The Legal Frameworks of the Right to Request the Deletion of Personal Data in the EU, the U.S. and Japan and the Right to Be Forgotten: A Study Focusing on Search Businesses

Mika Nakashima

The Legal Frameworks of the Right to Request the Deletion of Personal Data in the EU, the U.S. and Japan and the Right to Be Forgotten: A Study Focusing on Search Businesses

Mika Nakashima[1] [0000-0002-4265-5414]

[1] Chuo University, Faculty of Global Informatics (Tokyo, Japan)
nakashima@tamacc.chuo-u.ac.jp

Abstract. The issue of the "right to be forgotten" presents a modern problem with regard to a person's right to request search engine providers for the deletion of search results generated by entry on his/her name. In recent years, legislation introducing the right to request the deletion of personal data has been taking place in the EU and the U.S. This paper reviews the legal frameworks with regard to the right to request the deletion of personal data in the EU, the U.S. and Japan and studies whether there is a right for a natural person to request the deletion of search results on him/her from search businesses (in other words, the "right to be forgotten") in each of these jurisdictions. In addition, the author examines the challenges of the Japanese legal system.

Keywords: GDPR, CCPA, APPI, Right of Deletion, Right to Be Forgotten

1 Introduction

Through the development of information technology, it has become possible to easily reproduce, preserve, and spread digitized information. On the other hand, digitized information is not expected to fade into obscurity; hence, once information related to an individual's privacy is made open to the public on the internet, it may not only create serious damage at the time of publication but also be harmful, being preserved in the internet space, for many years or possibly for good—a problem of "digital tattoo," so to speak. [34]

The issue of the "right to be forgotten" presents a modern problem in that it is centered around a person's right to request search engine providers for the deletion of search results generated by entry on his/her name. This is a novel issue, occurring as a result of the dramatic rise in access to information on the internet because of the spread of search services. Even if information exists on the internet, it would be highly difficult if not impossible practically to access such information without the assistance of a search engine.

In recent years, legislation introducing a person's right to request the deletion of personal data has been taking place in the EU and the U.S. This paper reviews the legal

frameworks in The EU, the U.S. and Japan with regard to the right to request the deletion of data and studies whether there is a right for a natural person to request the deletion of search results based on his/her name searches from search businesses (in other words, the "right to be forgotten") in each of these jurisdictions. In addition, the author would like to outline the present situation and issues concerning the topic in Japan.

Please note that while the General Data Protection Regulation (hereinafter referred to as "GDPR") uses the term "erasure," the California Consumer Privacy Act of 2018 (hereinafter referred to as "CCPA") and the Act on the Protection of Personal Information (hereinafter referred to as "APPI") uses the term "deletion" to mean the erasure of data. This paper basically uses the term "deletion" like the CCPA and the APPI, but, where it considers the GDPR, conforms to its terminology. Similarly, while the GDPR uses the term "personal data," the CCPA and the APPI use the term "personal information" to mean the information related to an individual. The APPI also uses the term "personal data" when the information is recorded in a "personal information database, etc." so as to be searchable. This paper basically uses "personal information" like the CCPA and the APPI, but where it considers the GDPR, conforms to its terminology.

2 The Legal Framework of Each Jurisdiction

2.1 The EU (GDPR)

On April 27, 2016, the EU adopted the "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation)". The GDPR came into force in member countries on May 25, 2018. Article 7 of the Charter of Fundamental Rights of the European Union, which was signed in 2000, establishes the "respect for private life and family life," and Article 8 thereof establishes the "protection of personal data[1]." Based on the Charter, the GDPR, in its preface, states that it respects the protection of personal data as a fundamental right of natural persons. It should be noted that the GDPR superseded the preexisting the "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (hereinafter referred to as "Directive").

The GDPR establishes the rights of data subjects and provides the "right to erasure (right to be forgotten)" in Article 17. Paragraph 1 of the Article states that the data subject shall have the right to request the controller the erasure of personal data where,

[1] For example, in the case of the European Court of Human Rights, Rotaru v. Romania, 4 May 2000, the applicant alleged a violation of his right to respect for his private life on account of the holding and use by the Romanian Intelligence Service of a file containing personal information and an infringement of his right of access to a court and his right to a remedy before a national authority that could rule on his application to have the file amended or destroyed. The ECHR concluded that both the storing of that information and the use of it, which were coupled with a refusal to allow the applicant an opportunity to refute it, amounted to interference with his right to respect for his private life as guaranteed by Article 8, Paragraph 1.

