The Challenge of Indonesia in Applying the Right to be Forgotten

Sayid Mohammad Rifqi Noval
Faculty of Law, University of Islam Nusantara, Indonesia
E-mail: juristdomain@gmail.com, sayidrifqi@uninus.ac.id

Article History
Received: 20 June 2018 **Revised:** 11 July 2018 **Accepted:** 20 July 2018

Abstract
The results of the amendment of Law No. 11 of 2008 on Electronic Information and Transactions (UU ITE) not only solving problem but also causing new problem. UU ITE No. 19 of 2016 regulates the authority of a person to delete his/her personal information on an internet page or otherwise known as the Right to be Forgotten (RTBF) which was previously popular in European countries. In many studies this Right is always confronted with the right of the freedom of expression, thus the fundamental issue concerning this right is an attempt to balance the two. This paper shall discuss the history of RTBF, review several cases related to the implementation of RTBF in several countries, compare the RTBF concept to be applied in Indonesia, analyze the challenges in the implementation process, as well as try to find models for the proper implementation in Indonesia. Indonesia should immediately prepare government regulations in response to the RTBF, given the potential problems if there is no detailed instrument of the implementation. As well as to further determine the competent authorities to assess each submitted application is based on the RTBF.
Keywords: Right to be Forgotten, Data Protection, Right to Privacy

Introduction
Internet has become a familiar term for some of Indonesians. The use of internet technology is an outstanding phenomenon. First, internet has global characteristics and knows no national boundaries; Second, every internet user can communicate interactively or non-interactively, even can conduct broadcasting activities with relatively lower costs; Third, no one can claim that they are the "owners" of internet which is the compilation of hundreds of networks; Fourth are extraordinary internet user growth and rapid internet technology development; Fifth, internet is not under the scope of governance of a certain country or organization so international cooperation is necessary to mitigate the occurring legal issues. The aforementioned things have made internet technology unique so it is necessary to find regulation or law which can be applied optimally in information technology activities (Budhijanto, 2010).
Numerous studies have been conducted related to the relationship between virtual world and law, including the thoughts doubting law's capability in regulating virtual world. After experiencing various evolutions of thought, Lawrence Lessig concluded that virtual world will eventually be regulated by law. This conclusion was made after Lessig reviewed the relationship between law in real world and its capability to regulate virtual world. Lessig claimed that there is a systematic competition between virtual and real worlds affecting legal regulations (Djafar and Veda, 2014).
According to the report released in 2011, UN special reporter for freedom of speech and expression Frank La Rue said that the issue currently faced in utilizing internet technology, besides digital disparity issue, is the increasing attempts to restrict contents, which tends to

restrict human rights, especially the rights over internet access. Some of the content restriction attempts are specifically regulated in national laws, while the others are merely governmental policies. La Rue identified that content restrictions are materialized in forms of (1) Arbitrary internet content filtering and blockade; (2) Criminal sanctions for internet users over legitimate expressions; (3) Implementation of legal liability to middlemen (ISP); (4) Internet access termination under the reason of HaKI; and (5) Weak personal data and privacy protection (Jafar, 2013).

As we know, internet-based information has *free* flow of information principle, which means the spread of the information cannot be hindered, but it does not mean all internet-based information can be accessed by anyone without any restriction. Every information owner can determine privacy protection against the information owned by the related person in internet media (Kantaatmadja, 2002), so similar understandings about things related to privacy is necessary. David Flahaerty explained a list of descriptions about information related to privacy, namely: (1) The right to individual autonomy; (2) The right to be left alone; (3) The right to a private life; (4) The right to control information about oneself; (5) The right to limit accessibility; (6) The right to exclusive control of access to private realms; (7) The right to minimize intrusiveness; (8) The right to expect confidentiality; (9) The right to enjoy solitude; (10) The right to enjoy intimacy; (11) The right to enjoy anonymity; (12) The right to enjoy reserve; and (13) The right to secrecy (Makarim, 2005).

