Forming a New Dimension of Digital Human Rights: A Research Agenda for the Right to be Forgotten

Chanhee Kwak
KAIST College of Business
kchhee@business.kaist.ac.kr

Junyeong Lee
USTC
junyeonglee@ustc.edu.cn

Heeseok Lee
KAIST College of Business
hsl@business.kaist.ac.kr

Abstract

The right to be forgotten has emerged so as to build legal foundations for data subjects to be relieved from misappropriation of personal data on the Internet. However, studies of information systems (IS) on the right to be forgotten and related issues are rare as agreements of the right are diverse according to legal and cultural backgrounds. IS researchers should conduct both explorative and exploitative research in order to build a firm knowledge base for a better understanding of the right to be forgotten from the IS perspective. Doing so would help academia, legislators, and governments, and individuals to understand effects of the right on social, technological and psychological point of view. By suggesting a research agenda to investigate the right to be forgotten, this study sheds light on IS research direction of the right to be forgotten.

1. Introduction

Memory is a certain quality that people have been eager to possess since human beings are destined to forget things in a natural circumstance. The cost of memory was considerably high and those who own memories are regarded as powerful and prestigious. Diverse methods and technologies were devised to remember facts and stories including printing, recording, and oral transmission.

Emergence of early computers and information systems did not significantly change memorizing capability completely. It was impossible to memorize every single activity occurring on systems and machines owing to storage limits. Old legacies and outdated data have to be deleted or moved for long-term preservation. Even if one had a set of data, low computing power made finding and processing a certain type of data extremely costly. In this sense, it is similar to the human memory system which forgets old information and remembers novel ones.

As technologies have developed tremendously, memorizing capabilities and potentials of computers have been increased massively. In particular, improvements in data storage technology are rather impressive in that storage has become cheaper, faster, and larger rapidly. Compared to past versions of hard disk drives (HDD) comprising few gigabytes, even personal computers today are equipped with multiple terabytes with extremely fast solid state drives (SDD) for booting up. If such storages are connected to networks, it is possible to store every single bit of information existing in the world in real time. With the help of the Internet, current technologies are mature enough to take advantage of virtually unlimited repository of data, and data accessibility has been dramatically enhanced. These technological improvements reduce the cost of information storage than that of information deletion and free storage space. Consequently, the "default of remembering" has become the new norm rather than the "default of forgetting" [1].

The "default of remembering" is beneficial, as it has introduced the era of big data. By utilizing myriad data, enormous business opportunities have emerged, which has unleashed a huge wave of innovation. Thanks to the utilizations of big data, highly elaborated and personalized services have improved the quality of life [2]. Enterprises have been eagerly collecting and analyzing a significant amount of personal data for their success. On the other hand, however, memorizing everything can also be problematic in that some people may want to erase records regarding their past such as childhood delinquencies, embarrassing private history, or some miscellaneous information about individuals. Under the new norm of remembering, it becomes extremely difficult to correct or delete such data on the Internet. In other words, individuals are losing their informational autonomy [3].

URI: http://hdl.handle.net/10125/41269
ISBN: 978-0-9981331-0-2

The right to be forgotten has emerged for legal foundations so that data subjects can be relieved from misappropriation of personal data on the Internet. Basically, the right focuses on the guarantee of an individual's claim on the deletion of private information if there is no or less contending interests. Although the importance of the right has started to receive attention, the right has not introduced an entirely new concept; rather, the declaration of the right tries to clarify such right based on existing legal articles and clauses of privacy to deal with technological complexities and information asymmetry. Many countries have debated on the legal procedures for the right from different perspectives while it is the European Union that has initiated and taken the matter forward. Accordingly, the implementation of the right is diverse, ranging from delinking of search result to deleting original data depending on contexts.

The studies of information systems (IS) on the right to be forgotten and related issues are rare partially because the agreements of the right are diverse according to legal and cultural backgrounds of countries. Though the current situation is somewhat complicated and fragmented, we believe that IS research community has to start to build a firm knowledge base for a better understanding of the right to be forgotten. This study provides a research agenda for analyzing the right to be forgotten from an IS research perspective.