e.g., the personal data is no longer necessary for the original purposes, the data subject withdraws consent to or objects to the processing of personal data, or the personal data has been unlawfully processed. Paragraph 2 of the Article provides that where the controller has made the personal data public and is obliged to erase them under the Paragraph 1, the controller must take reasonable steps, including technical measures, to inform (other) controllers that are processing them that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. Paragraph 3 of the Article also provides that Paragraphs 1 and 2 shall not apply to the extent that processing is necessary for exercising the right of freedom of expression and information, 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, for reasons of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, for the establishment, exercise or defence of legal claims.

Considering that the European Court of Justice (hereinafter referred to as "ECJ"), in its preliminary ruling of May 13, 2014 (mentioned below) , acknowledged that under the Directive, a request for deletion could be made for search results based on name searches, that Article 17, Paragraph 2 of the GDPR specifically prescribes the erasure *"of any links to*, or copy or replication of, those personal data" (italicized by the author), and that the Directive was the predecessor and basis of the GDPR, it may safely be concluded that the GDPR contemplates the cases where under Article 17 search engine providers shall be obliged on the request of the data subject to erase the search results. [6, p.99] [18, p.156]

However, if we check the description of the GDPR's preface on the "right to be forgotten", we find that the main focus of the right to erasure is rather in cases where the data subject seeks the erasure of information posted on SNS that he/she used in his/her childhood, and not explicitly search services are mentioned.

Article 82, Paragraph 1 states that when a person has suffered material or non-material damage as a result of an infringement, he/she shall have the right to receive compensation from the controller or processor for the damage suffered. The liability for an infringement will not stop there, however. The following Article 83, Paragraph 5 prescribes administrative fines as a direct sanction, whereas Article 24 of the Directive would entrust the member states what sanctions to adopt. The fines imposed may run up to €20 million or up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

2.2 The State of California, the United States (CCPA)

In the U.S., federal law in relation to privacy and personal information protection is based on self-regulations in the private sector, and individual laws exist in specific

fields such as finance, medical treatment, and communication. However, there is no encompassing Data Protection Law at the federal level.[2]

The State of California enacted "California Consumer Privacy Act of 2018," and it went into effect on January 1, 2020. CCPA is the first comprehensive Personal Information Protection Law in the U.S. While the State of California is a global leader in the development of new information technologies and related industries, the California Constitution guarantees the right of privacy, and the State has enacted several privacy-related laws as concrete endeavors to protect privacy (for example, the "Online Erasure Law," which was enacted in 2013, grants minors the right of deletion of posts made by themselves on SNS and related platforms). The CCPA is also one of these concrete endeavors. It is incorporated to Part 4 of Division 3 of the Civil Code as "Title 1.81.5 California Consumer Privacy Act of 2018 [1798.100—1798.199]". Global companies must comply with the CCPA. While they have already been preoccupied with responding to the GDPR, they are pressed to respond to the differences between the GDPR and the CCPA.

The CCPA is thought to have been influenced by the preceding GDPR; there are several similarities in the two acts. For example, the Section 1798.100(d) of the CCPA which defines the business's obligation to consumers to disclose and provide personal information establishes "if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity". This is similar to the right to data portability of Article 20, Paragraph 1 of the GDPR which establishes "the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided". Section 1798.105 states that "(a) The section provides that a consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer," and, "(c) a business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any 'service providers' to delete the consumer's personal information from their records." However, it is not clear as to the kind of situations this section anticipates, and it is also not clear whether deletions must be made by search businesses.

The CCPA provides statutory damages in the case of lawsuits brought by individual consumers and class action lawsuits (Section 1798.150). Furthermore, the CCPA establishes a civil penalty system enforced by the California Attorney General (Section 1798.155). Statutory damages are available, and in those cases, either damages of between $100 and $750 are available for each consumer per incident of infringement, or the consumer may recover actual damages, whichever amount is larger. Hence, it is possible for the consumer to institute a civil action (however, the framework of the

[2] On the other hand, the Federal Trade Commission (FTC) of the U.S. has operating authority based on the Federal Trade Commission Act of 1914 from the position of consumer protection. [11, p.408]

statutory damages system seems to fundamentally assume cases of data breach). Regarding the civil penalty, violators may be liable for a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation.