However, this development brings another impact related to privacy protection. In various countries, privacy-related issues and regulation about privacy have been growing as a complete part of social development. Therefore, it is understandable that in several democratic countries, positive law and jurisprudence about privacy have occurred far before privacy becomes a complete part of a human rights legal regime (Indriaswati and Djafar, 2013). Therefore, the regulations protecting the rights are created. In general, protection against rights occurring in conjunction with the activities is a necessity. There are three (3) dimensions of rights which are protected and whose implementation is guaranteed by Article 19 of ICCPR, namely (Jafar, 2016); (1) Freedom to deliver opinion without disturbance; (2) Freedom to seek and obtain information; (3) Freedom to forward information.

William L Posser realized that inconsistency is developed even leads to confusion when explaining about privacy, but Posser cited at least four things describing the privacy, namely: (1) Intrusion upon a person's seclusion or solitude, or into his private affairs; (2) Public disclosure of embarrassing private facts about an individual; (3) Publicity placing one in a false light in the public eye; (4) Appropriation of one's likeness for the advantage of another (Ritchie, 2009).

One of the most essential concepts related to privacy according to Neil Richards is called *Fair Information Practice* (FIPs). FIPs is a set of principles developed in 1970 by the government of United States of America and regulates the relationship between business and governmental entities which collect, use, and disclose personal information about "data subject" (a person whose data is being collected and used). In its report, the government of United States of America introduced FIPs by describing it as five basic principles to be guaranteed by automatic data system (Richards, 2016): (1)*There must be no personal-data record-keeping systems whose very existence is secret*; (2) *There must be a way for an individual to find out what information about him is in a record and how it is used*; (3) *There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purpose without his consent*; (4) *There must be a way for an individual to correct or amend a record of identifiable information about him*; (5) *Any organization creating, maintaining, using, or disseminating record of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data*.

In the development of international human rights law, the protection of rights to privacy is regulated in Article 12 of General Declaration of Human Rights, which emphasizes: "No one shall be disrupted arbitrarily in their personal, family, household or correspondence matters and no attack shall address their honors and reputations. Every person is entitled to obtain legal protection against such disruption or attack." In the context of Indonesian law, the protection against rights to privacy has been acknowledged as one of citizens' constitutional rights, as emphasized by 1945 Constitution, after amendment. The provision of Article 28G section (1) of 1945 Constitution states: "Every person is entitled to the protection of personal, family, honor, dignity, and asset under their possession and entitled to sense of security and protection from the threat of fear to do or not to do something which is human right."

Even though several countries, especially in Europe, have regulations related to privacy data protection, Europeans have relatively great anxiety over personal data. It can be seen from the result of survey conducted in 2015 against 28,000 citizens of European Union that 66% feel anxious to not have full control over the information they give online. Approaching 70%, an explicit agreement is needed before data collection and processing and the use of data is not suitable with its initial purpose (Urquhart and Rodden, 2017).

In Europe specially, privacy has been seen to have a temporal aspect: the right at some point to be free of the past. European privacy law has recently come to recognize what is called the "*right to be forgotten (RTBF)*" (Francis and Francis, 2017). The term RTBF draws wide attention after the case of Mario Costeja Gonzales was decided by *the Court of Justice of the European Union* in 2014. The review of RTBF progresses with various criticisms and supports for it, and in its development in 2016, Indonesia promulgated Law No. 19 of 2016 about amendment of Law No. 11 of 2008 about Information and Electronic Transaction (UU ITE) containing provisions which, for some elements, are deemed as the form of RTBF or known as 'Hak untuk dilupakan' in Indonesia.

The Case of Mario Costeja Gonzales

On 13 May 2014, *the Court of Justice of the European Union (CJEU)* judging the case of *Google Spain v AEPD* and Mario Costeja Gonzales stated that *right to be forgotten* occurred in the context of data processing in search engine sites. The case was filed by Mario Costeja Gonzales, after he attempted to delete the information about his house auction event in 1998 posted on a newspaper site *La Vanguardia*, which was newspaper with the most reader in Catalonia (Kampmark, 2015). *La Vanguardia* conducted digitalization process against its news archives, including which released in January and March 1998 related to the auction of Mario's house due to his social guarantee debt. Mario was objected by the news since it raised issues related to his profession. His request was initially rejected by Google, but eventually on 5 March 2010, Mario filed his complaint to *Spanish Data Protection* (AEPD) to face *Google Spanyol SL and Google Inc*. Mario reasoned that both news had to be deleted since his debt had been paid off and the news made inaccurate impression related to his current economic condition (Carbone, 2015).

