Comparative Study of Limitation In Realizing the Right to Be Forgotten in Terms of Technology and Service: Focusing on Access Exclusion and Information Deletion

Mina Shim

Abstract Background/Objectives: *The purpose of this study is to investigate the difficulty of realizing the right to be forgotten from the perspective of existing technologies and services based on differences in the legal and technical realization of the right to be forgotten. The possibility of realizing the forgotten right through existing technology is low, but it is necessary to overcome difficulties and increase the possibility of realization gradually.*

Methods/Statistical analysis: *Therefore, this study examines the previous studies on the legal requirements and concept of the right to be forgotten, the application of technology based on the law, and analyzes the limitations and difficulties of the technology and services to realize the requirements. Because the analysis of difficulties can be ambiguous, the limitations are specified based on "access exclusion" and "informationdeletion" which are especially applied to domestic law.*

Findings: *Realistic application of the right to be forgotten is very important. However, research on the application of existing technologies and services is very limited. This study is meaningful because it focused on the concept of 'access exclusion' and 'deletion of information' to specify the difficulty of realizing the right to be forgotten.In particular, based on the concept of deleting information, we distinguish characteristics of related technologies and services and analyze their practical limitations in detail.If previous studies have simply identified a GAP with legal requirements, this study is an in-depth study that analyzes each of the limitations according to legal requirements in detail.*

Improvements/Applications: *Understanding the limitations and difficulties of related technologies and services is a big milestone in the development of realistic technologies and services in the future. In this sense, it is expected that it will have a practical effect in realizing the right to be forgotten by the system design considering the reality and the service model development considering the technology.*

Keywords: *The Right to be Forgotten, GDPR, Access Exclusion, Information Deletion, Information Destruction, Privacy, Personal Information*

I. INTRODUCTION

The problem of realizing the right to be forgotten is the representative problems such as conflicting with other basic rights, information deleting technology or system limitations, and conflict between countries.In Korea, legislative debate is active, but the stage of technical discussion is only the beginning.Domestic laws are being accessed through the Information and Communication Network Act in the form of 'temporary measures' or in the form of 'deleting personal information' through the Personal Information Protection Act.The realization range can also be very narrow. This is because it is possible to realize a simple delete function.It is therefore very meaningful to study the application of technology and service perspectives on the right to be forgotten.

We can analyze how the regulation surrounding the right to forget the difference in approach of each country is reflected in the technology and service.For example, the norms of the major countries represented by the EU and the United States differ depending on the approach to privacy exclusion, the restriction of personal information processing, and the exclusion of deletion or processing restrictions. As shown in Table 1, the approach of each country can be compared.From a technical point of view, it is also possible to compare the level of each country by separating steps. The proposed step can be divided into five stages: idea conceptualization, patent application, technology development, service modeling, and service operation.

Revised Manuscript Received on May 22, 2019.
Mina Shim Dept. of Computer Engineering, Sungkyul Univ., Republic of Korea
mnshim@sungkyul.ac.kr

Table 1: Comparison of national approaches

Related law and regulation	Right of deletion	Right of Restriction of processing	Exception
8 Principles of Data Protection (OECD Guidelines)	Δ	X	-
EU General Data Protection Regulation, GDPR (2016)	**O**	**O**	**O**
US Bill of Rights	**O**	Δ	X
Personal Information Protection Act of Korea	◎	**O**	**O**
Korea Act on Promotion of Information and Communication Network Utilization and information Protection, etc.	Δ	**O**	**O**

We have identified differences in technological realities based on the legal requirements of the right to be forgotten in previous studies.Therefore, in this study, we try to understand the difference of legal and technical coverage more precisely. As in the previous studies, the analysis standard is composed of the type of information processing (online / offline) and characteristics (information type, legal obligation, entitlement, etc.). It also aims to analyze the limitations and difficulties of application of technology and services according to legal requirements. This analysis can be ambiguous.Therefore, we analyzed the limitations of 'access exclusion' and 'information deletion', which are especially applied to domestic laws such as the Information and Communication Network Act and the Personal Information Protection Act, based on analysis criteria.To do this, we examine the existing research on the difference between the legal requirements of the right to be forgotten and the application of technology through the previous research. And then the concepts of 'access exclusion' and 'information deletion' are analyzed, and the limits of technologies and services focusing on two criteria are analyzed.

