The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 17, No. 3, pp.235-241, Jun. 30, 2017. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2017.17.3.235
JIIBC 2017-3-29

# 디지털시대 강제해독에 따른 자기부죄 거부 권리에 관한 미국과 한국의 제도 비교 연구

# Comparative Study of US and Korean Legal System on the Privilege against Self-Incrimination through Forced Unlocking in Digital Era

이 욱*, 지명근*, 이동한**

**Ook Lee*, Myung Keun Jee*, Dong Han Lee****

**요 약** 디지털 시대의 발현과 함께, 암호화는 생활의 한 부분이 되었고 대부분의 사람들이 쉽게 암호화 프로그램을 취득하여 제3자로부터 그들의 정보를 보호하게 되었다. 그러나 이런 암호화 프로그램의 확산으로 말미암아, 범죄자들조차도 범죄증거를 암호화하여 정부는 범죄 수사에 큰 난항을 격고 있다. 이에 따라서 여러 국가에서는 암호화된 범죄증거들을 강제해독하기 위한 시도를 하고 있으며 여기서 헌법상 자기부죄거부라는 기본권의 문제가 발생하게 되었다. 본 연구에서는 전반부에 이와 관련된 미국 헌법 및 미국 대법원의 판례를 분석하여 주요 기조를 제시하였으며, 후반부에서는 대한민국의 헌법과 형사소송법에 기초하여 암호화된 디지털 증거의 강제해독 여부에 대한 분석을 실시하였다. 마지막으로 결론에서는 공공의 안전과 복리를 위하여 법적 제도 측면에서의 강제해독의 접근 방향을 제시하였다.

**Abstract** With the coming of the digital era, encryption has become common in everyday life. Almost anyone can easily acquire encryption software and use it to prevent unwanted third parties from accessing one's private information. However, the spread of encryption has also seriously hindered law enforcement during the investigation of cybercrimes, which hides incriminating digital evidence in encrypted hard drives and files. Therefore, many countries have attempted to compel criminals to decrypt encrypted evidence and it has been inevitable to examine privilege against self-incrimination as basic right on the side of constitution. This study analyzed the past court decisions on the issue of compelled decryption in the US and whether the Government can compel a defendant to disclose his password in Korean legal system on the constitutional side. Finally, this study suggests an approach to create a legal procedure to make it a crime for a suspect or defendant to refuse to disclose his password to law enforcement for criminal cases in Korea.

**Key Words :** Digital Era, Forced Unlocking, Legal System, Privilege against Self Incrimination

## Ⅰ. Introduction

According to The Wall Street Journal on 4th April, the Trump administration is considering requesting more visa applicants undergo substantial security reviews and that embassies abroad spend more time

*정회원, 한양대학교 정보시스템학과
**정회원, 가천대학교 산학협력단
접수일자 : 2017년 5월 1일, 수정완료: 2017년 6월 7일
게재확정일자 : 2017년 6월 9일

Received: 1 May, 2017 / Revised: 7 June, 2017
Accepted: 9 June, 2017
**Corresponding Author : lawdhl@gmail.com
Dep. of Industry-University Cooperation, Gachon Universtiy

reviewing and interviewing such applicants[1]. Throughout his presidential campaign, Donald Trump repeatedly committed to introduce extreme vetting to make it harder to enter the US, which he claimed would stop possible terror attacks against the US[2]. The White House is discussing ways to put into place the "extreme vetting" measures President Trump has vowed to use on foreigners entering the US, including methods like making people reveal their mobile phone contacts, social-media passwords, financial information, and subjecting people to questions about their political ideology[3]. This may be extreme defense for social and national security, even we can not clearly say whether this policy is right or wrong in all respects including privacy because today digital revolution has completely changed the whole of society and the evidence of crime has become digitalized. Therefore, it is no exaggeration to say that the success or failure of investigation to reveal the truth depends on how digital evidence is secured and recognized. In this way, our society is rapidly changing into a digital society, but the law has not been completely improved, and it maintains the analog legal system of the past in a lot of ways.

By the way, the recent upsurge of powerful and reasonable encryption technology has given both law-abiding citizens and criminals an ability to keep their secrets safe[4]. Powerful encryption software is freely available online and even most computer beginners now know methods to protect their private and confidential data[4]. Yet, the proliferation of encryption has seriously hindered law enforcement during the investigation of cybercrimes[4].