In its verdict, CJEU considered Article 14 EU Directive 95/46/EC which covers personal data processing and the freedom of distribution of the data. One of essential points to be noted is about to what extent the liability of a company like Google against information provided through search engine sites. On the trial, judge decided that search engine operator was liable over the processing of personal data posted on the web page published by third party (Kampmark, 2015).

One thing drawing the attentions of legal and policy experts related to the verdict given by CJEU in Gonzales case is a philosophical basis in its association with data control aspect. One of which is the belief that the system is result of human works, created by human and intended for human. The opening of Article 1 EU Directive 95/46/EC states that "*data*

processing systems are design to serve man;....they must, whatever nationality or residence of natural persons, respect their fundamental rights and freedoms notably the right to privacy, and contribute to... the well-being of individuals". In the case, either Google Spain or Google Inc opted to act by referring their arguments to '*the act of processing data*'. The argument stated that search engine sites "*cannot be regarded as processing the data which appear on third parties' web pages displayed in the list of search results*". According to them, the information in search engine is processed without selection process between *personal data* and other information. Disagreement was shown by Gonzales and the Government seeing search engine sites as "controlling parties" in data processing. However, in the end, the Court agreed with Gonzales' argument and deemed that applicant's privacy rights waived not only economic interest of Google, but also public's interest against information access on search engine sites related to the name of applicant. Applicants in EU are entitled to ask for information deletion under reasons that the information is *inadequate, irrelevant* or *no longer relevant* and *excessive* in its initial purpose is processed (Kampmark, 2015).

This decision is not only devoted to Google, but also to other search engines which run in the scope of EU's market such as Bing and Yahoo. The search engine sites need to prepare infrastructures to respond to the presence of *right to be forgotten*. However, Google still needs to be the most hard-working party since 90% of European market uses its search engine (Carbone, 2015).

Responding to the verdict of *Court of Justice of the European Union (CJEU)* related to the deletion of links about personal information, Google asked for considerations from groups of international experts in deciding and responding to the requests submitted to its company. Board of experts briefly suggested Google to (a) implement delisting decision for all sites in European region (such as Google.de, Google.it, Google.es and others); (b) give information to information *publishers* when delinking process was initiated. Four other criteria were given to guide Google in assessing *delisting* requests: (i) conducting evaluation against public roles from data subject; (ii) considering whether information which will be deleted from list affects public or personal interests; (iii) considering information sources; (iv) information time interval becomes one of criteria in determining its relevance (Taddeo, 2016).

Right to be Forgotten Concept

George Brock stated there is no legal basis unity which is applicable internationally and is used to enforce *right to be forgotten* principle. *The European Convention on Human Right* warrants *right to privacy* on Article 8 and *right of free expression* on Article 10. *The UM Declaration of Human Rights* regulates similar provision on Article 12 and 19. *The EU Charter of Fundamental Rights* regulates *rights to privacy* on Article 7, *the right to data protection* on Article 8, and *the right to free expression* on Article 11. *The UK's Human Rights Act* re-emphasizes the rights previously regulated in *European Convention* (Brock, 2016).

Right to be Forgotten can be implemented on two correlated things but different designations: *First*, data collected about a person - due to business or governmental interests - is not allowed to be used besides its initial designation purpose and the data has to be deleted immediately if it is no longer needed based on its initial purpose; *Second*, that *search engines* are required in special conditions to delete a *link* leading to certain information when searching the name of a person on a search engine, even though the information is correct but inflicts loss to the person or when the person opts to not be involved in the result of the searching system. The second idea describes restrictions of the type of information which has to appear when searching the name of a person on search engines (Isom, 2016). However, an interesting thing occurred when Koutnatzi explained about the legal basis of *Right to be Forgotten*. Koutnatzi explained that RTBF can be used for someone who has served a

sentence for their crime, due to difficult *reintegration* process for an ex-convict to social environment and rejections to them (Koutnatzi, 2012). Koutnatzi's perspective as if rams privacy right and public right to obtain information, after previously several newspaper portals complained about threat potentials if the RTBF was not carefully implemented.