2.3 Japan (Civil Code and APPI)

The legal framework of personal information protection in Japan is based on the right of privacy and the APPI.

The right to privacy has been formulated by case law over the past half century under Article 709 of the Civil Code. The Article states "A person who has intentionally or negligently violated any right of others… shall be liable to compensate any damages resulting in consequence" (the omitted part indicated with "…" is a phrase inserted in a recent amendment of the Code) . The right of privacy came to be counted as a "right" protected under the Article. In 1964 the Tokyo District Court explicated the right of privacy as the legal basis of its decision in the case of the novelist Yukio Mishima's roman-à-clef, *After the Banquet*. [1] In 1994 the Supreme Court acknowledged the "legal interest as not to have facts related to criminal records, etc. made public" in the case of a non-fiction book, *Reversal*. [21] Since then, more Supreme Court cases have followed, some with explicitly mentioning "privacy," and it can now be said that the right of privacy is part of law in Japan.

Although Article 709 the Civil Code only prescribes monetary compensation as its remedy, an order of injunction has now been established in lieu of or in addition to damages through case law. In a case of 2002, the Supreme Court upheld the decision of the High Court which ordered an injunction against publication of a roman-à-clef, which is regarded as the precedent for the availability of injunction based on the right of privacy[3].

The APPI was promulgated on May 30, 2003, and enforced on April 1, 2005. It is an administrative law that establishes rules related to the proper handling of personal information. On the basis of the Act, the Personal Information Protection Commission (hereinafter referred to as "PPC"), was established as an administrative organization, independently enforcing its authority. The APPI fulfills preventive functions against the improper handlings of a person's personal information but it does not directly provide him/her private remedies. [9, p.3]

A decade passed and, given the need to prepare for an environment wherein proper utilization and application of big data—including personal data—are to be made more readily possible and in view of responses to the globalization of business activities, the amendment to the Act was promulgated on September 9, 2015, and enforced on May 30, 2017. [28] Furthermore, in accordance with the "revision in every 3 years" provision of the amended law (Article 12 of the supplementary provisions), the Act for Partial Amendment of the APPI (Act No. 44 of 2020) was enacted on June 5, 2020. It was passed and promulgated on June 12 of the same year. The following is based on the latest amended APPI, 2020 (not yet in force at the time of writing).

---

[3] "*Fish that swim in rocks*" Case, Decision of the Supreme Court on September 24, 2002, Hanrei-jiho, No. 1802, p. 60.

The APPI establishes the data subject's rights to request with regard to the disclosure of information about him/herself (Article 28) and the correction, etc. (Article 29) and the utilization cease, etc. (Article 30) of the retained personal data. A framework that allows the involvement of the data subject in certain cases is established. In relation to the deletion of personal data, apart from Article 19, which requires the personal information handling business operator to make reasonable efforts to delete the personal data that has become unnecessary, Article 29 establishes the right to request a deletion. It provides that the principal may, when the contents of retained personal data that can identify the principal are not true to the facts, request the business operator to make a correction, addition or *deletion* (hereinafter referred to as "correction, etc.") in regard to the contents of the retained personal data. With this regulation, however, it should be noted that even though the word "deletion" is used here, its nature is not that of the right to request the complete erasure of data by the business but is no more than being a method of "correction." [9, pp.312-316] [10, pp.238-244] [14, pp.214-218]

Article 30, Paragraph 1 stipulates that a principal may, when the retained personal data that can identify the principal is being handled in violation of the provisions of Article 16 or has been acquired or used in violation of the provisions of Articles 17 and 16-2, demand of a personal information handling business operator a utilization cease or deletion of the retained personal data. In addition, a new clause has been added to the Act to prescribe that a principal may do the same where there is a possibility that his/her rights or legitimate interests are harmed (Article 30, Paragraph 5). Prior to the Amendment, utilization cease, etc. was a remedy limited to cases where personal information was used for purposes other than those for which it was intended or acquired inappropriately (inappropriate use has been added in the Amendment 2020),[13] but it is extended to cases where there is a possibility that his/her rights or legitimate interests are harmed, which is noteworthy as it eases the requirements for requesting the erasure of personal data. [33]