2. Emergence of the right to be forgotten and current status

The right to be forgotten, which is defined as "the right of individuals to have their data no longer processed when they are no longer needed for legitimate purposes [4]", has emerged only recently. Although the concept indirectly existed in the current legal system, it is the famous case of Google Spain vs. AEPD (Agencia Española de Protección de Datos, Spanish Data Protection Agency) in 2014 which initiated a forum for discussing the right to be forgotten. In this milestone case, Mario Costeja González wanted that a notice showing the foreclosure of his house in a Spanish newspaper, La Vanguardia, be deleted. He insisted that the information was not relevant to his current financial status and withdrawal of it did not harm social interests. Additionally, he argued that the information should not be exposed when his name was searched on Google Spain. According to the Court of Justice of the European Union (CJEU)'s decision, while the newspaper company could maintain the contents for the purpose of freedom of speech, Google Spain had to remove their links to the notice. The result showed the assent to his arguments since these search results contained information that is "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the [data] processing at issue carried out by the operator of the search engine"[5]. Subsequently, not only the E.U. but also other countries have begun to define the right to be forgotten and find ways to guarantee the right for their people.

As a pioneering movement, the CJEU's decision has meaningful implications. First, search engines, including Google, are not mere pipelines for information delivery; rather, they are data processors and controllers that can manipulate and utilize personal data. The CJEU made the decision based on the fact that Google could store, organize, retrieve, collect and disclose data. Consequently, their legal liabilities and responsibilities have been expanded to cover the right to be forgotten. Furthermore, even if a certain dataset is correct and lawfully posted, an individual's right should be properly evaluated against public interests and freedom of speech. When an individual's present status has little relevance to information about his/her past life, determining the degree of information accessibility can be a prime issue in near future [6].

In contrast, the US treats the right to be forgotten in a different manner since the First Amendment has been powerfully protecting the freedom of speech which can contradict the right to be forgotten either directly or indirectly [7]. It seems that arguments for having a right to be forgotten are usually ended up with results in the favor of the public interests in the US since the US legal system interprets the right as a potential threat to the First Amendment and freedom of speech [8]. Furthermore, compared with the EU, the US emphasizes the freedom of business and free enterprise [9]. Therefore, in terms of restrictions and regulations of enterprises, introduction of the right has been discouraged.

The transatlantic difference between the two approaches, the EU's and the US's, is obvious. Because their value priorities are different from the other. When the Spanish lawyer requests to delete his foreclosure notice against Google, the US legal system may reject his claim owing to the freedom of speech. However, this dichotomy cannot be applied to other countries owing to their diverse cultural and legal backgrounds. Moreover, these relative differences of laws and provisions can create other problems due to the Internet. Since the borderlines of the Internet are vague, it becomes extremely difficult to decide which rule a service provider should follow

and who is responsible for dealing with the requests of data subjects.

In addition to cultural and legal differences, the degree of implementation of the right to be forgotten is diverse. While some countries strictly support the deletion of privacy data, the CJEU's decision is to delink relevant information from search engine results of a specific keyword. However, due to jurisdiction issue, it is still possible to find the delinked search results from Google that has domain name outside of the EU. For that reason, some have argued that such limited delinking is not enough for guarantee of the right [10].

Multiple parties have tried to explore the right to be forgotten, yet individuals, companies and even governments have somewhat confused views on the right to be forgotten. As IS researchers, we believe that there is a role for us to relieve the complexity of chaotic situation.

3. The right to be forgotten from the IS perspective and a research agenda

Research on the right to be forgotten, from the IS perspective is in an embryonic stage since only a small number of countries enforce the right explicitly. Having said that, it does not lessen the importance of the right; rather, it is high time for IS researchers to expand their knowledge and understanding of the right, although the clash of multiple rights and complicated value evaluations will certainly be problematic.

A clear understanding of the existing IS and privacy concepts and subjects related with the right to be forgotten offers guidelines for developing an IS research agenda. The right to be forgotten should be analyzed not only from the IS perspective, but also from that of other research disciplines, including law, psychology, and ethics. We, therefore, suggest the multidisciplinary approach to build a research agenda for the right to be forgotten.

3.1. Information privacy and the right to be forgotten

Nowadays, activities which were once considered as private have been transformed digitally. That is, reading a book, writing a diary, or drinking a cup of coffee at one's favorite café may not be a private activity anymore due to ubiquitous data collections occurring all the time. Furthermore, people get accustomed to uploading their private information on a social network service (SNS) more easily and willingly. Additionally, companies eagerly seek and collect data since complicated analytics technologies need a great set of data regarding transactions, behavioral logs and personal information to provide highly personalized services and products [11]. Though it is a matter of consent of data subjects, data collection and analysis themselves are not harmful; however, the use of abundant individual-related data can increase infringements of information privacy [12].