At least the supporting group like German newspaper *Der Spiegel* states that individual rights need to be enforced over economic interest of search engine sites. Similar with *Der Spiegel*, Spanish newspaper *El Pais* states that "*.. it did not seem logical that in a "democratic society in which even criminal records may be cancelled after a certain period of time, the Internet could become a life sentence for some people*". However, the opposing group like US newspaper *New York Times* states its rejection explicitly and sees that RTBF can hinder journalists' works and make their sounds unheard and will harm freedom of press and expression (Santin, 2017).

Weber explained a perspective which often correlates *Right to be Forgotten* with *right to forget*, since one last decade the debate related to *right to forget* used to take place. Weber explained that actually, both rights are different. Weber comprehensively states: *The "right to forget" refers to the already intensively reflected situation that a historical event should no longer be revitalized due to the length of time elapsed since its occurrence; the "right to be forgotten" reflects the claim of an individual to have certain data deleted so that third persons can no longer trace them* (Weber, 2011). According to Weber's perspective, the essential point related to the difference of both rights above, is individual power against their information to not be found again by other parties, so the original data remains in the site but Google's search engine cannot find it.

The policy of *Right to be forgotten* in UK applies on search engines like Google, and does not restrict whether the information is a journalistic product, as experienced by *The Guardian*'s site which has to lose six of its articles from Google's search engine (Ball, 2017).

Several journalistic media reported the removal of several of their articles on Google's search engine. BBC media reported the article published in 2007 about a former director of an investment company Merrill Lynch involved in a financial scandal was no longer indexed on Google's search engine. The Guardian used to protest about a Scotland referee involved in a fraud case of penalty in a match (Santin, 2017).

One of the influences of digital world is the presence of digital memory. Schonberger explained Three features of digital memory make this possible (Schonberger, 2009).: (1) **Accessibility**. In an analog world, data and information will be restricted to be known by other parties, since information owners are capable of restricting them. An example is a hepatitis B patient asking his doctor to not deliver the disease information to anyone. The other example is the collection of photos saved in an album, when being published to virtual world, the opportunities of other parties to access or see them are possible, especially when the photos are "tagged"; (2) **Durability**. Storing information previously was a burden to be specifically prepared since it was proven to require costs. For example, a communist country has never forgotten information related to identities, acts, and words from opposing people. However, in digital era, similar intention is not a heavy burden. Google remembers every search query of a person, even though every day sees one billion queries. A person currently cannot get away from their pasts related to the access in virtual world; (3) **Comprehensiveness**. Digital memory has capabilities to process information comprehensively, due to its capabilities to collect and complete data, data location/region is no longer an obstacle. However, this, on the other side, will be a potential issue since the capability to record information without confirming about data validity eventually leads to conclusion unfounded or not suitable with the context of time and space. As experienced by Andrew Feldmar, a Canadian psychotherapist, who was not allowed to enter USA by border

officers, was based on the search they conducted on Google's search engine, which was the consumption of drugs conducted by Andrew Feldmar in 1960.
Several examples of RTBF requests delivered by individuals from various countries to Google are as follows:

Table 1 Examples of requests google received from individuals

No.	Country	Request	Outcome
1.	Austria	Google received a request from the Austrian Data Protection Authority on behalf of an Austrian businessman and former politician to delist 22 URLs, including reputable news sources and a government record, from Google Search.	Google did not delist the URLs given his former status as a public figure, his position of prominence in his current profession, and the nature of the URLs in question.
2.	Finland	Google received a request from the wife of a deceased individual in Finland to delist a forum page from Google Search that alleges the deceased individual committed several sex crimes. The request was to remove for the deceased individual's name.	Google delisted the URL under Finnish data protection law.
3.	France	Google received a request from an individual to delist several URLs from Google Search about his election as leader of a political movement and other political positions he held when he was a minor.	Google delisted 13 URLs as he did not appear to be currently engaged in political life and was a minor at the time. We did not delist 1 URL as the page referred to a different person who had the same name as the requester.
4.	Germany	Google received a request to delist 4 news articles about an academic's research that contained the individual's photo because the academic changed gender and identifies under a new name.	Google did not delist the articles as they continue to be relevant to the academic's professional life and research.
5.	Italy	Google received a request to delist dozens of recent, reputable news articles regarding the conviction of an individual for rape, including video footage of the victim.	Google initially refused to delist the articles and the Italian Data Protection Authority wrote to Google asking to explain our decision. We decided to maintain our decision to not delist the articles given their recency and the severity of the crime. The Italian Data Protection Authority agreed with our decision to not delist the content.

Table 1 (Con.)

No.	Country	Request	Outcome
6.	Netherland	Google received a court order directed to Google Inc. to delist from Google Search a blog post about a professional who was convicted for threatening people with a weapon on a city street.	Google appealed the decision, but lost our appeal. We delisted the blog post.

In the context of Indonesia, privacy protection has actually been acknowledged since long time ago. At least Criminal Code states several articles of criminal acts related to privacy such as prohibition to open letters, and prohibition to enter personal land/property and other criminal acts related to position crime. Despite its presence since long time ago, the protection for right to privacy has yet to be a part of protection given by Constitution. On 18 August 2000, the protection for right to privacy becomes a part of constitutional protection (Anggara, 2015), as stated on Article 28G of 1945 Constitution. Similar emphasis is also stated on the provision of Article 29 of Law No. 39 of 1999 about Human Rights, and Indonesia has also ratified International Covenant on Civil and Political Rights (ICCPR). However, the constitutional guarantee has yet to be well-materialized in statutory level. Even though identification was conducted, at least there are 30 laws in Indonesia whose materials are related to the importance of protection against citizens' personal data. In its practice, the handover of a person's personal data without the knowledge of data owners still often occurs, especially which is allegedly conducted by parties which record and store personal data, either conducted by governmental or private institutions (Djafar, Sumigar, Setianti, 2016).
The implementation of Law No. 19 of 2016 about amendment of Law No. 11 of 2008 about Information and Electronic Transaction (UU ITE) in Indonesia also generates various opinions about it. One of which is related to the existence of *Right to be Forgotten*. The provision is stated on Article 26 section (3): "Every electronic system organizer shall delete irrelevant electronic Information and/or electronic documents under their control over the request of the related person based on court's decision". Moreover, Article 26 section (4) states that: "Every electronic system organizer shall provide deletion mechanism for irrelevant electronic information and/or electronic documents based on statutory laws". Article 26 section (5) states: "Provisions about the procedures to delete Electronic Information and/or Electronic Document as stated on section (3) and section (4) are regulated in governmental regulations."

Research Methodology

This research chooses descriptive-evaluative and prescriptive approaches as its method. With its descriptive nature, this research is intended to provide some explanations about the background of the needs to regulate the use of internet technology, especially those related to *Right to be forgotten*, and the expected regulation models. Meanwhile, evaluatif approach is intended so that this research is able to provide expositions about several existing legal issues, in the implementation of *Right to be forgotten* in several countries which have implemented it, so renewal is necessary. On the other hand, prescriptive approach is intended to place this research as an instrument to obtain suggestions and solutions about what has to be conducted when arranging policies related to the use of internet technology, especially those related to *right to be forgotten*, to synchronize it with privacy data protection in Indonesia.