The "personal information handling business operator" defined in Article 2, Paragraph 5 of the Act are those who use a "personal information database etc." for business. Thus whether or not a search businesses is a personal information handling business operator as defined, depends on the meaning of Paragraph 4 of the same Article which states the definition of a "personal information database etc." . Looking into the discussion of the Bill for the Act in 2003, the opinion of the government introducing the Bill was such that the databases of search businesses would not fall under "personal information database etc." [31] [32] Presumably it is what has been accepted in academia. [10, pp.79-80] [14, p.72] The main reasons for it are that the databases of search businesses are mixed with information other than personal information, that searching for information other than personal information, such as place names, is possible, and that no attached index is available as personal information. Opposing views have also been asserted, with their reasoning being the following: that even when information other than personal information can be searched for, it will not be an obstruction for it to fall under "those systematically organized so as to be able to search for particular personal information using a computer" of Item 1 of Paragraph 4 of Article 2, that a keyword search performed on a specific person's name on the search service is based on the index that the search business has created, and that an expansive use of search

services in order to get a person's personal information is actually made. It may also be noted that at the time the Bill was introduced in 2003, search services were not as widespread as they are today. [9, pp.312-316] [4]

The APPI establishes criminal penalties. Imprisonment for not more than six months or a fine of not more than ¥ 300,000 is the penalty when the orders under the current APPI related to utilization cease, etc. have been infringed (Article 84 of the current Act). The amended Act, 2020 raises the statutory penalties for violations of the PPC's orders, false reports to the PPC, and other offenses. For violations of the PPC's order, the penalty is increased from the said above to "imprisonment for not more than one year or a fine of not more than ¥ 1 million" (Article 83). As for false reports, the penalty is raised from "a fine of not more than ¥ 300,000" to "a fine of not more than ¥ 500,000" (Article 85). As for the illegal provision of databases and the violations of the PPC's orders, the violating corporation (or natural person running the business) may be punished with a fine. In case of violations of the PPC's orders the maximum fine for a corporation is increased hugely to not more than ¥ 1 billion (from ¥ 300,000 under the current Act), taking into account the disparity in financial resources between a corporation and an actor (Article 87).

3 Judicial Precedents in Each Jurisdiction

3.1 The EU - The Preliminary Ruling of the ECJ in the González Case of May 13, 2014

On May 13, 2014 the ECJ delivered the preliminary ruling in Google Spain v. González, which is now credited as the first judicial precedent acknowledging a person's "right to be forgotten" as meaning the right to request the deletion of search results on his/her name searches. The ECJ held in summary as follows:

> The operator is, in certain circumstances, obliged to remove links to web pages that are published by third parties and contain information relating to a person from the list of results displayed following a search made on the basis of that person's name. When the data subject requests that links to web pages be removed from such a list of results on the grounds that he wishes the information appearing on those pages relating to him personally to be 'forgotten' after a certain time, and if it is found that the inclusion of those links in the list is, at this point in time, incompatible with the Directive, the links and information in the list of results must be erased.
>
> In this case, if one were to consider the sensitivity of information as far as the private life of the data subject was concerned and the fact that that information was first made public 16 years ago, then the information in question should no longer be linked to the name of the data subject through that list of search results,

[4] The search service of Google Inc., "Google," appeared at around 1998, and its Japanese version appeared at around 2000.

> and it is allowed for the data subject to make such a request directly to the search business. [5] [15]

The ruling was delivered in response to a request from Audiencia Nacional Spain concerning the interpretations of Articles of the Directive. Although the Directive was repealed and the GDPR superseded it, the latter provides “Right to erasure (‘right to be forgotten’)” as Article 17. Because it can be said that the data subject's right to request the deletion of search results based on his/her name searches is, practically speaking, the core concept of “right to be forgotten”, the González case will be taken to be a leading precedent pertinent to interpreting Articles of the GDPR.

3.2 The U.S.

Presently, no direct judicial precedents in the U.S. acknowledge the “right to be forgotten” as a right to request deletion from search services. In fact, the discussions in the U.S. are centered around the issue of whether to limit the liability of search businesses as providers. [19][5] Article 230 (c) (1) of the Communications Decency Act provides immunity from tortious liability for providers and users of an interactive computer service who publish information provided by third-party users. Reportedly the courts have in years been stretching the meaning of "interactive computer service" to immunize web hosts, websites, search engines, and content creators although no cases of search engines are cited therewith. [22, p.371]

3.3 Japan - The Supreme Court Ruling on January 31, 2017

In and around when the EUJ ruling in González case was reported, applications for provisional injunction or actions on the merits, seeking the deletion of search results, began to be brought before the lower courts. Some of those cases were reported by news media with referring to the EUJ's ruling. [18] One of those application cases went up in judicial ladder of appeals and, on January 31, 2017, The Supreme Court delivered its first-ever judgment on the topic matter. The Court decided, in summary, as follows: [3] [16]