Information privacy is defined as ″the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others" [13]. The importance of information privacy is getting greater since the usage of data analysis technologies have been expanded to almost all industries, and many privacy problems have been accompanied with the increased employments of such technologies. Eventually, individuals' data become more vulnerable to infringements of information privacy than ever.

The right to be forgotten is closely related with information privacy in that the right is to guarantee that the subjects have a right to decide which data to maintain, who can manage such data, and how long one's data is valid. Therefore, the study of the right to be forgotten contributes to the better understandings of not only the right itself but also information privacy.

3.2. Technologies regarding with the right to be forgotten

In order to implement the right in the digital world, technological support is essential. As a feasible solution, engineers suggest extensive use of digital rights management (DRM) [1, 14]. DRM is designed for a protection method of files from copyrights infringement. Once DRM is applied, files can only be accessed by owners who have earned the right to use them in a lawful way; for others, the files are meaningless and useless. By extending DRM's ability of data protection, it is possible to insert an expiration date into DRM files. Setting expiration dates for files is called data aging technique. That is, when a user creates a file or dataset, s/he can set a specific time period for data accessibility by indicating an expiration date. When a file meets its expiration date it becomes inaccessible, similar to human aging phenomena.

Although an expiration date seems to provide a plausible implementation of the right, it is not a perfect solution. Moreover, even though the expiration date mechanism can enhance users' control over their data, setting dates for every single

dataset can be troublesome even with automated suggestions. It is difficult for users to determine the expiration date due to uncertainty of data usage. At the point of file or dataset creation, it is difficult to define the time period regarding the usefulness of data. In addition to setting an expiration date, it is necessary to consider data type since different data types need to be handled in different ways. We propose possible research topics for DRM and expiration date as follows:

- How does one design DRMs for the implementation of expiration date in order to protect the right to be forgotten?
- What are the criteria for setting expiration dates for different data types?

One of the most recognizable technological examples of the right to be forgotten is Diaspora (http://joindiaspora.com). As a social network platform, Diaspora emphasizes privacy protection with a decentralized structure. It even allows users to have their own cloud so that they can manage their own data [1]. A user's data of Diaspora solely belongs to the one who creates it. Similar to Diaspora, KakaoTalk, the most famous mobile message application in South Korea, has made their effort to distribute their user chat messages to each user and delete original data on servers. Additionally, Instagram, one of the most successful SNS services, has recently introduced Stories which allows users to upload photos and videos that can be accessible for 24 hours. It is interesting to investigate the behaviors and interactions of individuals using alternative communication inventions such as time-limited messaging services. The following research questions can deal with these problems.

- Can alternative communication inventions relieve individuals' concern on the right to be forgotten? If so, what are the factors?
- How do alternative communication inventions affect users' communication behavior in terms of the right to be forgotten?

3.3. Social and cultural issues regarding the right to be forgotten

The perceived value and concept of the right to be forgotten differ from country to country owing to cultural and social differences. Therefore, without the investigation of cultural and societal differences, it is impossible to analyze the effects of the right to be forgotten.

From societal point of view, it is important to estimate the true value of the right to be forgotten. Since the right imposes restrictions and limitations on service providers, it can be interpreted as a type of cost. By comparing the benefits that individuals gain with the imposed costs, the worth of the right can be measured [15]. This is necessary since governments and policy makers seem not to have recognized the true costs and benefits of the right [16]. Therefore, we propose the following research question:

- What are the key factors for the analysis of the social costs and benefits of the right to be forgotten?

It has been argued that the right to be forgotten cannot coexist with the freedom of speech since their interests seem incompatible with each other. However, there are opinions that the behavior of individuals is not the same when they feel they are being watched. Manifested personalities of an individual may not be consistent with the real oneself, and this masquerading behavior can be a potential threat to freedom of speech and democracy which is hugely dependent on the freedom [17]. In fact, the right to be forgotten can enrich the values of freedom of speech such as truth seeking and autonomy [18]. In order to investigate the relationships and dynamics between the right and other rights, the following research questions are proposed:

- Can the right to be forgotten encourage freedom of speech or democracy?
- How can legal systems support symbiosis between the right to be forgotten and other interests?