Research Result

The research related to the challenge of RTBF implementation in Indonesia found that Indonesian government currently has yet to be fully ready to implement the RTBF. At least, the government needs to prepare some regulations to regulate the details of RTBF implementation flows to the technical guidance of RTBF performance. Europe Union (EU) has ratified General Data Protection Regulation (GDPR), a regulation about data privacy enacted for all companies across the globe which store, compile, or process EU citizens' personal information, has been in force since 25 May 2018, and has replaced EU Directive 95/46/EC which so far has been used as the basis of RTBF. The provisions about RTBF in GDPR are stated on Article 17 namely:

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

1.1 the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

1.2 the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

1.3 the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

1.4 the personal data have been unlawfully processed;

1.5 the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

1.6 the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

3.1 for exercising the right of freedom of expression and information;

3.2 for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

3.3 for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

3.4 for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

3.5 for the establishment, exercise or defence of legal claims.

The enforcement of GDPR currently becomes homework for Indonesian government to prepare regulations about RTBF since GDPR applies in an extra-territorial basis. Moreover, big criticism delivered to the concept of Indonesian RTBF can refer to the GDPR which does not implement RTBF without limitation. Article 3 above has properly regulated several limitations/exceptions against the RTBF. The other challenge is the existence of Law No. 14 of 2008 about Public Information Transparency (UU KIP) and Commission of Information Institution. UU KIP provides warrants to people to access public information and if some

people feel that their accesses are blocked, they can deliver their complaints to Commission of Information. Conflicts may occur between the rights of people to obtain information and the right of an individual to have their information removed.

The other challenge is court ruling instrument as a prerequisite to perform RTBF. Several countries in Europe use similar flows before proposing RTBF to Google's search engine even though a release from Google states that there are 1 forged Canadian court order, 1 forged US court order, 4 forged Indian court orders, 4 forged Peruvian court orders, and 5 forged German court orders (Google, 2018). Compared to the conditions in Indonesia whose case issues have yet to be well-mitigated, Indonesia needs to consider an authorized institution to decide RTBF proposal in Indonesia. As information, in 2016, from 352 courts across Indonesia, only 64 courts or 18% had positive performances (green reports). The recapitulation to assess the performances of those district courts is performed using Case Handling Information System (SIPP) application. This system shows the courts whose case handling is over 90 percent will obtain green reports, while those whose performances are less than 90 percent will obtain yellow reports (Tempo). An institution authorized to make the decision needs to have special trainings, just like Google preparing its review teams which specifically conduct the role and are mostly placed in Dublin, Ireland.

Conclusion

Fundamental differences can be seen related to RTBF concept implemented in Indonesia and in Europe. At least there are two main differences of it. First, the implementation of RTBF in European countries is addressed to search engine sites like Google, Yahoo, and others. RTBF becomes a basis for an individual to ask search engine sites to delete on search results personal information which may appear when the name of a person is typed. However, public will still find original articles of the information if they search it on original sites without search engine sites. Different from Europe, Indonesia takes extreme measures by regulating that content deletion has to be conducted by electronic system organizers over the request of the related person based on court's decision. It not only makes the information hardly searched but also it may not be found since deletion has been conducted on its original sites.

Another difference is related to the basis of RTBF application. Applicants in EU have rights to ask for information deletion under the reasons that the information is *inadequate*, *irrelevant* or *no longer relevant* and *excessive* in its initial purpose is processed. However, in Indonesia, only based on the reason of irrelevant, a person can apply for RTBF request.

The difference of RTBF concept has brought up homework for Indonesia. Indonesia needs to immediately prepare Governmental Regulation to ensure the technical preparation of RTBF and to ensure individuals who may propose for the rights due to the potentials of certain parties which may propose it such as corruptors, malpractice perpetrators, pedophilia perpetrators, business fraud players - religious travel agencies. Furthermore, it needs to ensure what information sources can be proposed, especially related to the information published on newspaper. If other countries implement information deletion from newspaper, Indonesian needs to conduct careful measures to balance rights to obtain information and RTBF, as well as the importance of Press Council's involvement to ensure the information deletion.

Acknowledgments

This study was funded by the Ministry of Research, Technology and Higher Education of the Republic of Indonesia (Kemenristek-dikti RI). The views expressed are those of the authors and do not necessarily reflect the views of the Kemenristek-dikti RI.