> The interests of not having facts of one's privacy made public unless one gives permission” should be protected by law as this Court has held repeatedly. As search programs are created in such a way that search engines collect information on the internet which aligns itself with their programing policies, providing search results generated by the search engine is an “act of expression” by the search engine provider itself. Also as the provision of search results generated by search engine fulfills a major role as the foundation of information distribution on the internet in modern society, facilitating the public to publish information

[5] See [26] [23] [8] for details on the state of debate in the U.S.

> on the internet or get information they need from the vast quantities of information on the internet, to hold a search engine provider liable for providing a certain search result and obliged to delete it would constitute a restriction of this role, as well as a restriction of the act of expression.
>
> In the light of the nature and the functions of the search engine providers said above, whether a provider should be made liable for providing search results, in response to a search request on one person, with URLs to the articles on the internet which contain facts of that person's privacy should be decided on balancing of interests, taking into consideration the circumstances for the legal interest of not having the said facts made public, such as the nature and content of the said facts, the range of transmission enabled and the level of actual damage that person has suffered by way of the said URLs provided, the social status and influence of that person, the content and purpose of the said article, the social situations of the time and afterward it was published on the internet, and the necessity of publishing the said facts in it, and also the circumstances in respect of reasons for providing the URLs in the search results. One may request the search engine provider to delete the said URLs from the search result if on balancing the legal interest of not having the said facts made public is *clearly* superior to the other interest (italicized by the author).
>
> In this case, the fact that the appellant was arrested for child prostitution is a fact of privacy that he would not want to be known by others without permission, but in light of child prostitution being a subject of strong social reproach and banned with penalties, it still remains a matter related to the interests of the public. Even upon considering the circumstances, such as the appellant not having committed a crime for a certain period of time since then, it cannot be said that the legal interest of not having the facts of his arrest made public is superior. The ruling of the High Court (the appellate court) to turn down the appellant's application is correct.

In the first instance of this case the court referred to “the right to be forgotten” when it approved the order of deleting search result. The High Court (in the appellate instance) repudiated the introduction of the concept, annulling the order. Expectations were raised that the Supreme Court would possibly give some words of approval or disapproval on it but nothing was referred to. It may be safe for now, therefore, to say that the concept of “the right to be forgotten” has not been settled judicially in Japan.

4 The Present Situation of the Legal Framework in Japan and the Future

In relation to the “right to be forgotten” as a right to request deletion from search services, assessing the present situation of the legal system in Japan leads to the following.

Whereas the right of privacy and the injunction order as a remedy for its infringement have well been established through case law under the Article 709 of the Civil Code, the right to be forgotten has yet to be acknowledged judicially.

Article 30, Section 5 of the amended APPI, 2020 provides that a person may request the utilization cease or deletion of the retained personal data "where there is a possibility that his/her rights or legitimate interests are harmed". If a search business operator is to be construed as a "personal information handling business operator" under the Act (Article 2, Paragraph 5), this newly established provision may serve as a ground for requesting the deletion of search results when the amended Act comes into force.

Since the government opinion at the time of the introduction of the Bill, as shown above (p.7), it has been a common understanding that the APPI does not assume the databases of search businesses to be the "personal information database etc." and, accordingly, that the search businesses do not fall under the "personal information handling business operator." Considering the rapid prevalence of search services since then, [6] however, we face an untraversed situation in which information of a diverse nature regarding any person, whether most famous or unknown, can be searched by merely making a name search of the individual on the internet. There is room for Japan to reconsider the way in which she think about the legal nature of search businesses. [7]

The APPI does not only establish the obligations of businesses as of administrative level but also acknowledges the rights of a data subject to request utilization cease, etc. in certain cases. However, it merely acknowledges the involvement of data subjects within the prescribed aims. The GDPR, grounded on fundamental human rights, gives strong "personal data protection" and guarantees the "right to erasure (the right to be forgotten)," whereas the CCPA, based on the "right of privacy" of the Constitution, guarantees a consumer the "right to request that a business delete any personal information about the consumer which the business has collected from the consumer". In contrast with them, Japan's APPI does not directly establish the rights of the individual and an actor committing an infringement of an obligation under the Act is punished with imprisonment and/or fines (a committing corporation also suffers the latter sanction in certain cases) but is not rendered liable to an aggrieved person for damages, unlike the GDPR and the CCPA, which provide for a data subject's or consumer's right to claim damages. Admitting in the APPI the right to request deletion of search results (whether through further amendments to the Act or through interpretation of the Act) would be incompatible with the legislative intent of the Act. The legal framework of the right to request deletion has no choice but to depend on the right of privacy as the right to request under private law; this is the situation at present.