II. RELATED RESEARCH

2.1. Concept and legal requirements of right to be forgotten

The right to be forgotten comes from the 2009 French legislation (recognition of the right of oblivion). The EU General Data Protection Regulation ("the GDPR draft") states "the right to be forgotten". Commission refers to the right to be forgotten as “the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. This is the case, for example, when processing is based on the person's consent and when he or she withdraws consent or when the storage period has expired.[1]” In 2014, the EU Parliament's amendment (GDPR Amendment) defined it as 'Right to erasure' instead of the words 'right to be forgotten'. The contents of the right to delete are as follows. i)The right to remove personal information from the administrator ii) the right to cease the further distribution of personal information from the manager iii) the right to remove links to personal information from third parties. The GDPR amendment removes the uncertainty concerns raised. And amendment added “the right to delete links or copies of such information to third parties” [2].The subject information of the exercise of rights was defined as "personal information that is illegally handled". In the event that the Controller is not justified in the proper handling of personal information, it shall take all reasonable steps to remove the personal information as well as deletion by the third party.As above, the GDPR amendment includes the Controller and the "third party, if applicable," as the subject of the deletion and is clarified. However, there are exceptions to the deletion for the right to be forgotten.It may be limited in terms of historical records, freedom of speech, and freedom of expression.

Since the GDPR amendment was released in 2014, various studies are being conducted on the comparison and scope with the relevant laws of each country.The main issues are: i) the right to delete personal information or self-determination, ii) the issue of an article removal request, and iii) the issue of a post removal request.The comparative study with the related laws of Korea(Personal Information Protection Act, Korea Act on Promotion of Information and Communication Network Utilization and information Protection) compared the requirements and limitations of exercise of rights in the right of deletion[3].The Personal Information Protection Act of Korea has the obligation of the personal information processor to destroy the personal information, and personal information may be destroyed by the exercise of the right of withdrawal of consent.Since the Privacy Act does not have the requirement to delete the certificate, it is possible to delete it without restriction in principle. The GDPR amendment specifies specific requirements for the exercise of the right to delete.However, detailed restrictions were made to balance the interests. As shown in table 2, the Privacy Act has a relatively narrower scope of judgment than the GDPR amendment.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Table 2: Legal requirements of each country

Related Law		Requirements	Limitations
EU	**EU GDPR Article 17 (Amendment)**	• if the personal information is no longer needed for the purposes for which it is collected or processed • if there is no legal basis to process the personal information, the withdrawal of consent for processing or expiration of the period of storage • when an information subject exercises opposition rights • if a court or regulatory body in the EU makes a final and absolute decision that related personal information should be deleted • when personal information is illegally handled	• for exercise of freedom of expression • If necessary for public interest • when necessary for historical, statistical, or scientific research purposes • if there have a legal obligation to keep personal information in accordance with the laws of the EU or Member States that the Controller complies with. • when the processing of personal information should be restricted
Korea	**Korea Act on Promotion of Information and Communication Network Utilization and information ProtectionArticle 29, 30**	• cancellation according to withdrawal of consent • in case of destruction reason	• if personal information must be preserved in accordance with other laws
	Personal Information Protection Act of Korea Article 36	• no requirement	• if personal information is specified in the other statute as collecting object • (exceptions) Collection of public institutions by statistical methods, collecting and requesting for the purpose of analyzing information related to national security, collecting information for policing, etc.