Current solutions to prevent infringement of the right to be forgotten are a posteriori approach because such damages can be observed only after intrusions. Unfortunately, the right can only prevent further processing and usage of data [14]. It requires individuals' awareness change to solve real problems. Although privacy studies have found that the privacy awareness affects individuals' behavior, it is uncertain whether enhancing privacy awareness always leads individuals to privacy concerned attitude [12, 19]. Often, individuals' behavior and privacy awareness can disagree with each other. Regarding the right to be forgotten, it is possible to observe a similar discordance. In order to study the relationship between privacy awareness and the right

to be forgotten, a milestone can be set by answering following questions:

- What are the factors to enhance awareness of individuals when they provide data about themselves?
- What are the effects of awareness enhancement of the right to be forgotten? How can individuals' behaviors change accordingly?

3.4. Law and policy

Legislation is the key component for the right to be forgotten since it is difficult for information providers to protect their own rights due to information asymmetry without appropriate legal support. Furthermore, from the viewpoint of service providers and information processors, they only have minor incentives to be voluntarily equipped with forgetting capabilities which can cause additional financial costs. Consequently, governments and legislators should take the lead in introducing relevant policies and laws.

Ever since companies and organizations began to store personal data, collateral issues have consistently arisen. Researches have pointed out the importance of timely disposal of data [17]. When it comes to deletion, Peter Fleischer, a chief privacy counsel of Google states three types of deletion requests [20]: (1) a data subject's own data ("If I post something online, do I have the right to delete it?"); (2) others' data which were copied from a data subject's data ("If I post something, and someone else copies it and re-posts it on their own site, do I have the right to delete it?"); and (3) others' data, which are relevant to a data subject ("If someone else posts something about me, do I have a right to delete it?"). The first argument is somewhat less controversial since the deletion of subject's own data is unobjectionable if deletion is not against public interest. However, the other two are debatable in that they can infringe other rights such as the freedom of expression [8]. It is critical to balance multiple rights simultaneously for both the right to be forgotten and information privacy and this is the primary role for laws and policies.

In addition to balanced decisions, the original CJEU's decision was implemented by delinking relevant information from search results when specific keywords are entered. However, delinking is not enough for complete implementation of the right to be forgotten [10, 21]. The issue in this case is the level of being forgotten. The following research questions will shed light on disputes over legal and politic issues:

- What are the key rules in determining the infringement of the right to be forgotten?
- How does one make a balanced decision for the right to be forgotten when multiple rights are colliding?
- How can one decide a proper implementation level of the right to be forgotten when country-dependent contexts are taken into consideration?

The roles of data protection authority (DPA) and data controllers need to be discussed. Many countries already have a DPA in place, which arbitrates in disputes relating to privacy interests; however, it is impossible for DPAs to deal with all privacy infringements requests since they need to deal with nation-wide privacy problems as a governmental organization. For this reason, it is necessary to separate responsibilities for authorities and organizations. The related questions of interest are:

- What are the roles and responsibilities of the DPA for the right to be forgotten?
- How can DPA solve information asymmetry between large companies and individuals in terms of the right to be forgotten?

An important characteristic of the Internet is borderlessness. As digital data can be transferred from place to place, borderlines between countries become vague in the online world. Accordingly, individual's behaviors are getting extremely complicated when it comes to jurisdiction. On one hand, through the Internet, individuals can use various services provided by not only domestic but also multinational companies. On the other hand, many companies today can have distributed servers and data processing systems located worldwide. As a result, the implementation of the right to be forgotten often faces with the jurisdiction problem [7, 14]. For example, when Google Spain implemented delinking according to the original decision of CJEU, only the EU and EFTA domains were modified, in which the CJEU's decision is effective and valid. That is, when the Spanish lawyer's name is typed in Google.com or other non-European countries, search results will still display foreclosing notices of the newspaper.

In order to solve the jurisdiction problem, international agreements and cooperation for the

protection of one's rights are essential. International organizations such as UN (United Nations) and OECD (Organization for Economic Cooperation and Development) put effort into building consensus about the right, but different legal value systems and their non-compulsiveness result in a stalemate. From academia, some studies have dealt with this issue [22-24], yet IS-driven studies are lacking. Majority of existing studies focus on differences between the EU and the US although many other countries adopt diverse legal and value systems. The difference of legal and value systems needs to be further studied:

- How can conflicts related to the right to be forgotten be mediated when the jurisdiction is blurred?
- How can rules and policies be determined for international service providers and web sites to deal with the right to be forgotten?

