike past ciphers, which were simply composed of letters and numbers, ciphers using Personal Identification Number(PINs), patterns, and biometric information have emerged. Furthermore, in application of technologies to encrypt files, drives, and even for whole devices have become common. However, due to the failure to decrypt advanced cryptographic technologies, the number of cases that have difficulty finding the truth has increased rapidly. Typically, the investigation progress was slow in the case of Nth Room, which became a social issue due to the production and distribution of child sexual exploitation in 2020[1], and the Samsung Galaxy S21 was confiscated in the case of bribery in 2021, but when someone attempted to decrypt it arbitrarily, the investigation was difficult due to the privacy policy that all data stored on the device was deleted[2]. Cryptographic technology emerged under the name of 'personal information protection', on the other hand, it is emerging as a new challenge that must be solved socially by providing both sides, such as causing fundamental difficulties in discovering substantive truth.

Law enforcement agencies, such as investigation agencies, respond to various types of encryption, figuring out decryption methods. Still, manufacturers enhance their encryption technologies and strengthen their policies whenever decryption methods are known. The circumstance leads to technical limitations and increases difficulties in solving cases. In addition, due to strong guidelines for personal information protection and legal procedures, there is a good possibility of controversy over legality and it is difficult to ensure the reliability of the evidence collected in Korea. We therefore present the necessity of introducing the Compelled Decryption based on the technical limitations of unlocking the device. In addition, we would like to present an efficient and realistic introduction plan by reviewing legal issues. To this end, in this paper, we discuss both methods that can be normatively overcome instead of technical measures for various cipher types. We hope that this study will help law enforcement agencies that face technical limitations on device encryption can normatively overcome and establish substantive truths about events.

1.2 Research Methods

In order to understand the public's perception of the introduction of the Compelled Decryption, a survey was conducted on the general public and experts. And based on the results, we tried to present a realistic alternative that everyone could accept. This study finally selected 95 survey participants using the purposive sampling method[3]. The survey was conducted between June 22, 2022, and July 12, 2022. It was intended to collect opinions from scholars interested in compelled decryption system and ordinary citizens. This survey also sought to recognize problems caused by the introduction of the compelled decryption system from a legal and technological perspective. Hence, we divided sample into 3 groups : (A) Individuals specialize in decryption system that are aware of or heard of compelled decryption, (B) ordinary citizens, (C) legal and technical experts. A total of 95 respondents participated, including 43 in the group (A), 31 in the group (B), and 21 in the group (C). By gender, 42 males and 54 females. by age, 41 in their 20s, 41 in their 30s, 11 in their 40s, 1 in their 50s, and 1 in their 60s. By specialization, respondents consist of 24 from liberal arts and sciences, 32 from social sciences, 23 from engineering, 6 from natural sciences, and 9 from arts and physical education. 92% of participants

set passwords on their mobile devices, and 48.2% out of them set additional passwords for applications. Through this, the scope of compelled decryption system needs to be extended to the mobile devices and the applications. We presented the questionnaire based on scholars' papers who proposed opinions for or against the introduction. For example, the first question was whether the respondent was correctly aware of the compelled decryption system. In addition, we divided a subject into individuals and third parties and presented problems from each point of view, then questioned whether it would be appropriate to enforce the system. The questionnaire presented that if the subject is an individual, it may be a severe invasion of privacy. In contrast, if the issue is a third party, it may affect sales due to be stigmatized as a company that provides users' information. The questions were answered on 5 point scale, and as for the measurement scale, the metric scale with interval scale form, precisely the Likert-type scale, was used[1][4]. The Likert-type scale was chosen in this survey because the analysis result was only possible to allow advanced interpretation by combining with the results of other questions but did not affect between questions. Finally, the analysis focused on identifying citizens' legal minds based on survey results.

2. Advances in Encryption Technology and Limitations in Decryption

2.1 Advances in Encryption Technology

Passwords are the most well-known means of control that require authorization to perform tasks such as modification and generation through plaintext. Information processing technology made it easier to operate data and conveniently obtain it in open spaces like Online but on the one hand, by restricting access to data, the need to restrict unauthorized work performance has increased[5]. As a result, the importance of personal information protection is strengthened and research on solid technologies is required[6], and the targets for applying Encryption Technology are gradually expanding such as clouds and devices beyond files and drives. The types of Encryption are also diversifying, they can be classified into Knowledge-Based such as Password, Personal Identification Number, Patterns, and Biological Characteristics-Based such as voice and fingerprints[7][8]. The development of Encryption Technology has also brought about great changes in Cryptosystem. The basic principles are the same, but Biometrics that encrypts Biometric Data using one-way function, Steganography that conceals secret message and Quantum Cryptography that requires different decryption keys when hacking is being developed. Furthermore, hardware and software equipped with the latest encryption technology are maintaining a growth trend at an unexpected pace. Typically, the device is equipped with Full Disk Encryption, which encrypts the entire disk or volume with bitwise operation[9]. Even there are software that can easily perform encryption, such as Pretty Good Privacy (PGP), has increased. We cannot be verified real data if it is successful in decrypting the media or fails to decrypt internal data stored on the device even if a copy is obtained[10]. Decryption is the process of converting ciphertext into plaintext and requires the server to present a key to gain Access Rights. Various Decryption Techniques are being studied according to the type of cypher, but in order to apply them to prove Admissibility of Evidence, trust and legality in the process of collecting evidence must be proven. Even if it is technically possible, if there is a legal dispute, it cannot be said that the Admissibility of Evidence is unconditionally guaranteed, and the encryption technology that is difficult to obtain the decryption key continues to emerge, revealing technical limitations. For example,

[1] The metric scale is measured without any influence between different questions, and there is no reference point or comparison with other research subjects. Among them, the Likert-type scale is a scale in which respondents answer questions according to the category suggested by researchers.

the public began to recognize the need for the Compelled Decryption in 'the Case of Former Prosecutor', which was impossible to digital forensics by citing the Right to remain silence. Thereof, the discussion was active across political and academic as the Minister of Justice ordered a review of the "Mobile Phone Compulsory Unlock Act"[2][11]. According to the results of the survey conducted by this researcher team, regarding "Do you think Korea needs to introduce a decryption order?", 54% of respondents said "need", 40% said "normal" and 6% said "no need." **Table 1**. The reason for supporting the introduction were 50 people who said, "It is necessary for solving serious crimes such as National Terrorism and Digital Sexual Crime and Public Security," and 34 people said, "It hinders the investigation to reveal the actual truth." In other words, the public recognizes the necessity of bring in Compelled Decryption through a series of events that occurred in the past day, and recognizes it as necessary for solving serious crimes occurring in the state **Table 2**.

Table 1. Results of "Do we need to deploy Compelled Decryption?"

	Graduate students		Ordinary person	Experts			Total
	A	B	C	D	E	F	
Strongly agree	4	2	3		2	1	12
Agree	9	12	13	1	2	2	39
Neutral	4	8	13	3	5	5	38
Disagree		1	2				3
Strongly disagree	2		1				3

Table 2. Results of " Why are you in positive of introduction?"

	Graduate students		Ordinary person	Experts			Total
	A	B	C	D	E	F	
Because it's an obstacle to the investigation to reveal the real truth	12	4	14		3		33
It's already being implemented in other countries, including England and Australia	1	1	1				3
Because it is essential for public safety, such as serious crimes such as national terrorism and digital sex crimes	12	14	15	1	4	3	49
Because we can't solve it any other way except for a decryption order	1	5	1	1		3	11

[2] Nevertheless, 32 people answered "I know" and 63 people "I don't know" about the 'Compelled Decryption System'. Eleven, half of the university (graduate**)** students, answered "I know," but 18 out of 20 police school graduates said they did not know. 5 out of 8 legal experts said they knew about the system, but 9 out of 13 technical experts or practitioners said they did not know. Since the Compelled Decryption System is still a professional system and only discussions are active in academia, it is understood that most people are less aware of it except legal experts and related students.

2.2 Types of Technical Limitations of Decryption Technology

2.2.1 Algorithm-Based Decryption Technology

A traditional Decryption Technology is Session Hijacking. It is a technology that acquires a decryption key in the process of exchanging keys through analysis of algorithmic principles. It can neutralize the internal security network by pretending to be a normal user[12], Smishing and Phishing are used as the main means for 'key take-over'. In order to obtain the internal system state that is already logged in, it can be easily propagated through apps or the like and disguised as a legitimate user at any time[13]. In Germany and the United States, it is a useful method to trick users into securing evidence of crimes against Secure Instant Messenger or Secure System. In fact, the "Secure Instant Messenger," developed by the U.S. Federal Bureau of Investigation(FBI), was used by international criminal organizations as a means of communication to conspiracy crime, and through this, it succeeded in preventing crime and arresting 800 people[14]. In Germany, it is also known that a number of criminals were arrested using Remote Monitoring Software, that is to say ‘Bundestrojaner(German for state-sponsored trojan horse, Federal Trojan)’. However, it is rare to succeed in decryption by analyzing the structure in detail to investigate encrypted evidence. In oversea, law enforcement agencies order manufacturers to develop a kind of hacking version of encryption and provide it to investigative agencies. However, it was not actually executed by claiming that it was unconstitutional act of infringing personal information. Although the investigative agency recognizes the need to use technical means to respond to Encryption for the purpose of collecting evidences, the current Criminal Procedure Act lacks applicable provisions for the investigative agency's secret investigation[15]. In particular, there is still a dispute whether the act of monitoring and viewing or collecting stored content (Online Search) by secretly accessing the user's system[16] can be treated as an Entrapment or without due process. Moreover, since it is necessary to access the system distributed by the investigative agency while logged in with the user's account, it is difficult to apply to evidence that have already been seized.

2.1.2 Knowledge-Based Decryption Technology

Knowledge-Based Decryption(What You Know) authenticates through passwords previously shared by users and servers. Representative decryption of systems that have access to accounts such as e-mail and cloud includes Brute Force Attack, Dictionary Attack, and Educated Guess Attack. A brute force attack can access the user's sensitive credentials stored on the server by randomly substituting a string that can be combined with user’s information [17]. A Dictionary Attack assumes that there is a decryption key in a kind of 'dictionary' that lists expected passwords[18]. And an Educated Guess Attack is to guess user information and access it[19]. At this time, user information such as birthdays and anniversaries needs to be secured. There are two methods one is "OSINT" which obtains information from open sources and "Tracking". In fact, in the "Case of Illegal Comment Manipulation[20]" using TrueCrypt, it is known to have succeeded in decryption by securing that the Chinese astrologer’s name(he usually believes in) and the Internet cafe named ‘KKM’, combined that information and used it as a password. Thereof, they could get some evidence.

However, passwords use a total of 95 characters, including letters, numbers, and spaces, and do not limit the number of digits. If it is 10 strings, the number of cases are 95^{10} that is, in the case of 59,873,693,923,837,890,625. In addition, if special characters are used, it takes more than 100 years to substitute them all. PINs use numbers of 0-9 and usually use 4 or 6 digits. In this case, the probability of successful decryption is respectively one in ten thousand and one in one million. The pattern must constitute a trajectory from nine dots, the connection of four or

more dots. It spawns the maximum number of 389,112 cases. As such, the number of cases that are needed to attempt decryption reached a significant amount. Therefore, it is not possible to see the plaintext by indiscriminately substituting it. In addition, it is unlikely to use a well-known password. In the U.S.A, there is a case in which the government attempted decryption for years, however, failed to secure evidence[21]. Recently, decryption has been attempted through a method that quickly and automatically substitutes using high-tech technology. For example, in the United States, there is a program that automatically attempts to decrypt by learning users password patterns[22], like John the Ripper[23], which operates on various operating systems. However, English-based programs are inefficient in Korea because Korean does not set their passwords as ‘HONGGILDONG’ and sometimes set and use Korean typing as English typing like "GHDRLFEHD" (Hong Gil-dong in Korean typing). And we can also use forensic tools such as Cellebrite's UFED. It is known to have a function that guarantees time to bypass the security technology set by the manufacturer and make multiple attempts. However, since security technology and internal firmware vary depending on the operating system version, each version must be approached with a new decryption method. However, the technology does not keep up with the development speed of the operating system. In other words, decryption remains a challenge if you do not know the exact password used in the account.