2.2. Legal and technical application

The application of technology through domestic legalization is mainly discussed in the information communication network.In other words, legal and technical applications related to search are discussed.The review requirements include the method and subject of the exercise of rights, the object of search exclusion, the request requirement, the deliberation request, reasons for rejection, and the subject of judgment. First, when anyone searches on a portal site, a method of excluding specific personal information from the search list is referred to as a right exercise method.And excludes search results such as posts, replays, links, videos, etc., with or without articles from the media.The search exclusion review considers the following: In other words, the time and purpose achievement, the damage, the third party profit, other laws, etc. The reason for refusal of search exclusion shall be deemed to correspond to a public figure or a public matter. The subject of judging the exclusion of search is discussed as an information communication service provider or a deliberation arbitration committee.

Some studies on application and limitations are underway[4].In the study of the institutions of Korea Act on Promotion of Information and Communication Network Utilization and information Protection and the right to be forgotten, we examined 'temporary measures' for the application of the right to be forgotten.This institution is designed to allow a provider of information and communication services to take temporary measures such as deleting information in response to a victim's request when information that infringes an individual's defamation or privacy is circulated.It can be widely used not only for the right to delete personal information, but also for restrictions on distribution defamation or invasion of privacy.On the other hand, in the case of the right to exercise the right to exclude the search list, it was deemed that there was no legislative space because it was applied to the deletion and processing abruption of the Personal Information Protection Act, temporary measures in the Korea Act on Promotion of Information and Communication Network Utilization and information Protection, correction of the Internet arbitration. However, there are some legislative blanks in terms of the requirements for rejection of search or reasons for rejection.In April 2016, the "Guidelines for requesting access exclusion from Internet self-posting", which specifies the procedure for requesting access exclusion from self-posting, has been enacted.The right to request the exclusion of the self-post access to the

board administrator corresponds to the "right of withdrawal of the uAdd a blankser's consent" (Article 30) of Korea Act on Promotion of Information and Communication Network Utilization and information Protection. The right to request the exclusion of the self-posting search list for the search service provider corresponds to the "Request for Abruption of Personal Information Processing" (Article 37 of the Act) of the Personal Information Protection Act.It can be difficult to say that your post is legal for personal information. However, the scope of personal information is not really limited. Since it is interpreted as any information about the individual, there is no problem if private matter is included. However, there is a limit to the reason for denial of access (public interest). This is because there are conflicts with the reasons for the exception of the related laws. There is a limit to enforce the system such as reverse discrimination with foreign companies, difficulty in identifying the user when requesting exclusion (difficulty in proving technical identity due to withdrawal of membership, etc.) and technical limitations for access exclusion instead of post deletion.On the other hand, ultimately, technical limitations for deleting Internet information are serious problems.Due to the nature of the Internet, it is difficult to find information to search and delete worldwide sites.Even if you delete the archive information from the site with the search engine, you can't delete the information of the personal storage medium. Even if information is searched, the question is who will erase it with what authority.

Recently, the concept of deletion has been classified into three levels as shown in table 3. First is 'Erasing Data Originating from the Data Subject'. Second is 'Erasing Reposted Data that Originated from the Data Subject'. Third is 'Erasing Other People's Data about the Data Subject'[5]. It appears to be included in most legal applications. The first concept of deletion is the deletion of data originated by a data subject.You already have the right to delete your posts from Facebook and other SNS.The second deletion concept is created from the data subject, but the other user deletes the data that has been reposted.You can also request an implementation on a platform such as Facebook or Twitter.However, there is a controversy because a simple link is not recognized as a copyright infringement.The third concept of deletion concerns the deletion of content when a third party posts content for an information subject.This is likely to conflict with freedom of expression[6].