Criminals are able to conceal incriminating digital evidence in encrypted hard drives or electronic devices like smart phone. This can make it impossible for investigators to access the data[5]. Sometimes the only way for the Government to be able to gain and access to a suspect's or defendant's data is to compel the suspect or the defendant to disclose their password by a court order[6]. However, this way, which has been called "forced unlocking" or "compelled decryption", has had mixed results in the US, since the US courts have found that the Fifth Amendment privilege against self-incrimination that protects defendants from being forced to disclose their password or decrypt their data[6]. This research analyzed the past court decisions on the issue of compelled decryption in the US and whether the Government can compel a defendant to disclose his password in Korean legal system on the constitutional side. Finally, this article suggests an approach to create a legal procedure between the needs of law enforcement and the privilege against self-incrimination.

## II. Encryption and Increase of Cybercrime

People use the word password and use our cryptography to protect ourselves and our information. We have a tremendous amount of sensitive information such as personal documents, pictures, and e-mails on the computers and electronic devices we use. If one of our devices is lost or stolen, those who have learned it will be able to see all the sensitive information on the device. In addition, online banking or shopping can send sensitive information online. If someone is monitoring our online activities, he can steal our information such as financial accounts or credit card passwords. In this situation, passwords permit that only authorized persons can access and modify information. Cryptography has evolved over thousands of years. Passwords today are much more complex, but they do the same. That is, when you send confidential information from one place to another, only authorized people can access and read the information. When the information is not encrypted, we call it plain text. This means that anyone can easily access and read information. Cryptography technology changes plain text information into invisible, formalized text in cipher. We use key to encrypt or decrypt information. Most keys are passwords.

Symantec announced the 22nd Internet Security Threat Report (ISTR), an analysis of key cybercrime

and security threat trends in 2016. The year 2016 was the year in which new changes in the purpose of the cyber attack activity were seized, including bank robberies of millions of dollars, open attacks by state-sponsored hacking organizations to influence the US electoral process. Symantec's Internet Security Threat Report provides comprehensive information about the cyber threat environment, such as insights into cyber threat trends around the world and motivations for criminals to attack. According to this report, Cyber attackers revealed new levels of ambition in 2016, a year marked by extraordinary attacks, including multi-million dollar virtual bank heists, overt attempts to disrupt the US electoral process by state-sponsored groups, and some of the biggest distributed denial of service (DDoS) attacks on record powered by a botnet of Internet of Things (IoT) devices[7].

Within the last ten years, powerful and free encryption software has become widely available on the Internet[8]. It has also provided criminals with a potent tool to thwart law enforcement[4]. Many times, the only way for law enforcement to get the password is by attempting to compel the defendants to disclose thier password, usually through a court order in the US[9],[10].

## Ⅲ. Analysis

Analysis on the cases, terminologies and doctrines relating to constitutional law in the US is important to propose approach to legal system for the Republic of Korea.

The Fifth Amendment provides that "No person shall be held to answer for a capital, or otherwise infamous crime, unless on presentment or indictment of a grand jury ….Nor shall any person be subject for the same offense to be twice put in jeopardy of life and limb, nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law, nor shall private property be taken for public use, without just compensation[11]."

Defendants have applied their Fifth Amendment privilege against self-incrimination in cases where the government has compelled them to disclose the password to their encrypted files[12].

The Supreme Court has made it clear that the term "privilege against self-incrimination" is not an "entirely accurate description of a person's constitutional protection against being compelled in any criminal case to be a witness against himself[13]."

A defendant's compelled act of producing incriminating documents before the court or a grand jury does not automatically apply the Fifth Amendment protection, even if the documents contain incriminating assertions of fact or belief on the part of the defendant[13]. The protection of the privilege extends only to compelled incriminating communications that are, what the Court calls, "testimonial" in character[13]. Testimonial means the government must have compelled the individual to use "the contents of his own mind" to communicate some statement of fact[6].

The production of a document may be testimonial if it conveys a statement of fact that certain documents are under the defendant's control or possession, or are authentic[6]. This is called the "act-of-production" doctrine[6].

However, even if the defendant's act of producing documents is testimonial, if the government can demonstrate that it had prior knowledge of the existence, possession, or authenticity of the documents, the testimonial protection of the documents will be destroyed[6]. This is what is known as the "foregone conclusion doctrine[14]."

### 1. United States v. Fisher, 425 US 391, 411 (1976)

The Supreme Court case United States v. Fisher established the basis for the modern act-of-production doctrines and foregone conclusion doctrines[14].

In this case, a taxpayer got personal tax returns and related documents from his accountant and gave them

to his attorneys, who are representing taxpayers under investigation for violating federal tax laws. They refused to transfer their clients' taxpayer documents to the Internal Revenue Service (IRS) and insisted their clients' Fifth Amendment privilege[15].

The Supreme Court ruled for the IRS, and in its holding the Court articulated the foregone conclusion doctrine[15].

The Court held that the Government can compel production where the existence and location papers are a foregone conclusion and defendant adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers[14]. The Court made it clear that the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence, but applies only when the accused is compelled to make a testimonial communication that is incriminating[14].

The Court held that the act of producing the documents was not testimonial in nature, because the subpoena did not force them to testify regarding the contents of the documents and only forced the defendants to hand the documents over investigators[16].

### 2. United States v. Doe, 465 US 605, 104 S. Ct. 1237 (1984)

Eight years after the Fisher case's decision, the Supreme Court reconsidered the issue of act-of-production doctrine in United States v. Doe[17].

In this case, the government was investigating corruption in county and municipal contracts and Doe, a sole proprietor of several businesses was investigated by a grand jury. The jury served five subpoenas on the dependant in an attempt to get certain business records[17]. The subpoenas sought various business records from the sole proprietorships, including telephone records, bank statements, and listings of all business records[17].]

The defendant filed a motion in federal district court, trying to quash the subpoenas. The district court granted the motion except as to records that were required to be kept by law or to be disclosed to a public agency, finding that the act of producing the records would involve testimonial self-incrimination[17]. The Court of appeals affirmed the district court월's decision, and the case was appealed to the Supreme court[17].

Next the court of appeals considered whether the documents at issue in this case are privileged. The court noted that this court held in Fisher v. United States[14] and that the contents of business records ordinarily are not privileged because they are created voluntarily and without compulsion[17].

However, the Court recognized that if a defendant were to produce these records, he would be admitting that they existed, that they were in his possession, and that they were genuine[17].

So, in this case the Court held that the act of producing the documents would involve testimonial self-incrimination although the contents of a document may not be privileged[17].

In addition, the Court of Appeals noted that no formal request for use immunity had been made, although the Government contended that the court should enforce the subpoenas because of the Government's offer not to use respondent's act of production against respondent in any way[17].

### 3. United States v. Hubble, 530 US 27, 120 S. Ct. 2037 (2000)

The United States v. Hubbell case on 2000 is recent Supreme Court case relating to the foregone conclusion doctrines and the act-of-production.

Webster Hubbell, in a plea agreement, promised to provide the Independent Counsel Ken Starr investigating matters relating to the Whitewater Development Corporation with information relevant to his investigation[13].

However, the Independent Counsel became suspicious that the defendant Hubbell had violated his promise to fully cooperate and afterwards the Independent Counsel served respondent with a subpoena calling for the production of eleven different categories of documents before a grand jury in Little Rock, Arkansas[19].

Hubbell invoked his Fifth Amendment right against

self-incrimination and then the prosecutor produced an order from the district court directing Hubbell to respond to the subpoena and granting him immunity over his act of producing the documents[13][19]. Then Hubbell produced over 13,120 pages of documents and records, and responded that these documents were all the documents in his control or custody that were responsive to the subpoena[13]. The Independent Counsel then used those documents to indict Hubbell on tax and fraud charges on April 30th 1998[13].

The district court dismissed the indictment because all the evidence the prosecution would offer against Hubbell derived from the testimonial aspects of respondent's immunized act of producing the documents[13].

In vacating and remanding, the court of appeals directed for the district court to hold a hearing in which the prosecution should demonstrate with reasonable particularity a prior awareness that the documents sought in the subpoena existed and were in Hubbell's possession[13].

When this case was appealed to the Supreme Court, the main issue was whether the indictment should be dismissed because the subpoena and questions by the Government had violated Hubbell's Fifth Amendment privilege[12][13]. The Supreme Court ruled in favor of Hubbell. The Court held that the Fifth Amendment privilege against self-incrimination protects a witness from being compelled to disclose the existence of incriminating documents that the Government is unable to describe with reasonable particularity. The Court also ruled that if the witness produces such documents, pursuant to a grant of immunity, the government may not use them to prepare criminal charges against him[12][13].

As a final note on the Supreme Court's interpretation of the Fifth Amendment, the Court has suggested that compelling a defendant to produce the key to his safe would have a different testimonial nature than if he were compelled to produce the combination to the safe[20]. The Court has indicated that producing the key to the safe would not be a testimonial act, but the production of the combination from memory would be protected under the act of production doctrine since it is an "expression of the contents of an individual's mind[20]."

### 4. Legal system of the Republic of Korea

Article 12 paragraph 2 of the Constitution of the Republic of Korea stipulates that "No citizen shall be tortured or be compelled to testify against himself in criminal cases". This law clause guarantees the privilege against self-incrimination as the fundamental right of the people[21].

First, this is to protect human rights of defendants or suspects prior to the discovery of substantive truths or the realization of social justice. In the second place, this is to realize the ideology of fair trial by promoting equality of parties between the defendant or the suspect and the prosecutor.

The subject of the privilege against self-incrimination in Korea is not only the suspect in the investigation stage and the defendant in the trial procedure, but also the person who is likely to become a suspect or a defendant in the future.

Statement refers to expression of thoughts, knowledge, and empirical facts through language. Such language acts include pronunciation, writing of characters, and physical movements.

All citizens shall not be subjected to criminal offense against him, and in accordance with Article 244-3 of the Criminal Procedure Act the prosecutor or the judicial police officer shall notify the suspect the privilege against self-incrimination in advance[22].

And in accordance with Article 283-2 (2) of the Criminal Procedure Act and Article 127 of the Criminal Procedure Code, the judge also has an obligation to explain to the defendant the intention to refuse to give a statement on the question. If a confession is made without notice, the statement will be denied evidence[22][23].

Article 12 paragraph 2 of the Constitution guarantees the fundamental rights of the people not to be compelled to make statements that are disadvantageous to the criminal responsibility[21].

The guarantee of fundamental right by the

Constitution is to protect human dignity and survival value prior to the national interests of discovery of the substantive truth of the criminal lawsuit or realization of concrete social justice and to eradicate the inhuman confession and torture.

In other words, the essential part protected by the privilege against self-incrimination is to force a statement against him in a forced manner such as torture against human dignity.

Therefore, the privilege against self-incrimination in the Republic of Korea cannot force the defendant or the suspect to release the decryption regardless of the foregone conclusion doctrince, because it does not ask for the advantage or disadvantage of the statement unlike the US.

Moreover, there has been no such case concerning decrypted documents and data by compelling on internet, electronic devices and cyber space in Korea.

## Ⅳ. Conclusion

It is natural that if criminals have a encrypted means of communicating which law enforcement agencies cannot understand then it is a serious obstacle to both detection and investigation. So governments have attempted to compel suspects or defendants to decrypt encrypted evidences and here the problem of privilege against self-incrimination has come to the fore[24][25].

This study analyzed the Fifth Amendment Self-Incrimination Clause and three United States Supreme Court decisions.

First, the act of production doctrine is a creature of the Fifth Amendment's privilege against self-incrimination. The doctrine depends on the concept that while the contents of pre-existing documents are never subject to a claim of the Fifth Amendment privilege, the compelled act of producing them in response to a subpoena can itself be testimonial on the facts of a given case, because the recipient of the subpoena would be effectively testifying to the existence, his possession, and the authenticity of the documents.

Second, if the government can already show the existence, location, and authenticity of the documents with reasonable particularity, compliance with the subpoena and production of the documents are not "testimonial" because the government already knows everything that would be revealed through the act. This is foregone conclusion doctrine.

At the end of the research, it is examined that the Constitution of the Republic of Korea can not force defendants or the suspects to release the decryption regardless of the foregone conclusion doctrince, because it does not ask for the advantage or disadvantage of the statement unlike the US.

Moreover, there has been no such case concerning decrypted documents and data by compelling on internet, electronic devices and cyber space in Korea. Therefore, this study finally suggests an approach to create a legal procedure to make it a crime for a suspect or defendant to refuse to disclose his password to law enforcement for criminal cases in Korea.

## References

[1] https://www.wsj.com/articles/trump-administration-considers-far-reaching-steps-for-extreme-vetting-1491303602 (last visited April 24, 2017).