Regarding whether the right to request deletion from search businesses is acknowledged as the right of privacy, according to the aforementioned Supreme Court decision,

---

[6] On July 27th, 2010, Yahoo Japan Corporation gathered attention when it used the search engine of Google Inc., as the back engine of "Yahoo! JAPAN." See [25] for the market share of search engines in Japan.

[7] On December 13th, 2019, the PPC made public an outline of system amendment in reviewing the APPI every 3 years. [33] This outline holds up the easing of the requirements of "deletion," but it is unclear whether debates have been carried out in relation to the right of deletion and the "right to be forgotten" that has search businesses as the subject. Furthermore, according to the written report gathered together by workshop under the Ministry of Internal Affairs and Communications after the first decision of the ECJ mentioned below was given, the issue of the deletion of search results carried out by search businesses has the premise of fundamentally entrusting to the self-regulation of the businesses and carrying out inspections within the legal framework related to the existing the right of privacy. [17]

the possibility of acknowledging the request of deletion is left open in the case where search results should "clearly" be deleted upon comparison with the "act of expression" of the search business (n.b., which reasoning is an obiter dictum because the application for an order of deletion in the case was not approved). In relation to the requirement of "clear"-ness, it is hoped that further judicial cases will help clarify its meaning [8] as well as academic discussion should be made on it, in which the peculiar characteristics of search businesses—such as only providing a list of search results, being unable to know details with regard to the information on the original website that the links displayed in the search results lead to (they are not in a position to determine the veracity of the information published on the original website), and being able to actively continue to display a person's past privacy information through search results based on his/her names— should be considered to determine when and how the new media of search business should be obliged to delete a person's privacy information on his/her request.

References

1. "*After the Banquet*" Case (1964), Decision of the Tokyo District Court on September 28, 1964, Hanreijiho, No.385, p. 12.
2. California Consumer Privacy Act of 2018, 1.81.5. CIVIL CODE §§1798.100 - 1798.199 (2018). http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=
3. Deletion of Posted Articles Case (2017), Decision of the Supreme Court on January 31, 2017, 2016 (Appeal by Permission Case) No. 45, Order of Provisional Injunction of Deletion of Posted Articles and Appeal Rejected, Minshu, Vol. 71, No. 1, p. 63; Hanreijiho, No. 2328, p. 10; Hanrei Times, No. 1434, p. 48.
4. DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en
5. González Case (2014), 131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González (2014). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&form=EN
6. Hiroshi Miyashita (2018), The General Data Protection Regulation, Keiso Shobo.
7. Hiroshi Miyashita (2015), The Restoration of The Right of Privacy – The Clash of Freedom and Dignity, Chuo University Press.
8. Hiroshi Miyashita (2016), *The Right to be Forgotten and the Legal Liability of Search Engines,* Comparative Law Journal, Vol. 50, No. 1, p. 35.
9. Hisamichi Okamura (2017), The Act on the Protection of Personal Information 3rd Edition, Shojihomu.

[8] On December 12, 2019, in a case requesting deletion of search results (decision on the merits), where a man requested the deletion of search results from Google LLC, the Sapporo District Court stated that the interests of not making it public are superior to that of maintaining of the display and gave a decision of ordering deletion (Westlaw. JAPAN, reference number：2019WLJPCA 12126001).

Furthermore, for the tendencies inside and outside the country before the aforementioned decision of the Supreme Court, see [35]. The summary of domestic developments since the Supreme Court decision, see [24].

10. Itsuo Sonobe and Shizuo Fujiwara (Editor) (2018), Explanation of the Personal Information Protection Law <Second Revised Edition>, Gyosei.
11. Kaori Ishii (2017), New Edition: The Present and Future of the Personal Information Protection Law – Global Trends and the Future Image of Japan, Keiso Shobo.
12. Kaori Ishii (2018), *Supreme Court Decision in Google Search Results Removal Request Case*, Hanreijiho, No.2353, p. 148.
13. Kaori Ishii (2019), *Legislation of the so-called 'Right to be Forgotten': Outline of Interim Arrangements for Revisions to the Personal Information Protection Law*, Business Law, Vol. 19, No.8, p. 82.
14. Katsuya Uga (2018), Article by Article Explanation of the Act on the Protection of Personal Information – Act on the Protection of Personal Information, Act on the Protection of Personal Information Held by Administrative Organs, Act on the Protection of Personal Information Retained by Independent Administrative Institutions 6th Edition, Yuhikaku.
15. Mika Nakashima (2016), *Search Services and the Right to be Forgotten – On the Preliminary Ruling of the European Court of Justice in the Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González Incident (May 13, 2014)*, Legal Practices of Information Networks, Daiichi Hoki.
16. Mika Nakashima (2019), *The Deletion of Search Results and the Right to be Forgotten: Regarding the State of the Debate of Theories, Starting from the Supreme Court decision of January 31, 2017*, Tokai Law Review, No. 56, p. 117. https://www.u-tokai.ac.jp/academics/undergraduate/law/kiyou/pdf/2019_56/07.pdf
17. Ministry of Internal Affairs and Communications (2015), *Regarding Responses Towards t he Distribution of Personal Information, User Information, Etc., on the internet: Written R eport by ICT Service Safety and Security Research Society*. http://www.soumu.go.jp/main_content/000369245.pdf
18. Paul Voigt and Axel von dem Bussche (2017), The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer.
19. Parker v. Google, Inc., 422 F. Supp. 2d 492 (2006).
20. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504
21. "*Reversal*" Case (1994), Decision of the Supreme Court on February 8, 1994, Minshu, Vol. 48, No. 2, p. 149.
22. Rustad and Koenig (2005), *Rebooting Cybertort Law*, Washington Law Review, Vol. 80, p. 355.
23. Satoshi Narihara (2015), *The State of Debate in Japan, the U.S. and The EU Surrounding the "Right to be Forgotten,"* Administration & Information System, Vol. 51, No. 6, p. 54.
24. Satoshi Narihara (2020), *"Freedom of Expression and Moral Rights Regarding Search Engines" - A Review of the Supreme Court Decision in 2017 and Case Studies on the Deletion of Search Results since that Decision* - , Journal of Law and Information System, No. 7, p.47.
25. StatCounter GlobalStats, *Search Engine Market Share Japan* (Jan 2009 - Nov 2019). https://gs.statcounter.com/search-engine-market-share/all/japan/#monthly-200901-201911
26. Taro Komukai (2015), *"The Right to be Forgotten" and the U.S. Communications Decency Act*, Information Processing Society of Japan Research Report Vol. 2015-EIP-69 No.15. https://ipsj.ixsq.nii.ac.jp/ej/?action=repository_uri&item_id=144945&file_id=1&file_no=1
27. Taro Komukai and Kaori Ishii (2019), Outline: The GDPR, NTT Publishing.

28. The amended Act on the Protection of Personal Information (enforced on May 30, 2017). https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf
29. The Communications Decency Act (CDA), 47 U.S.C. Article 230 (1996).
30. The General Affairs Agency Administrative Management Bureau (Supervision) (1991), Article by Article Explanation of the Act on the Protection of Personal Information, Newly-Revised Edition, DaiichiHoki, Publishing.
31. The House of Councillors (2003), *Special Committee Related to the Protection of Personal Information*, Record of Proceedings on May 13, 2003 (No. 3), Answers by Akio Fujii as Government Witness. http://kokkai.ndl.go.jp/SENTAKU/sangiin/156/0071/15605130071003.pdf
32. The House of Representatives (2003), *Special Committee Related to the Protection of Personal Information*, Record of Proceedings on April 18, 2003 (No. 6), Answers by Minister of State, Hiroyuki Hosoda. http://kokkai.ndl.go.jp/SENTAKU/syugiin/156/0017/15604180017006.pdf
33. The Personal Information Protection Commission (2019), *The Act on the Protection of Personal Information : Revision in Every 3 Years – Outline of Framework Amendment*. https://www.ppc.go.jp/files/pdf/seidokaiseitaiko.pdf
34. Viktor Mayer-Schönberger (2011), Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press; Revised.
35. Yoshimichi Okuda (Editor) (2015), Internet Society and the Right to be Forgotten – Court Cases of Deleting Personal Data and their Legal Principles, Gendaijinbunsha.