Table 3: Three Degrees of Deletion

Degree of Deletion	Description	Examples
First Degree of Deletion	• Data subject's own postings and pictures online.	• Data subject posts embarrassing pictures of himself on Facebook and seeks to erase them.
Second degree of deletion	• Data subject posts content that a third party copies and reposts on the third party's own site.	• Data subject posts on Twitter, and third party retweet it on her own site. Data subject seeks removal of retweet.
Third degree of deletion	• Third party posts data not created by the data subject but that is about the data subject.	• Third party posts picture of or data about data subject on Facebook. Data subject requests removal of posting.

III. THE LIMITATION OF TECHNOLOGY AND SERVICES RELATED TO THE RIGHT TO BE FORGOTTEN

According to the ENISA, there is a fundamental problem to be solved in order to realize the right to be forgotten. (ii) to keep track of all copies of personal information and all copies of the information derived therefrom; and (iii) to remove any personal information from you. Deciding whether or not you have the right to make a request, (iv) performing the removal of all the information and copies of the information you want, if the person exercising the rights exercises such rights[7]. For i and ii, it is about tracking and detection technologies in the distribution process. Iii and iv is about access control (access-exclusion) and deletion technologies. With existing technology it is difficult to realize the right to be forgotten yet. The limitations and difficulties of the above mentioned problems are analyzed as follows.

3.1. Limitations of technology according to legal requirements

The exclusion of access(access control) to stored or distributed personal information is related to DRM and policy awareness-based Symantec Web technologies. These technologies require techniques that limit whether or not to allow access to personal information. In addition to deleting information, information on stored or circulated personal information is related to information expiration date technology. These technologies require a technique to permanently delete personal information according to the determinations of the information subject. The related technology has the limitation as shown in Table 4.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Table 4: Limitation of related technology

Related technology		limitation
Access Exclusion	DRM technology	• The scope of application is limited because it is only for storage and distribution of applicable information through central management. • Due to interoperability issues, it is difficult to create standardization technology.
	Symantec Web technology based on policy recognition	• Confusion about the same directive may occur in reinterpreting the association of information according to the ontology.
Delete Information	Personal information deletion technology	• There is a difficulty in determining information to be installed on the self destructing device such as contents capable of long-term storage. • There is also a question about who should install it, such as the subject or producer. • If the creator has to install it, it is difficult to judge the personal information.
	Information expiration date technology	• Continuous activation of data is possible after expiration date. • The right to be forgotten about unauthorized copies is still vulnerable. • It is difficult to easily encode data with expiration dates for all information.

Limitation of DRM technology

DRM technology is a digital copyright protection technology that is used extensively in the area of privacy protection. Especially, it plays a role of protecting digital contents from unauthorized persons by using encryption technology. As the detailed technology, there are access control and use control. The former is used when there is a right to certain personal information, and the latter is used to continuously control the use rights according to the granted right.DRM technology is limited to the storage and distribution of applicable information through centralized management. Especially, due to interoperability problems, there is a big obstacle to making standardization technology[8].

Limitation of Symantec Web technology based on policy recognition

Based on policy recognition, Symantec Web technology is a technology that expresses contents and concepts of information based on the meaning of object or URI, which is an object accessible to the Internet. In accordance with the personal information policy that is set up, we support sharing and sharing information on the Internet only within the scope. That is, it is an http technology that provides an extended protocol for applying and exchanging basic information about personal information through a rule-based policy language. These preferences are coded into metadata according to policy.It is possible to set a certain time point as described above, and to restrict connection, circulation and use after the period arrives. But there is a question as to whether this is a full implementation of the right to be forgotten. Confusion about the same directive may occur in reinterpreting the association of information according to the ontology to give meaning to it[9].

Limitation of Personal information deletion technology

The deletion technology detects a personal information file stored in each public or closed system and reports it to the central management server. According to the management policy, it finds a file containing personal information, and forcibly deletes or encrypts it.The deletion technique may be a permanent deletion by installing a self-destruct device or a deletion manager. The self destructing device is a method of installing the content in the contents containing personal information, but it is difficult to decide whether or not it should be installed in all contents capable of long-term storage. There is also a question about who should install the information, such as the subject or the producer. It is also a problem that it is difficult to judge whether personal information is harmful when the manufacturer has to install it.