2.1.3 Biological Features-Based Decryption Technology

Biometric Authentication is the technology to authenticate users that uses an individual's unique physical characteristics[24], and is designed to check plaintext recorded in device by directly touching the sensor with biometric identification, which is the decryption key. In particular, since Motorola "Atrix" in 2011, the introduction of biometric authentication, and installed on mobile like "iPhone 5S" (2013) and "Galaxy S5" (2014), the biometric authentication has been expanded. Therefore, in order to decrypt biometric authentication, the owner's biometric information is absolutely necessary. However, it is not easy to obtain a decryption key unless the biological site’s owner cooperates. There is not enough legal basis for the state agency to forcibly or arbitrarily collect it due to the investigation. In 2019, the Seoul Central District Court issued a warrant saying that the suspect's biological site could be collected for device decryption. In contrast, there was a controversy issue that the minimum privacy area should be protected. Furthermore, it was criticized by the reason of unconstitutional[25]. If the owner dies, the fingerprint cannot be authenticated due to the disappearance of the current, and the possibility of face authentication failure is also increased due to closed eyes, facial swelling, and wounds. In 2018, when a suspect died in a U.S. police shooting, it failed to secure evidence because it could not be decrypted with the corpse's fingerprints[26]. Moreover, in 2019, it confiscated LG smartphone from suspect arrested for drug sales but failed to certify Multimodal Sensors with ToF technology[27]. Like this, even after securing digital evidence, decryption is impossible, so it is failing to secure major evidence or solve cases by closing the Decision of an Interim Investigation Case or converting them into Cold Cases. However, regarding fingerprint authentication, there have been relatively various attempts as vulnerabilities have been found. In the 2016 USA, there was a case of success in decrypting fingerprint authentication with an artificial fingerprint made by a 3D printer. In detail, the murder victim’s Galaxy S6 was secured in the United States and decrypted[28]. In 2018, a laser printer and gelatin were used for a successful experiment[29]. E.A. Maro produced fake fingerprints using laser printers and gelatin, and successfully decryption the iPhone 6 and Meizum5s. Leave an afterimage of the fingerprint on the tape, take a picture with a digital camera of more than 2,400 pixels, and output it with a laser printer. It was immersed in gelatin and cured for a period to complete the fake fingerprint and successfully bypass it. In addition, successful cases are obtained by fake

fingerprints using cooking foil and wood glue[30] and using 3D printers and gold/bronze[28]. We applied these cases to the latest device version, but it was impossible except for using cooking foil and wood glue.[3] In 2022, there was a case in which the mold was manufactured using a 3D printer by analyzing previous issues, covered with wood glue, and successfully decryption the latest smartphone such as the Galaxy S20 Plus. Since this experiment targets fingerprints obtained from the investigative agencies' database, duplicate fingerprints can be produced even if the suspect runs away. However, Korea is the only country with a fingerprint database for the entire nation, and it is sporadic for investigative agencies to have individual fingerprints. In addition, even if such information is held in the state, there is a limit to the use of fingerprints at a time when privacy protection is emphasized. In face authentication, it is reported that it is not recognized according to the environment due to the influence of ambient brightness, and authentication is impossible even if you close your eyes or wear a mask. On the other hand, there have been cases of successful decryption of face photos[31], reproduced faces using 3D printers[32] and even family faces that resemble each other[33]. However, whenever these cases are found, the manufacturer responds quickly, so it is impossible to determine whether decryption always succeeds. Comprehensively judging, there is practically no way to legally secure evidence in the case of device encrypted through an individual's biometric information.

2.3 Explanation: Difficulty in Technical Issue of Decryption

Various attempt cases have been made to decrypt the secured devices, but South Korea is frequently treated as illegally collected evidence as it strictly restricts seizure and search and the procedure. In addition, manufacturers are strengthening their security levels through policies, so they cannot proceed with the other investigations. For example, it is designed to limit the number of times for typing a password, wait for a long time, or be fully formatted after a certain number of times. If we respond to the manufacturer's technology that is constantly updated, we will face a situation in which we cannot respond to important issues such as terrorism and national security in a timely manner[34]. In addition, even if the device can be confiscated and internal data can be searched, it does not simply set a password, Still, it reaches the level of concealment, and it is not even recognized. In fact, there was a case in which an imaging file of the laptop was obtained by checking the suspected possession of child sexual exploitation in the U.S. Still, at the time, they cannot recognized that the Z drive was fully encrypted with PGP, and eventually they failed to obtain evidence. Accordingly, the US investigation agency applied for a grand jury subpoena that forced him to provide a password but was dismissed because of violating the rights of the 5th Amendment[35]. Technologies such as Chip-Off and JTAG requires physical separation of memory, which is require a significant level of technology to obtain internal data without deleting them because the memory is susceptible to heat. Moreover, since the latest model is being released except for the hardware necessary to use the technology, such as JTAG ports, application can also be limited. Decryption plans through manufacturers can also be considered. But it is already widely known that Apple, which is known for its high security level using only its developments, does not cooperate even if law enforcement orders it for investigative purposes. In 2016, the court ordered the creation of a hacking version of the iOS for digital forensics on the suspect's iPhone to the FBI in the San Bernardino shooting terrorism, but Apple filed a cancellation request. Furthermore, in 2020, the court ordered the decryption of the suspect's iPhone in the Florida shooting, but it also refused.

[3] This experiment was part of a study conducted by Oh, SoJung for her master's thesis in the Department of Scientific Investigation at Sungkyunkwan University in 2022

As such, it is difficult to respond to important national issues such as terrorism or confidential information in a timely manner to expect technical development as well as cooperation from manufacturers. In addition, recently devices using artificial intelligence or super intelligent computers have accelerated, and multimodal methods using more than one encryption method are also increasing. Accordingly, high-tech has reached the level required as a prerequisite, and investigative agencies have increased the burden of decryption to discover the complete truth. Now, the time has come; we have to complete the normative system by preparing not only technical responses but also the law systematic solution to prevent future digital forensics investigations from being neutralized.

3. Legal Trends and Countermeasures

3.1 Legal Trends in Decryption

The "Law Enforcement Access to Keys" (LEAK) is largely primarily into ① using Public Keys and ②using compelled decryption[36]. The method of using the public key can be said to be regulated by technical means, and compelled decryption or undercover investigation of the encryption key corresponds to a normative regulatory means[37]. However, countries that adopt advanced methods such as Key Escrow and Key Recovery are not identified, and only some countries are all or part legislated in a 'post-mortem' means[38]. The United States has not legislated compelled decryption because it infringes the right to remain silent in the 5th Amendment. However, the number of cases in which the Federal Supreme Court accepted compelled decryption, based on two criteria about privilege against self-incrimination and the All Writs Act is increasing. The Federal Supreme Court suggested that in order to apply the privilege of the 5th Amendment, it must be proved to be a statement(certification), disadvantageous in criminal proceedings (indictment), and must be enforced (compelled)[39]. Exceptionally, those who fail to comply with the order to submit a decryption key based on ‘the privilege of foregone conclusion doctrine’[4] are punished for contempt of court. In 2000, the UK stipulated 'the Mandatory Decryption Notice' in Part 3 of the Regulations of Investigative Powers Act (RIPA 2000), and in 2016, further expanded its authority through the Investigative Powers Act (IPA 2016). Authorized officials may issue a Section 49 Notice of the RIPA to make public the decryption key or request that internal data be submitted in a known form. This notice may be issued if there are in the interest of the state, if it is necessary to detect or prevent crimes, or if it is necessary for the economic interest of the State. However, if the invasion of privacy is serious or there are other methods for decryption, it cannot be used. Since it should be the 'only means' as stipulated in the regulations. In addition, investigative agencies can compelled decryption from individuals and organizations or more.(RIPA 4.3) If a corporation or company, it is necessary to determine whether there is any actual infringement, and it can be applied in limited circumstances, and only judges, the Secretary of State, and authorized persons are authorized to issue orders[40]. For example, if the compelled decryption is not complied with, the U.S. punishes it as a crime of obstructing court orders or judicial activities, that is, ‘Contempt of court’[41]. This is only a collateral measure in response to the suspect's refusal to comply with the investigative agency's request for cooperation, and it cannot solve the essential problem of responding to advanced encryption technology for the

[4] Foregone Conclusion Doctrine refers to the principle that a suspect cannot refuse to make a statement about truth based on the privilege against self-incrimination if the investigative agency has specific and enough evidence.(Kim Hakkyong & Jung Jeyong, Comparative Analysis of UK’s Mandatory Decryption Notice: Focused on Regulations of Investigatory Powers Act 2000 and Schedule 7 of Terrorism Act 2000)

device. On the other hand, the UK is forced to dispose of it through the RIPA and the IPA, but controversy over privacy infringement continues. In other words, only the United Kingdom, etc. specifically stipulates the compelled decryption as a law, and even this can be applied only in extremely limited circumstances. In Korea, there is no law that can enforce decryption such as contempt of court, obstruction of justice, or RIPA. In addition, Korea has a history of suppressing the media according to political changes, so the public's sensitivity to privacy is high. Therefore, in order to legally introduce Compelled Decryption in Korea, legal issues must be reviewed in consideration of the historical background and to seek a reasonable normative solution.

3.2 Legal Issues with the Introduction of Compelled Decryption

3.2.1 The issue of whether or not the right to remain silent is violated

The Compelled Decryption can require access to data recorded in the suspect's device.[5] Methods are largely divided mainly into ① receiving authority information to access account credentials from suspects, ② requiring a suspect to enter authority information or submit decrypted digital evidence(or device), ③ receiving a decryption key for biometric authentication, such as fingerprints.[6] However, if the password corresponds to a statement, an infringement of the right to remain silent may occur, and even if it is not a statement, a problem of the Right to Personal Data Self-determination or Privacy infringement may arise.[7] The Korean Constitution guarantees the right to remain silent as a fundamental right by stipulating that "No citizen shall be tortured or be compelled to testify against himself/herself in criminal cases."(Article 12, Paragraph 2) The right to remain silent is the right of the defendant or suspect to refuse to state unfavorable to the court or investigative agency's inquiry in a trial or investigative procedure[42]. A statement means 'expression' of thoughts, knowledge, and experiences through 'language,' which is part of mental action[43]. Some people think of smartphones as an expanded self[44] or part of the body[45], but they cannot be said to be the same as a person's mind or brain. And it is difficult to say that protection from the right to remain silent can be applied because the password itself is not essential in the case but is just a technical means for searching data in the device as an incidental disposition to achieve the purpose of seizure and search[46] **Table 3**. In the survey conducted by this team, 35 people answered that the password was a statement, 18 were normal, and 37 answered that it was not a statement. In addition, more than 75% of the respondents said that the password for the device was information. As a result, the public divided opinions on whether the password is a statement or not, but the absolute majority said it was information. This is similar to the confrontation

[5] The subject of the right to remain silent as prescribed by the Constitution includes not only the suspect in the investigation and the defendant in the trial but also the suspect or defendant in the future.(Constitutional Court of Korea, Decision of 27 March 1997, 96 헌가 11)

[6] The U.S. scholar Sacharov categorizes ① forcing a suspect to tell the code, ② as requiring the suspect to enter the password, and ③ as requiring the provision of biometric information such as fingerprints and facial recognition.(Laurent Sacharoff, "Unlocking the Fifth Amendment: Passwords and Encrypted Devices," 87 Fordham L. Rev. 203 (2018), 222-223.)

[7] Lawmakers' opposition to the Minister of Justice's order to review legislation to punish suspects who refuse to provide device passwords to investigative agencies was strong. This is because it is an unconstitutional idea that is directly contrary to the constitutional Privilege against self-incrimination, which means the right not to be forced to make unfavorable statements.The Constitution guarantees the right to remain silent as a fundamental right to protect the human rights of criminal suspects or defendants above the national interests of discovering factual truth or realizing social justice, thereby ensuring human dignity and survival, and equality between the accused and the prosecutor. The Constitution stipulates many criminal procedural rights. This can also be said to be an expression of the will to guarantee the rights in the Criminal Process, which are very core to the Constitution, as fundamental rights.

between academia as to whether it is a statement or not that the suspect provides the decryption key to the investigative agency himself. In other words, passwords are not statements, but they are decryption keys that make personal information available and are recognized as 'important values' for individuals. Thus, when introducing the Compelled Decryption, legislating it without infringing on an individual's privacy and the Right to Personal Data Self-determination is ‘the minimum standard’ for social consent.

Table 3. Results of " Do you think the password is a statement?"

	Graduate students		Ordinary person	Experts			Total
	A	B	C	D	E	F	
Strongly agree		2	2		1	1	6
Agree	3	5	13	**2**	3	3	29
Neutral	3	4	8	**1**	1	1	18
Disagree	6	7	6	**1**	4	3	27
Strongly disagree	5	4	1				10

3.2.2 The issue of whether or not the invasion of the Right to Personal Data Self-determination and Privacy

The argument that a password is not a statement is a view that information such as a password is not directly related to the proof of evidence in itself, and is only a means to allow access to evidence in criminal proceedings. In other words, providing information related to passwords is not directly or indirectly related to criminal responsibility[47]. However, if the password is personal information, it can result in a problem of the Right to Personal Data Self-determination and invasion of privacy. When the decryption key is released, there is a possibility that private content that was encrypted can be disclosed. In particular, the device records individual information, private and public data. This is information that must be kept secret and is subject to the Right to Personal Data Self-determination, so individuals must be able to control the collection, storage, and use of passwords. In other words, if it is not permitted by the owner or related to the public interest such as national security, it has the right not to be collected or used without permission.[8] [9] Comprehensively judging, the Compelled Decryption is sufficient to infringe on the Privilege against self-incrimination or the Right to Personal Data Self-determination depending on whether the password is information or not. However, in serious crimes such as terrorism and leakage of state secrets, it is necessary to examine whether the compelled decryption can be applied exceptionally if the only decryption of the suspects’ device is a solution to the problem. In particular, if it is difficult to apply to an individual, it is necessary to review the service provider(third party).

[8] The majority opinion of the Supreme Court explicitly emphasizes the "guarantee of the Right to Personal Data Self-determination" in ‘the part of criminal compulsory execution of investigative agencies(seizure and search)’.(Supreme Court, Decision of 16 July 2015, 2011 모 1839)

[9] In the Supreme Court's supplementary opinions justice, Lee In-bok, Lee Sang-hoon, and Kim So-young, "Just as freedom of the body from unfair public power were important in the past, the Right to Personal Data Self-determination about electronic information is precious in the information society. Furthermore, freedom from illegal seizure and search and privacy are important constitutional values guaranteed by our Constitution with long historical experiences and origins."

3.3 Review of Compelled Decryption to Service Providers

According to a survey conducted by this team, only 14 people said that the decryption technology of the investigative agency follows the development speed of the device manufacturer's technology. It was confirmed that 67% of the respondents said that service providers such as manufacturers should cooperate when investigative agencies request to decrypt evidence **Table 4**. However, when companies in other countries do not comply with requests for cooperation, 35 people voted for the disadvantage of domestic operations, 22 for neutrality, and 37 for the opposition **Table 5**. In other words, the majority of the opinion that companies should cooperate with investigative agencies, but if they do not comply, it is judged that the views are divided because discrimination against domestic and other countries could occur.

Table 4. Results of " Do you think we should cooperate when an investigative agency requests decryption?"

	Graduate students		Ordinary person	Experts			Total
	A	B	C	D	E	F	
Strongly agree	6	2	6	1	2		17
Agree	10	12	17	1	3	3	46
Neutral	2	3	1	1	1	3	11
Disagree		4	5	1	2	2	14
Strongly disagree	1	1	3		1		6

Table 5. Results of " Do you think it can give domestic business disadvantage to foreign companies that do not cooperate despite the request of the investigative agency for cooperation on decoding?"

	Graduate students		Ordinary person	Experts			Total
	A	B	C	D	E	F	
Strongly agree	2	1	4		2		9
Agree	5	7	11		2	1	26
Neutral	7	3	8		2	2	22
Disagree	1	9	6	2	2	4	24
Strongly disagree	4	2	3	2	1	1	13

The Korean Personal Information Protection Act provides restrictions on the use and provision of individual information outside of the purpose. (Article 18) Exceptionally, the act stipulates that the information and communication service provider can use or provide individual information for another purpose to investigative agencies, only if ① the case of consent from the subject, ② the case of special provisions in other laws. (Same Law, Article 18 Paragraph 2) The same paragraph stipulates that public institutions can use individual information for other than prescribed purposes or provide it to third parties only in cases of

subparagraphs 5 through 9.[10] In particular, since paragraph 7 is "Where it is necessary for the investigation of a crime, indictment, and prosecution," if third parties are not public institutions, there is no way to be provided with information for the investigation. Therefore, it is necessary to review the compelled decryption for third parties, including private companies, focusing on the Convention on Cybercrime[11], which is ratified by 66 countries including the United States, Canada, and Japan[48]. The European Convention on the Prevention of Cybercrime stipulates that law enforcement should take the necessary steps to order those in their country to submit information recorded on the device and service providers to submit managed subscriber information (Article 18). The regulation for seizure and search of digital evidence stipulates that necessary laws should be enacted so that law enforcement agencies can search or access information stored devices, such as computers in their own countries (Article 19). Among the members of the Convention, Germany[12], France[13], and Japan[14] stipulate that offshore search and seizure are allowed under the prestigious provisions of their criminal procedure law. It is time for Korea to revise by establishing prestigious regulations on the Criminal Procedure Act, the Protection of Communications Secrets Act, the Telecommunications Business Act, and the Act on Promotion of Information And Communications Network Utilization And Information Protection to join the Convention. As cloud computing became more common, jurisdiction became a problem as data was distributed and stored on servers in various regions, and the actual stored location was unknown(loss of location)[49]. As a solution to this, it is expected that joining the European Cyber Prevention Convention will be able to cooperate with 65 countries and resolve other countries with Mutual Legal Assistance (MLA)[15]. However, it is necessary to preemptively resolve the fact that it takes an average of more than a year for legal procedures must be carried out through the Ministry of Justice and the Ministry of Foreign Affairs and that jurisdiction over the server may be in many countries. Through ‘the United States v. Microsoft Corp.,’[50] the United States allows companies to disclose information by

[10] 6.Where it is necessary to provide personal information to a foreign government or international organization to perform a treaty or other international convention; 7.Where it is necessary for the investigation of a crime, indictment, and prosecution; 8.Where it is necessary for a court to proceed with trial-related duties; 9.Where it is necessary for the enforcement of punishment, probation, and custody.

[11] Convention on Cybercrime (ETS No. 185), an international agreement led by the Council of Europe as an efficient international cooperation measure against cybercrime on July 1, 2004.

[12] Refer to Article 110 Paragraph 3 of the Germany Criminal Procedure Act. “ The examination of an electronic storage medium on the premises of the person affected by the search may also be extended to cover physically separate storage media insofar as they are accessible from the storage medium if there is a concern that the data sought would otherwise be lost. Data which may be of significance for the investigation may be secured.”

[13] Refer to Article 57-1 of the French Criminal Procedure Act. “Judicial police officers or judicial police agents under their supervision may, during a seizure carried out in the conditions laid down by the present Code, access any data relevant to the inquiry in progress stored in a computer system set up within the premises where the seizure is carried out or in another computer system, provided the data is accessible from the initial system or is available for the initial system.”

[14] Refer to Article 99 Paragraph 2 of the Japanese Criminal Procedure Act. “If the article to be seized is a computer, and with regard to a recording medium connected via telecommunication lines to such computer, it may be reasonably supposed that such recording medium was used to retain electronic or magnetic records which have been made or altered using such computer, or electronic or magnetic records which can be altered or erased using such computer, the computer or other recording medium may be seized after such electronic or magnetic records have been copied onto such computer or other recording medium.,” Article 107 Paragraph 2, “When making the ruling provided for in Article 99, paragraph (2), in addition to the particulars prescribed in the preceding paragraph, the seizure warrants set forth in the preceding paragraph must contain the range of recording medium to which the electronic or magnetic records are to be copied and which is connected via telecommunication lines to the computer to be seized.”

[15] Based on Articles 2 and 5 of the Act-On International Judicial Mutual Assistance In Criminal Matters, it refers to providing or receiving cooperation such as investigation of criminal cases, collection of evidence, delivery of evidence, hearing statements, and seizure search.

enacting the CLOUD Act, which states that even if they have servers overseas, they must provide data stored on servers according to warrants or subpoenas. In this way, it is necessary to find a way to seek the cooperation in mutual investigation by signing administrative agreements between countries.

3.4 Explanation: Necessity of applying compelled decryption to third parties

The problem of forcing the suspect to provide a decryption key to the investigative agency cannot guarantee the suspect's right to self-defense and the principle of the equal party[51]. However, even though encryption technology is developed and used for serious crimes that threaten the country and the people, it will not be the value pursued by the Constitution to only protect the suspect's right to self-defense. According to the survey conducted by this team, 79 said murders, 78 said human trafficking, 74 said rape, and 73 said kidnapping and abandonment, among the crimes related to life and body crimes subject to the Compelled Decryption. And 69 said embezzlement, 66 said fraud, and 56 said breach of duty among property crimes. Among the crimes related to national security, 87 said terrorism, 76 said security threats, 75 said spies, 81 said digital sex crimes, 67 said financial fraud, and 56 said hacking **Table 5**. In particular, in the case of terrorism, most said that forced access to devise data by investigative agencies could be allowed. This is judged to be acceptable by many to restrictively allow crimes only related to national security, such as the UK's RIPA, which enforces decryption. The Compelled Decryption implemented in the United Kingdom and others should set exceptions like introducing only when there is a limit to the technology possessed by investigative agencies. Because the password for the device is not evidence of guilt in itself, but only 'information' that leads to evidence[47]. And since it is a 'technical means' to perform a search for the device, the scope of discussions related to the right to remain silent needs to be reduced.

Table 5. Results of "What kind of crime do you think the compelled decryption can be applied to?"

	Graduate students		Ordinary person	Experts			Total
	A	B	C	D	E	F	
Murder	15	21	26	2	9	6	79
Human trafficking	18	16	25	3	9	7	78
Rape	18	19	22	3	8	4	74
Kidnapping and Abandonment	16	16	25	2	9	5	73
Embezzlement	17	19	21	1	8	3	69
Fraud	18	15	22	1	7	3	66
breach of duty among property crimes	17	15	16	1	4	3	56
Terrorism	18	21	28	4	9	7	87
Security threats	18	17	23	3	9	6	76
Spied	18	19	20	3	9	6	75
Digital sex crimes	18	20	26	3	9	5	81
Financial fraud	18	13	23	2	7	4	67
Hacking	15	12	20	1	6	2	56

4. Conclusion

In Korea, the level of security through policy is strengthened by manufacturers and the search and seizure procedures are strictly limited, making it difficult for investigative agencies to decrypt devices even if they secure them. In addition, encryption technology is accelerating, there is a limit to how to technically respond to it. Now, it is time to reorganize the normative system by preparing not only technical responses but also institutional solutions for efficient investigation. Korean considers the protection of personal information an important value, which can be confirmed through strong the Personal Information Protection Act by the 'legal appraisal'. In particular, according to the survey we conducted, 73 said positive and 13 said negative confirmed on "what do you think of the investigative agency's request for decryption of mobile for criminal investigation purposes?" More than half said they would provide it to investigative agencies, but many said it was reasonable to limit it to serious crimes such as personal body or national security, and that need procedural restrictions that do not infringe on privacy. To summarize the survey result, most respondents set a password on their mobile phones, including each file. It was also confirmed that even experts, most of them have no cognition about compelled decryption system. However, when we explained compelled decryption system in detail, most agreed with the suggested implications. For example, no one answered 'Strongly agree' to the question about whether the technical capability of the investigation agency is following the encryption technology of mobile devices. The result indicates that respondents agree with the point that investigation agencies have technical limitations and need normative countermeasures. Regarding targets subject to compelled decryption, most opinions agree to introduction without classifying crimes. However, they agree that the enforcement of individuals can lead to a severe invasion of privacy. Therefore, we present a normative countermeasure that can introduce compelled decryption while recognizing limitations in technical responses to devices and preserving the rights to individuals. We also discussed how Korean law should be changed in reference to preemptive foreign laws. We divided the subject into individuals and third parties. Then, we suggested that the enforcement of individuals is likely to become a global issue regarding privacy and the Right to Personal Data Self-determination. It is contrary to the privilege against self-incrimination set out in Fifth Amendment to the United States Constitution. Furthermore, it is contrary to the Korean Constitution. Regarding enforcement to third parties, Convention on Cybercrime ratified by 66 countries such as the United States, Canada, and Japan stipulates the obligation to provide information to third parties. In addition, the United States enacted the Clarifying Lawful Overseas Use of Data(CLOUD) Act and resolutely stipulated the obligation. On the other hand, in Korea, there is no stipulation about enforcement for individuals or third parties. Similar regulations are defined in Criminal Procedure, Protection of Communications Secrets, Telecommunications Business Act, and Act on Promotion of Information and Communications Network Utilization and Information Protection. However, the subject is limited to public institutions. In other words, compelled decryption cannot be enforced on private companies that manufacture mobile devices and have the key for decryption. We should seek ways to promote accession to the European Convention on the Prevention of Cybercrime by specifying the regulations in the law and cooperating through administrative agreements at the national level. However, first, related laws such as the Criminal Procedure Act and the Protection Of Communications Secrets Act should be revised so that companies can be ordered. In particular, when faced with a reality that hinders the development of investigations and hinders the discovery of substantive truth, investigations according to due process and the control of Warrant Requirement should be accompanied. We hope that this study will be a normative response that can clarify the truth of the case and guarantee the country’s security by presenting solutions to the pending issues.

References

[1] HUFFPOST, “Police have unlocked one of Jo's two mobile phones in two months,” May. 15. 2020. [Online]. Available: https://www.huffingtonpost.kr/news/articleView.html?idxno=97272, Accessed on: Aug. 10, 2022.

[2] The Korea Times, “Locked Inspection Galaxy S21 Phone… The Fake Fisherman, The Real Lobby, Is the Truth Trapped?,” Jul. 14. 2021. [Online]. Available: https://n.news.naver.com/article/469/0000617132, Accessed on: Aug. 10, 2022.

[3] Miles, M. B., & Huberman, A. M., Qualitative data analysis: An expanded sourcebook, *Sage*, 1994.

[4] H.J.Jong, “Ordered Logit Model,” *Planning and policy*, vol. 310, pp. 94-102, 2007.

[5] R. Morris and K. Thompson, “Password security: a case history,” *Communications of the ACM*, vol 22, no.11, pp. 594-597, Nol. 1979. Article (CrossRef Link)

[6] C. Lee, Y.M. Kim, S.J. Yoo, “Information Hiding Application Method Using Steganography,” *Journal of information and security*, vol.10, no.2, pp. 19-26, June. 2010.

[7] Y.J. Kim, D.M. Moon, S.B. Pan, Y.C. Chung, K. Chung, “Implementation of Embedded Biometrics Technologies: A Case of a Security Token for Fingerprints,” *The Institute of Electronics Engineers of Korea - Computer and Information*, vol.40, no.6, pp. 39-46, Nov. 2003.