3.5. Service provider as a data processor and controller

Service providers, who process users' data, need to make preparations to abide by the regulations related with the right to be forgotten. In essence, they ought to find a way to compromise two different values simultaneously: user privacy protection and business success. Some fortunate service providers may have dealt with a similar situation of copyright issue. Request handling for copy right and the right to be forgotten shares similarities in that not only owners or creators, but also the third person can claim a right to manipulate certain data. However, it is less clear when it comes to the decision making on whether an argument is justifiable in terms of the right to be forgotten and information privacy [25]. In order to manage complexities, data management departments should be able to evaluate privacy-related information in various ways since their decisions depend on public interests vs. personal interests. Hence, we propose the following research questions:

- What is the required process to evaluate the value of a specific dataset when an individual demands the right to be forgotten?
- What are the capabilities that can guarantee individuals' information privacy and the right to be forgotten?

Among many information processors, the search engine industry is the most relevant to the right to be forgotten. Search engines were considered as a neutral medium for data delivery. Similarly, they defended themselves from legal responsibilities as they portrayed themselves as innocent information providers. However, as CJEU decided differently, they had to reconsider the concepts of search engine services [26]. The following questions try to analyze the dynamics of the search engine within the context of the right to be forgotten:

- What type of service provider needs to be considered as data processor and controller other than search engine?
- How can authorities decide which service is a mere intermediary or not?

Some European countries require companies to have data protection officer (DPO), who is dedicated to dealing with data management and privacy issues. Similar to other positions, however, a DPO cannot enhance organizational data protection without enterprise-wide support. Further studies should reveal roles of DPO and how organizational structure can support DPOs and their activities:

- What are the roles and responsibilities of the DPO?
- How does one design an organizational structure and procedures in order to support not only DPO but also the whole data management?

Organizational readiness of service providers is worth mentioning here. The protection of the right to be forgotten is more complex than simple policies and expertise; rather, organizational readiness should be evaluated from technological, procedural, and structural perspective. Additionally, transparency of the overall processes is critical in that it shows a company's process is conducted in legal and just ways.

- What are the criteria for evaluating a company's readiness for the right to be forgotten?
- How does one assure transparency of data management processes for the right to be forgotten?

3.6. Online reputation system and privacy agents

As every activity on the Internet is saved and recorded, the cumulative online history can establish individual online reputation. Traditionally, online reputation refers to a peer review system in a certain online group [27, 28]. Today, however, the Internet itself has become a gigantic reputation system: one's online reputation can be easily assessed by typing his or her name in search engines. Search results can include not only one's vocational and professional data, but also private and delicate data that the data subject may not want to make them public, and these results can constitute one's online reputation and possibly offline reputation. The right to be forgotten is directly related to online reputation and digital foot prints since both of them deal with personal digital history on the Internet [14]. Online reputation agency was once considered as a luxurious service for public figure and celebrities; however, it becomes common occasion for an ordinary person to use such services because of the difficulties of cleaning up personal information on the Internet.

A common side effect of the online reputation system is that these reputation evaluations are biased since accurate ratings and feedbacks are not available. Incorrect information can be harmful to one's online reputation and possibly offline reputation [15]. Furthermore, the same problem can occur when we expand the notion of online reputation system to the Internet. It is of interest to investigate online reputation services in terms of the right to be forgotten:

- What is the potential impact of online reputation on the Internet for individuals and companies?
- What are the effects of incorrect information on online reputation in the Internet? How can IT system correct the incorrect information?
- What is the effect of anonymous information on one's online reputation?

4. Conclusion

People upload massive information about themselves on the Internet which can be used by many others who are interested in taking advantage of personal information. However, information providers are incognizant of these usages and are not aware of how to retrieve private information and stop the unwanted distribution. The right to be forgotten deals with this new dimension of digital human right which can possibly collide with existing laws, customs, and other rights.

In order to gain in-depth understanding and knowledge about the right to be forgotten, this study suggests a research agenda to investigate the right from IS perspectives. We do not claim that our research agenda covers all relevant research questions. Rather, we hope to see many other studies on the topic from diverse point of views.

As IS researchers, we expect that research from the IS field can help build a constructive forum for the right to be forgotten by offering a variety of studies. Our research agenda can be a good starting point for IS researchers to expand their knowledge of the right.

5. References

[1] Mayer-Schönberger, V., Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, 2011.

[2] Mcafee, A., and Brynjolfsson, E., "Big Data: The Management Revolution", Harvard business review, 90(10), 2012, pp. 60-69.

[3] Cohen, J.E., "Examined Lives: Informational Privacy and the Subject as Object", Stanford Law Review, 2000, pp. 1373-1438.

[4] European Commision, A Comprehensive Approach on Personal Data Protection in the European Union, (Communication) COM (609) 2010 final.

[5] Google Spain Sl Google Inc. V Agencia Española De Protección De Datos (Aepd) Mario Costeja González, (C-131/12) ECLI:EU:C:2014:317.

[6] Bygrave, L.A., "A Right to Be Forgotten?", Communications of the ACM, 58(1), 2015, pp. 35-37.

[7] Newman, A.L., "What the "Right to Be Forgotten" Means for Privacy in a Digital Age", Science, 347(6221), 2015, pp. 507-508.

[8] Rosen, J., "The Right to Be Forgotten", Stanford Law Review Online, 64(88), 2012.

[9] Bernal, P., "The EU, the US and Right to Be Forgotten": Reloading Data Protection, Springer, 2014, pp. 61-77.

[10] Mayer-Schonberger, V., "Omission of Search Results Is Not a "Right to Be Forgotten" or the End of Google", The Guardian, 13, 2014.

[11] Lee, D.-J., Ahn, J.-H., and Bang, Y., "Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection", MIS Quarterly, 35(2), 2011, pp. 423-444.

[12] Acquisti, A., Brandimarte, L., and Loewenstein, G., "Privacy and Human Behavior in the Age of Information", Science, 347(6221), 2015, pp. 509-514.

[13] Westin, A., "Privacy and Freedom", Atheneum, New York, 1967.

[14] Ausloos, J., "The 'Right to Be Forgotten'–Worth Remembering?", Computer Law & Security Review, 28(2), 2012, pp. 143-152.

[15] Ambrose, M.L., "It's About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten", Stanford Law Review, 16, 2013, pp. 369.

[16] Wigan, M.R., and Clarke, R., "Big Data's Big Unintended Consequences", Computer, 46(6), 2013, pp. 46-53.

[17] Blanchette, J.-F., and Johnson, D.G., "Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness", The Information Society, 18(1), 2002, pp. 33-45.

[18] Youm, K.H., and Park, A., "The "Right to Be Forgotten" in European Union Law Data Protection Balanced with Free Speech?", Journalism & Mass Communication Quarterly, 93(2), 2016.

[19] Norberg, P.A., Horne, D.R., and Horne, D.A., "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors", Journal of Consumer Affairs, 41(1), 2007, pp. 100-126.

[20] Fleischer, P., Foggy Thinking About the Right to Oblivion, http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html, accessed June 7, 2016.

[21] Bernal, P.A., "A Right to Delete?", European Journal of Law and Technology, 2(2), 2011.

[22] Bennett, S.C., "Right to Be Forgotten: Reconciling Eu and Us Perspectives, The", Berkeley Journal of International Law, 30(1), 2012, pp. 161.

[23] Rustad, M.L., and Kulevska, S., "Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow", Harvard Journal of Law and Technology, 28(2), 2015, pp. 349.

[24] Schwartz, P.M., "The EU-US Privacy Collision: A Turn to Institutions and Procedures", Harvard Law Review, 126, 2013, pp. 1966.

[25] Weber, R.H., "The Right to Be Forgotten: More Than a Pandora's Box?", Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 2(2), 2011.

[26] Mantelero, A., "The Eu Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten'", Computer Law & Security Review, 29(3), 2013, pp. 229-235.

[27] Resnick, P., Kuwabara, K., Zeckhauser, R., and Friedman, E., "Reputation Systems", Communications of the ACM, 43(12), 2000, pp. 45-48.

[28] Jøsang, A., Ismail, R., and Boyd, C., "A Survey of Trust and Reputation Systems for Online Service Provision", Decision Support Systems, 43(2), 2007, pp. 618-644.