Limitation of Information expiration date technology

The information expiration date technology is a technique of permanently deleting personal information each after an expiration date is specified. Depending on the importance of the information, the period can be specified long. Expiration Dates for Personally Identifiable Datawould make postings, comments, and other information automatically disappear after a designated period. Expiration dates allow the data subject to “act in time” which parallels the role that forgetting performs in human decision-making. However, “expiration dates are not about imposed forgetting.” Rather, they are about “awareness and human action, and about asking humans to reflect - if only for a few moments - how long the information they want to store may remain valuable and useful.” Therefore, despite the advantage that the expiration date is determined by the data subject and reduce administrative burden in deleting data, there is a limitation that the data may have a continuing vitality after the expiration date due to the public’s right to know[5].All existing technical approaches to ensure the right to be forgotten are vulnerable to unauthorized copying while the date is publicly accessible and a re-dissemination of such unauthorized copies once the data has expired[7]. It is difficult to easily encode data with an expiration date and to be reflected in the storage, sharing, and transmission processing of the Internet business model[5].

3.2. Limitations of services according to legal requirements

The exclusion of access to personal information(access control) is related to provisional measures service, which is a takedown service.This service is about enabling access exclusion when there is a break request for a post.In addition, information deletion is mainly related to deletion service of personal information on online.There are many deletion services mainly for reputation management, but they are well known as digital funeral.In addition, an online search result deletion, that is, a link deletion service is also performed. In particular, personal information destruction services using expiration date technology are included.There is a limitation that these services are commonly performed online. In detail, related services are limited as shown in Table 5.

Table 5: Limitation of related Service

Related service			limitation
Access Exclusion	Temporary Measures Service	Post-break request service	• It does not apply to personal service types such as mail, notes, and memos, and services with copyright providers or posts of external site. • That is, it does not apply to Self-information, Internet self-post or post of the dead.
Delete Information	Personal information deletion service	Online funeral/account deletion/reputation management/portal deletion service	• It does not target posts or search information about third parties. • It is not legal scope and SNS companies are gradually blocking this type of service.
		Online search result deletion service	• Self-post of internet, post of the dead does not apply.
	Personal information destruction service	Messenger's decaying SNS service	• It is provided by information system unit of the service provider, not per user service. • It applies only to the information generated by applying the expiration period from the beginning.

Limitation of Access Exclusion – Request for Posting

The Temporary Action Service will ask you to temporarily suspend the posting in the form of access exclusion to the posting. For example, Naver service is a takedown service for third party posts[10]. If a third party's post infringes on your unauthorized use or defamation, you may request that the post be temporarily suspended. This applies to legal coverage, and is applied to posts, comments, replies, comments, etc., in posts such as cafes, blogs, news comments, etc. of ordinary users.However, this service has limitations that do not apply to posts of personal service types such as mail, notes, memos, and services with copyright providers or posts of external site.

Limitation of Delete Information – Deletion of PI

There are two types of information deletion services. The first is services such as online funeral, account deletion, reputation management, and post deletion services. This service deletes all SNS posts or deletes posts based on the SNS account and password of the user. There is also a form in which digital information is deleted after the user makes a request in life. Suicidemachine, Seppukoo, and Life Ensured are a representative service.The second is a service that deletes online search results. Typically, Google has an information deletion service[11]. The user deletes illegal content (child sexual abuse imagery, copyright infringement) in accordance with Google's deletion policy. In addition, personal identification information (social security number, social security number, etc.), account number, credit card number, signature image, information uploaded or shared without consent (excessive exposure or obscene images, personal confidential medical records, etc.).However, in the former case, it does not fall under the legal scope. In particular, Korea limits the protected object to the information of the surviving individual. Also, it does not target the posts or search information of third parties.Moreover, Facebook is making it difficult to realize such measures by taking steps to block IPs to prevent such services.In the latter case, it falls under the legal scope of application but internet self-post and post of the dead are not applicable.