[8] S.G. Yoo, K.Y. Park, T.J. Kim, J.H. Kim, “Hardware Crypto-Core Based Authentication System,” *The Institute of Electronics Engineers of Korea – Telecommunications*, vol.46, no.1, pp. 121-132, Jan. 2009.

[9] B.S. Koo, J.S. Lim, C.S. Kim, E.J. Yoon, and S.J. Lee, “High-Speed FPGA Implementation of SATA HDD Encryption Device based on Pipelined Architecture,” *Journal of the Korea Institute of Information Security & Cryptology*, vol.22, no.2, pp. 201–211, Apr. 2012. Article (CrossRef Link)

[10] E. Casey and G.J. Stellatos, “The impact of full disk encryption on digital forensics,” *ACM SIGOPS Operating Systems Review*, vol.42, no.3, pp. 93-98, Apr. 2008. Article (CrossRef Link)

[11] Chosun Ilbo, “Han Dong Hoon, "Promote to release your phone password. Recommend a name for 'Lee Jae Myung and Chumae Prevention Act',” Jan. 16. 2022. [Online]. Available: https://www.chosun.com/national/court_law/2022/01/16/KEK4K5MFLJEPDKUHD22KTCLW34/, Accessed on: Aug. 10, 2022.

[12] N. Nishanth, J. Zareena and S. Suresh Babu, "Pseudo Random Alteration of Sequence Numbers (PRAS): A novel method for defending sessiion hijacking attack in mobile adhoc network," in *Proc. of 2013 15th IEEE International Conference on Communication Technology*, pp. 20-25, 2013. Article (CrossRef Link)

[13] S.J. Kim, “Secure Management Method for Private Key using Smartphon's Information,” *The Journal of the Korea Contents Association*, vol. 16, no. 8, pp. 90–96, Aug. 2016. Article (CrossRef Link)

[14] THE DONG-A ILBO, “FBI uses messenger app to trick criminals,” Jun. 10. 2021. [Online]. Available: https://www.donga.com/news/Inter/article/all/20210609/107358679/1, Accessed on: Aug. 10, 2022.

[15] S.Y. Kang, Y.S. Min, “Verdeckte personale und technische Ermittlungen im Internet,” *KOOKMIN LAW REVIEW*, vol.31, no.2, pp. 359-398, Oct. 2018. Article (CrossRef Link)

[16] H.Y. Park, “A permitted limitation of Telecommunications surveillance at the source(Quellen TKÜ),” *Korean Criminological Review*, vol.29, no.2, Jun. 2018.

[17] S.H. Chung, “Cloud-based IAM Technology Trends,” *Information & communications magazine*, vol.32, no.10, pp. 58-64, 2015.

[18] A. K. Kyaw, F. Sioquim and J. Joseph, "Dictionary attack on Wordpress: Security and forensic analysis," in *Proc. of 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, pp. 158-164, 2015. Article (CrossRef Link)

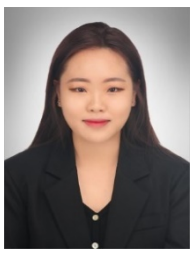
[19] Alphr, “The top ten password-cracking techniques used by hackers,” Oct. 15. 2021. [Online]. Available: https://www.alphr.com/features/371158/top-ten-password-cracking-techniques/ Accessed on: Aug. 10, 2022.

[20] Supreme Court of Korea, 2019Do12194 February 13, 2020

[21] United States v. Doe (In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011), 670 F.3d 1335, 23 Fla. L. Weekly Fed. C 795 (11th Cir. 2012)
[22] J.M.Lim, H.D. Kwon, J.M. Choi, S.J. Lee, "A Study of Construct Dictionary File for Password Recovery in Digital Forensics Investigation," in *Proc. of the Korean Society of Broadcast Engineers Conference*, vol. 2, pp. 155-158, Feb. 2008.
[23] John the Ripper password cracker. [Online]. Available: https://www.openwall.com/john/
[24] K.S. Kim, D.U. Kim, "Overview on Smart Sensor Technology for Biometrics in IoT Era," *Journal of the Microelectronics and Packaging Society*, vol.23, no.2, pp. 29-35, Jun. 2016. Article (CrossRef Link)
[25] A Legal Newspaper, "Controversy over 'fingerprint verification' warrant to unlock smartphones," Dec. 9. 2019. [Online]. Available: https://m.lawtimes.co.kr/Content/Article?serial=157842, Accessed on: Aug. 10, 2022.
[26] Yonhap News Agency, "U.S. police who used to open cell phones with body prints..."No response. Failed"," Apr. 24. 2018. [Online]. Available: https://www.yna.co.kr/view/AKR20180424003700075, Accessed on: Aug. 10, 2022.
[27] THE DONG-A ILBO, "LG Android phone, U.S. investigators couldn't penetrate it," May. 30. 2019. [Online]. Available: https://www.donga.com/news/article/all/20190529/95761089/1, Accessed on: Aug. 10, 2022.
[28] Detroit Free Press, "MSU professor helps police crack smartphone fingerprint lock," Jul. 31. 2016. [Online]. Available: https://www.freep.com/story/news/local/michigan/2016/07/31/michigan-state-university-fingerprint-smartphone/87719418/, Accessed on: Aug. 10, 2022.
[29] E.A. Maro, M.M. Kovalchuk, "Bypass Mobile Lock Systems With Gelatin Artificial Fingerprint," *INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING*, vol.6, no.6, pp.32-36, Jul. 2018. Article (CrossRef Link)
[30] Max Tech, "Galaxy S10 vs OnePlus 6T – Fingerpritn Sensor HACK Test," Mar. 9. 2019. [Online]. Available: https://youtu.be/8AxXr3hjFSg, Accessed on: Aug. 10, 2022.
[31] D.M. Choi, Y.S, Baek, H.S. Woo, I.Y. Chung, "Smartphone User Authentication Method using Motion Password," in *Proc. of the Korean Society of Computer Information Conference*, vol.23, no.2, pp. 285-286, Jul. 2015.
[32] Asia Economy, "Can I Unlock My 3D Printed Face, Smartphone?," Dec.18.2018, [Online]. Available: https://www.asiae.co.kr/article/2018121814475575041, Accessed on: Aug. 10, 2022.
[33] Star News, "Radio Star" Hong Hyun-hee and Jason's mother-in-law, "Releasing Face Recognition on Cell Phones" [Byul Byul TV]", Dec.1.2021. [Online]. Available: https://sports.v.daum.net/v/20211201230029190, Accessed on: Aug. 10, 2022.
[34] D.J. JO, "The necessity of introducing a decryption command system based on device encryption," Master dissertation, Seoul National University Graduate School of Convergence Science and Technology, Seoul National University, Korea, 2016
[35] In Re Boucher 2007. Case No. 2:06-mj-91, document 35, WL 4246473, 11/29/2007, United States District Court for the District of Vermont. [Online]. Available: https://ecf.vtd.uscourts.gov/doc1/1851273316, Accessed on: Aug. 10, 2022.
[36] E.J. Koops, "The Crypto Controversy: A Key Conflict in the Information Society," *Kluwer Law International*, pp.133-232, Jan. 1999.
[37] S.J. Baek, J.I. Lim, "A Study on National Control Policy for the Use of Encryption Technologies by an Accused Person," *Journal of the Korea Institute of Information Security & Cryptology*, vol.20, no.6, pp. 271-288, Dec. 2010. Article (CrossRef Link)
[38] H.K. Kim, J.Y. Jung, "Comparative Analysis of UK's Mandatory Decryption Notice: Focused on Regulations of Investigatory Powers Act 2000 and Schedule 7 of Terrorism Act 2000," *Contemporary Review of Criminal Law*, vol.71, pp. 229-273, 2021.
[39] O.S. Kerr, "Compelled Decryption and the Privilege Against Self-Incrimination," *Texas Law Review*, vol.97, no.4, Jun. 2019. Article (CrossRef Link)
[40] Code of practice for investigation of protected electronic information, Home Office, Sep. 8. 2010(Last Updated Sep.20.2018). [Online]. Available:

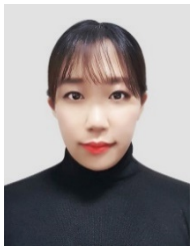
https://www.gov.uk/government/publications/code-of-practice-for-investigation-of-protected-electronic-information, Accessed on: Aug. 10, 2022.
[41] B.M. Palfreyman, "Lessons from the British and American Approaches to Compelled Decryption," *Brooklyn Law Review*, vol.75, no.1, 2009. [Online]. Available: https://brooklyworks.brooklaw.edu/blr/vol75/iss1/7, Accessed on: Aug. 10, 2022.
[42] Constitutional Court of Korea, 2001Hun-Ba41, November 29, 2001
[43] Constitutional Court of Korea, 2001Hun-Ga41, March 27, 1997
[44] B.H. Choi, "The Privilege Against Cellphone Incrimination," *Texas Law Review Online*, vol. 97, May. 2019. Article (CrossRef Link).
[45] H.K. Kim, "Law and Policy on Mandatory Key Disclosure – A case Study of UK Regulation of Investigatory Powers Act 2000," *Theories and Practices of Criminal Procedure*, vol.13, no.2, pp. 147-176, 2021. Article (CrossRef Link)
[46] D.H. Kim, "A study on the possibility of introducing decryption order to digital device," Master dissertation, Sungkyunkwan University, Korea, 2022
[47] The Washington Post, "A revised approach to the Fifth Amendment and obtaining passcodes," Sep. 25. 2015. [Online]. Available: https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/09/25/a-revised-approach-to-the-fifth-amendment-and-obtaining-passcodes/, Accessed on: Aug. 10, 2022.
[48] Chart of signatures and ratifications of Treaty 185, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185, Accessed on: Aug. 10, 2022.
[49] Cybercrime Convention Committee(T-CY), Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Council of Europe, 2016, [Online]. Available: https://www.coe.int/en/web/cybercrime/ceg, Accessed on: Aug. 10, 2022.
[50] Microsoft Corp. v. United States (In re a Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197 (2d Cir. 2016)
[51] K.M. Choi, "Constitutional Study on Forced Decryption of Smart Electronic Devices," *Korean Journal of Industry Security*, vol. 11, no. 2, pp. 159-184, 2021. Article (CrossRef Link)
[52] Y.J. Song, "Compelled Decryption and the Privilege Against Self-Incrimination: Recent Court Decisions in the United States and Legislation of the United Kingdom," *Korean Criminological Review*, vol.31, no.1, pp. 159-190, Mar. 2020. Article (CrossRef Link)

Chohee Bae received the bachelor's degree in law and Business Administration from University of Ulsan, Ulsan, Korea. She is currently studying for Integrated PhD program in Law from 2020 at Sungkyunkwan University, Seoul, Korea. She works as researcher at Research Projects of the Korea Research Foundation with professor since 2020. Her research interests include business and financial crime, Cybercrime Investigation.



Sojung Oh received the B.S. degree in Computer Science from SangMyung University, Seoul, Korea, M.S. degree in Forensic Science from Sungkyunkwan University, Seoul, Korea. She works at digital forensic laboratory as a researcher and simultaneously, she serves as the administrative staff of the Korean Society for Digital Forensics since 2020. Her research interests include Digital Forensic, the Criminal Procedure Act, Cybercrime Investigation.

Sohyun Joo received the B.L. degree in Law from SungShin Women's University, Seoul, Korea. She served as an employee of a Law Firm for four years. Now she is studying integrated course of Master's and Doctorate Degrees in Law at Sungkyunkwan University, Seoul, Korea. She works as researcher at Research Projects of the Korea Research Foundation with professor. Her research interests include Digital Law, the Criminal Procedure Act, a Cybercrime Investigation.



Jiyeon Joo received the B.L. degree in law from Chosun University, Gwangju, Korea. In 2020, She was a team member of the Advocacy Center for Online Sexual Abuse Victims. She is pursuing her Master's Degree in Forensics at Sungkyunkwan University and was researched on Technology & Policy of the Digital Forensic in Digital Forensics Lab. Currently, she is a researcher at Korea Information Society Development Institute. Her research interests include ICT Policy and Technology, Digital crimes and law, Digital Forensic etc.

Professor KyungLyul Lee teaches Criminal Law at Sungkyunkwan University Law School. Prior to joining the law faculty in 2015, he was a professor at College of Law of Sookmyung Women's University from 2003 until 2014, including his career as the dean of the college. He was a former chief editor of Korean Association of Comparative Criminal law (2013~2014) and Korean Association of Criminology (2017~2020). He received first Ph.D. degree of Criminal Law at Sungkyunkwan University in 1994 and second Dr.jus at University of Cologne in 2002. He is coauthor of Organized Crime and Criminal Law (2004), Understanding the 4th Industrial Revolution (2020) & Criminal Procedure Act (2021). He received awards in recognition of his research papers including <The Current States of Financial Crime and Socio-Legal Countermeasures in Korea> in 2003, <Über bleibende Frage nach einer nachträglichen Strafenbildung und Vollstreckung bei Tatmehrheit> in 2007, <Irrtum über Tatumstände und Seine Abgrenzung im §15 I des KorStGB> in 2014.