[2] http://www.independent.co.uk/life-style/gadgets-and-tech/news/donald-trump-immigration-check-phones-social-media-facebook-twitter-logins-a7668111.html (last visited April 24, 2017).

[3] http://www.nydailynews.com/news/politics/extreme-vetting-dig-social-accounts-financial-info-article-1.3018978 (last visited April 24, 2017).

[4] Eoghan Casey et al., "The Growing Impact of Full Disk Encryption on Digital Forensics", DIGITAL INVESTIGATIONS Vol.8, pp. 129-134, Nov 2011.

[5] Dario Forte, "Do Encrypted Disks Spell the End of Forensics?", COMPUTER FRAUD & SECURITY, No.2, pp. 18-19, Feb 2009.

[6] Erica Fruiterman, "Upgrading the Fifth Amendment: New Standards for Protecting Encryption Passwords", TEMP. L. REV., Vol.85, pp. 655-689, Mar 2013.

[7] SYMANTEC, "Internet Security Tehreat Report, SYMANTEC, Vol.22, Apr 2017.
[8] TrueCrypt, CNET, http://download.cnet.com/TrueCrypt/3000-2092_4-10527243.html (last visited April 24, 2017).
[9] John Leyden, "Brazilian Banker's Crypto Baffles FBI (http://www.theregister.co.uk/2010/06/28/brazil_banker_crypto_lock_out).", REGISTER, June 28, 2010,
[10] Sarah Wilson, " Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals when Third Parties are Forced to Hand Over Passwords, Berkeley Technology Law Journal, Vol.30, pp. 1-39, Spring 2014.
[11] United States Constitution, Amendment V.
[12] Nicholas Soares, "The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age", American Criminal Law Review, Vol.49, pp. 2001-2019, Fall 2012.
[13] United States v. Hubbell, 530 U.S. 27, 34-36 (2000).
[14] United States v. Fisher, 425 U.S. 391, 411 (1976).
[15] Vivek Mohan & John Villasenor, "Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era", Journal of Constitutional Law, Vol.15, pp. 11-28, 2012.
[16] Andrew J. Ungberg, "Protecting Privacy Through a Responsible Decryption Policy", HARVARD J.L. & TECH, Vol.22, pp. 537-558 Spring 2009.
[17] United States v. Doe, 465 U.S. 605-617 (1984).
[18] Kastigar v. United States, 406 U.S. 441, 455 (1972)
[19] United States v. Hubbell, 167 F.3d 553, 555-556 (D.C. Cir. 1999).
[20] David Colarusso, "Heads in the Cloud, a Coming Storm the Interplay of Cloud Computing, Encryption, and the Fifth Amendment's Protection against Self-incrimination", B.U. J. SCI. & TECH. L., Vol.17, pp. 69-102, Nov 2011.
[21] Constitution of the Republic of KOREA, Article 12
[22] Criminal Procedure Act of the Republic of KOREA, Article 244, Article 283
[23] Regulation on Criminal Procedure of the Republic of KOREA, Article 127
[24] Sang-Un Lee, Myeong-Bok Choi, Integer Factorization for Decryption, The Journal of The Institute of Internet, Broadcasting and Communication, VOL.13, No. 6, pp. 221-218, Dec 2013
[25] Yang-Ho Lee, Seung-Jung Shin, A Study on Efficient Encryption for Message Communication between Devices, The Journal of The Institute of Internet, Broadcasting and Communication, VOL.14, No. 5, pp. 19-26, Oct 2014

## 저자 소개

**이 욱(정회원)**

- 2002 ~ : Professor, Department of Information System, Hanyang University
- 1997 : Ph.D, Management Information System, Claremont University
- 1989 : Master, Computer science, Northwestern University
- 1987 : Bachelor, Scienc and Statistics, seoul national university

**지 명 근(정회원)**

- 2010 ~ : Enrolled in the Ph.D. program at the Department of Information Systems, Hanyang University
- 2010 : Master, Industry Management, Korea Polytechnic University
- 2003 : Bachelor Degree of geo and environmental system engineering, Cheongju University.

**이 동 한(정회원)**

- 2014 ~ : Section Chief, Gachon University
- 2014 : Ph.D, Information System, Hanyang University
- 2005 : Master, Ceramic Engineering, Yonsei University
- 2002 : Bachelor, Ceramic Engineering, Yonsei University