References

Anggara. et.al. 2015. **Menyeimbang Hak Tantangan Perlindungan Privasi dan Menjamin Akses Keterbukaan Informasi dan Data di Indonesia**. Jakarta: Institute for Criminal Justice Reform.

Ball, J. 2014. **EU's right to be forgotten: Guardian articles have been hidden by google.** Retrieved from www.theguardian.com/commentisfree/2014/julk/02/eu-right-to-be-forgotten-guardian-google.

Brock, G. 2016. **The Right to be Forgotten.** London: I.B. Taurius.

Budhijanto, D. 2010. **Hukum Telekomunikasi, Penyiaran dan Teknologi Informasi: Regulasi dan Konvergensi.** Bandung: Refika Aditama,

Carbone, C. 2015. "To be on Not to be Forgotten: Balancing the Right to Know with the Right to Privacy in the Digital Age." **Virgina Journal of Social Policy & The Law** 22 (3): 526-560.

Djafar, W. and Veda, J. 2014. **Internet Untuk Semua: Mengintegrasikan Prinsip Hak Asasi Manusia dalam Pengaturan Internet di Indonesia**. Jakarta: Elsam.

Djafar, W., Sumigar, B., and Setianti, B. 2016. **Perlindungan Data Pribadi di Indonesia: Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia**. Jakarta: Elsam.

Google. 2018. **Government requests to remove content FAQs.** Retrieved from support.google.com/transparencyreport/answer/7347744?hl=en&ref_topic=7295796.

Isom, D. 2015. **Google Search and The Right to be Forgotten.** Master of Library and Information Science Thesis, University of California.

Jafar, W. 2013. **Kebijakan Kontrol Versus Kebebasan Berinternet: Pengantar singkat tentang perkembangan dan dinamika regulasi terkait internet dan hak asasi manusia di Indonesia, Malaysia dan Filipina.** Jakarta: Elsam.

Kampmark, B. 2015. "To Find or be Forgotten: Global Tensions on the Right to Erasure and Internet Governance." **Journal of Global Faultlines** 2 (2): 1-18.

Kantaatmadja, M. et.al. 2002. **Cyberlaw: Suatu Pengantar.** Bandung: Elips.

Koutnatzi, F. 2012. **The Right to be Forgotten in the Digital Era.** (A paper presented in the 5th International Conference on Information Law, Greece).

Makarim, E. 2005. **Pengatar Hukum Telematika: Suatu Kompilasi Kajian.** Jakarta: Raja Grafindo Persada.

Francis, L. and Francis, J. 2017. **Privacy: What Everyone Needs to Know.** Oxford: Oxford University Press.

Richards, N. 2016. **Intellectual Privacy: Rethinking Civil Liberties in the Digital Age**. Oxford: Oxford University Press.

Ritchie, D. 2009. "Is it possibleto define'privacies' within in law? Reflection on the 'securitisation' debate and the interception of communication." **International Review of Law, Computer & Technology** 23 (1-2): 25-34.

Santin, M. 2017. "The Problem of the Right to be Forgotten from the Perspective of self-regulation in journalism." **El Profesional de la Information** 26 (2): 303-310.

Schonberger, V. 2009. **Delete: The Virtue of Forgetting in the Digital Age.** New Jersey: Princeton University Press.

Taddeo, M. and Floridi, L. 2016. "The Debate on the Moral Responsibilities of Online Service Providers." **Science and Engineering Ethics Journal** 22 (6):1575-1603.

Tempo. 2016. **Tumpukan Perkara, MA: PN Jakarta Utara Berkinerja Rendah.** Retrieved from nasional.tempo.co/read/831574/tumpukan-perkara-ma-pn-jakarta-utara-berkinerja-rendah.

Urquhart, L. and Rodden, T. 2017. "New Direction in Information Technology law: Learning from Human-Computer Interaction." **International Review of Law, Computers & Technology** 31 (2): 450-466.

Weber, R. 2011. "The Right to be Forgotten: More than Pandora's Box ?." **Journal of Inellectual Property, Information Technology and E- Commerce Law** 2 (2): 120-130.