Limitation of Delete Information – Destruction of PI

The personal information annihilation service implemented by the expiration date technology provides the extinct SNS service of the specific information system or the messenger. DAL's DAS service is representative[12]. The DAS service automatically expire the digital information and expires the information automatically. In recent years, it has also provided a function to set the disappearance time when sending SMS, LMS, and MMS of a mobile phone. However, this service, which is based on expiration date, is provided by the information system unit of the service provider, not by the user unit. In addition, there is a practical limitation in that it is applied only to the information generated by applying the expiration date from the beginning.

IV. CONCLUSION

The purpose of this study is to identify the limits of how difficult it is to realize the forgotten right that is being extended from the EU in terms of technology and services. It is very unlikely

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

to realize the right to be forgotten by existing technologies. Therefore, starting from understanding what technical and service limits are, it is necessary to increase the feasibility.For this purpose, this study examined the concept of the right to be forgotten, the legal requirements, and the application to the reality through prior research.We also looked at the requirements of the EU and national laws (Privacy Act, Information and Communication Network Act).In particular, we have understood the three levels of information deletion, which is a core concept for realization, and examined the characteristics of related technologies and services in terms of both exclusion of access and deletion of information.As a main result, we analyze the limits of realization of existing technology and service rights based on legal requirements.If the existing studies were only to confirm the simple GAP with the legal requirements, this study is meaningful in that the detailed limit of each technology and service is analyzed by the deepening study.In order to realize the rights, technology must be constantly changed, and a service model for realizing rights should be developed.I am confident that this study will serve as a cornerstone for this.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2017R1D1A1B03036486).

REFERENCES

1. European Commission Communication. “A comprehensive approach on personal data protection in the European Union”, 2010.4, COM(2010) 609 final,2010 ARP[cited 2018 SEP];8. Available from: http://ec.europa.eu/transparency/regdoc/rep/1/2010/EN/1-2010-609-EN-F1-1.Pdf
2. European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data(GDPR), COM(2012)0011 – C7-0025/2012 – 2012/0011(COD) (Ordinary legislative procedure: first reading),2014 MAR [cited 2018 SEP]; Available from: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212
3. Kyoungjin Choi. Right to be forgotten-A Personal Information Perspective. Korea association for information law. 2012; 6(2):97-120.
4. Changgeun Hwang. The limitation of domestic application and legislation of the right to be forgotten. Journal of hongik law review. 2016; 17(1):299-327.
5. Michael L. Rustad, Sanna Kulevska. Reconceptualizing the right to be forgotten to enable transatlantic data flow, Harvard Journal of Law & Technology, 2015 spring; 28(2):349-417.
6. Peter Fleischer. Foggy Thinking About the Right to Oblivion. PETER FLEISCHER: PRIVACY…? , 2011 Mar; [cited 2018 SEP]; Available from:http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html
7. Peter Druschel. Michael Backes. Rodica Tirtea. The right to be forgotten – between expectations and practice. ENISA. 2011 OCT; 8-13.
8. A study on plan to reflect ‘the right to be forgotten’ in the legislative system. KISA, 2012 DEC; KISA-WP-2012-0041:100 [cited 2018 OCT]; Available from: http://www.kisa.or.kr/public/library/report_View.jsp?regno=019470
9. Kieron O’Hara. Can Semantic Web Technology Help Implement a Right to be Forgotten. Computers and Law. Univ. of Southampton. 2012 JAN.
10. Naver Service. [cited 2018 OCT]; Available from:https://inoti.naver.com/guide/purpose.nhn
11. Google Delete Service. [cited 2018 OCT]; Available from:https://support.google.com/websearch/troubleshooter/3111061
12. Digital Aging Laboratory’s DAS Service. [cited 2018 OCT]; Available from:http://www.softdal.com/

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication