The Impact of the Right to be Forgotten on Information Archiving and Access in Libraries and Archives: Postprint

Authors: Lian Zhiying

Date: 2023-04-01T16:02:54+00:00

Abstract

[目的/意义] Understanding the impact of the right to be forgotten on information archiving and access in libraries and archives is of significant importance for memory institutions to undertake memory preservation efforts and to balance public interest with individual rights protection during the processes of memory preservation and access provision. [方法/过程] Through methods including case analysis and legal and policy text analysis, this study examines the content of the right to be forgotten and its influence on information archiving and access in libraries and archives, and offers insights and recommendations. [结果/结论] The establishment and protection of the right to be forgotten will not impede information archiving in libraries and archives, but may lead to certain archived personal information being unavailable or having restricted access. When archiving information, libraries and archives must adhere to the principles of data minimization and ensuring archived information integrity. Additionally, they need to establish and refine a comprehensive review mechanism throughout the entire process, including review mechanisms for information provision and access, information removal, and restoration of access to removed information. When necessary, personal information may also be pseudonymized to strive for a balance between the right to be forgotten and public interest.

Full Text

The Impact of the Right to be Forgotten on Information Archiving and Access in Libraries and Archives

Lian Zhiying School of Information Resource Management, Renmin University of China, Beijing 100872

Abstract

[**Purpose/Significance**] Understanding the impact of the right to be forgotten on information archiving and access in libraries and archives is significant for memory institutions to conduct memory preservation work and to balance public interest with individual rights protection in the processes of memory preservation and provision. [**Method/Process**] Through case analysis, legal and policy text analysis, and other methods, this study examines the content of the right to be forgotten and its impact on information archiving and access in libraries and archives, and proposes implications and recommendations. [**Result/Conclusion**] The establishment and protection of the right to be forgotten will not hinder information archiving in libraries and archives, but may result in certain archived personal information being unavailable or restricted from access. When archiving information, libraries and archives need to adhere to the principles of data minimization and ensuring information integrity, while also establishing and improving a whole-process review mechanism, including mechanisms for reviewing information provision and access, information removal, and restoration of access to removed information. When necessary, personal information may also be pseudonymized to achieve a balance between the right to be forgotten and public interest.

Keywords: right to be forgotten; right to erasure; right to delisting; information take-down policy

The "right to be forgotten" has been recognized, legislated, and implemented in several regions and countries worldwide, including the European Union, Argentina, and California in the United States. The establishment of this right in these regions and countries may directly or indirectly influence the formulation of relevant laws in other areas. Since the right to be forgotten involves the tension between memory and forgetting, libraries and archives as memory institutions will inevitably be affected by this right, drawing significant attention from the library and archival communities. In February 2016, the International Federation of Library Associations and Institutions (IFLA) issued a "Statement on the Right to be Forgotten," noting that the purpose of this right is not to destroy information or completely remove it from the internet, but rather to make published information difficult to find, which can damage name-based retrieval and undermine the rights to freedom of information access and freedom of expression. The statement also acknowledges that IFLA recognizes the necessity of protecting personal privacy, trade secrets, and government information security, provided this does not conflict with the public interest. Libraries and their staff believe that the acceptability of a particular right to be forgotten application depends on its specific circumstances, and IFLA calls on its members to participate in policy discussions regarding the right to be forgotten, supporting both individual privacy rights and helping users find needed information [1]. However, the statement equates the right to be forgotten with the right to delisting.

The theme of the 19th International Congress on Archives (ICA Congress) was also the right to be forgotten, with the organizing committee believing that this right is closely related to trust and evidence [2]. What impact does the right to be forgotten have on memory institutions such as libraries and archives, and how should the library and archival communities respond to these impacts? These are questions that our profession needs to consider and constitute the main research questions of this paper.

Current research in foreign libraries and archives on the right to be forgotten primarily focuses on its impact on memory preservation and information access. Even before the implementation of the EU's General Data Protection Regulation (GDPR) in 2016, the 2014 Google Spain case had already triggered debates about whether the establishment of the right to be forgotten would create memory holes or lead to the rewriting of history. For instance, then-Executive Director of Wikipedia L. Tretikov pointed out that the court's decision would weaken the world's ability to freely access accurate and verified documents about individuals and events, leading to the creation of memory holes [3]. A. De Baets also claimed that only in cases involving children would it be legitimate to delete previously online information about these children, or to anonymize outdated judgments. An overly broad right to be forgotten would lead to the rewriting of history [4]. Some scholars have expressed concerns about the impact of the right to be forgotten on libraries and archives' preservation of social memory, such as P. Henttonen, who noted that the right to be forgotten means an individual can choose to exclude themselves from collective or social memory, and that the concept of the right to be forgotten contradicts the principle of long-term information preservation [5].

However, M. D. de Rosnay and A. Guadamuz, based on in-depth analysis of the 2014 Google Spain case and the controversies it triggered, argued that given the limitations on the application of the right to be forgotten, this right would not affect the preservation of digital heritage or web archiving, and that archives need not worry [6]. S. Wyber analyzed IFLA's 2016 "Statement on the Right to be Forgotten," pointing out that while the right to be forgotten would make public name-based information retrieval difficult, Article 17(3)(d) of GDPR exempts library archiving based on public interest from deletion requests. However, what the provisions "(the right to erasure) makes archiving impossible" and "(the right to erasure) seriously impairs the archiving purpose" mean in practice remains worthy of further study [7]. Chinese scholars have also argued that although the right to be forgotten imposes certain restrictions on web information archiving, it does not completely hinder it, and have proposed establishing a "privacy by design" principle and developing "right to be forgotten review standards" to ensure the protection of personal information during web archiving [8]. However, these authors have not elaborated on what specific restrictions the right to be forgotten imposes on web information archiving.

Additionally, V. Dressler and C. Kristof believe that the right to be forgotten will eventually be established in the United States. They surveyed 23 libraries

of the Association of Research Libraries regarding their handling of information removal requests (take-down requests) and found that digital librarians had no clear answers or established practices for such requests, with responses often depending on individual librarians and reflecting only personal opinions. They argue that libraries should discuss this issue among themselves [9].

Overall, research on the impact of the right to be forgotten on memory institutions such as libraries and archives is limited both domestically and internationally. Moreover, existing studies have not clearly elaborated on the content of the right to be forgotten and have not closely examined its impact on libraries and archives in conjunction with the specific content of this right, nor have they proposed corresponding response strategies. Based on relevant legal provisions and cases, this paper analyzes the content of the right to be forgotten, emphasizing that this right essentially includes the right to erasure and the right to delisting (or right to de-referencing). It then examines the impact of the right to be forgotten on information archiving and access in libraries and archives through analysis of relevant concepts, legal provisions, cases, and the information take-down policies of institutions such as the British Library, The National Archives (UK), the National Library of Wales, and the National Archives of Scotland.

2. Content of the Right to be Forgotten

Based on existing national and regional regulations on the right to be forgotten and the 2014 Google Spain case judgment, the right to be forgotten essentially includes two aspects: the right to erasure and the right to delisting.

2.1 Right to Erasure

The right to erasure means that data subjects have the right to require data controllers to adopt effective technical measures to delete their personal data under statutory circumstances. For example, Article 17(1) of the 2016 GDPR explicitly stipulates the circumstances under which data subjects have the right to require data controllers to delete their personal data: (1) when personal data is no longer necessary for the purposes for which it was collected or processed; (2) when the data subject withdraws consent under Article 6(1)(a) or Article 9(2)(a) and there is no other legal basis for processing; (3) when the data subject objects to processing under Article 21(1) and there are no overriding legitimate grounds for processing, or when the data subject objects under Article 21(2); (4) when personal data has been unlawfully processed; (5) when personal data must be deleted to comply with legal obligations under EU or Member State law; and (6) when personal data has been collected in relation to the provision of information society services referred to in Article 8(1). Section 1798.105 of California's 2018 Consumer Privacy Act stipulates that consumers (data subjects) have the right to require businesses (data controllers) to delete personal information collected from them, and businesses must delete such information upon receiving a verifiable request from consumers.

The right to personal information erasure is an important component of personal data autonomy and self-determination [10]. Data subjects have autonomy over their personal data—they can consent to data controllers collecting and processing their data based on mutually agreed terms, and they can also legally withdraw consent and require data controllers to delete their data. The right to personal information erasure is not an entirely new right. G. Zanfir points out that Germany's 1977 Data Protection Act, France's 1978 Data Protection Law, the UK's 1984 Data Protection Act, and the Netherlands' 1989 Data Protection Act all stipulated the right to delete personal information or data [11].

2.2 Right to Delisting

Based on the 2014 Google Spain case judgment, the right to be forgotten also includes the right to delisting. If sensitive information about a data subject is deemed inappropriate, irrelevant, or excessive, the data subject can require search engine companies to remove links to such sensitive information from search results when searching using their name. The right to delisting grants data subjects the right to restrict and terminate the dissemination of personal data they believe is detrimental to their interests. However, the exercise of this right is subject to several conditions: (1) it only applies to searches directly using the data subject's name—relevant information may still appear in search results when using other search terms; (2) according to the September 2019 judgment in Google v. CNIL [12], the right to delisting only applies to searches conducted within the data subject's geographic region and does not apply to searches in other global regions; and (3) this information will only be removed from search engine results—the information may continue to exist on the website of the original publishing institution unless that institution is obligated to delete the information.

In summary, the right to be forgotten concerns personal information autonomy, personal privacy, and personal reputation. It is a fundamental human right whose establishment and protection aim not to allow an individual to rewrite their past or erase unpleasant traces, but primarily to protect individuals' autonomy over their information and to protect citizens from interference by inappropriate, irrelevant, and excessive personal information.

Given that the right to be forgotten mainly includes the above two aspects, its impact on libraries and archives is also manifested in two areas: (1) information archiving—whether the right to erasure will prevent certain valuable personal information from being archived and preserved; and (2) information access—whether the right to delisting will prevent certain personal information in library and archive retrieval systems from being accessed.

3. Impact of the Right to be Forgotten on Information Archiving in Libraries and Archives

The author argues that based on theoretical analysis of the concept of "archiving," existing legal provisions, and relevant judicial cases, the establishment of the right to be forgotten will not hinder information archiving in libraries and archives. That is, it will not prevent valuable personal information from being archived and preserved, thereby creating memory holes.

3.1 Conceptual Analysis of "Archiving"

Archiving refers to the process of preserving information that has been appraised as having permanent value. From the perspective of archiving scope, not all information is worth or necessary to archive. For instance, archival institutions establish appraisal standards and policies that clearly define the scope of documents to be archived. Therefore, the archiving process itself involves memory and forgetting. Although technological developments have led some to propose archiving all information, this view is currently unrealistic and difficult to implement. For example, when the Library of Congress launched its Twitter archiving project in 2010, it announced that it would collect all historical records on Twitter. However, in 2017, the Library of Congress announced that beginning in January 2018, it would no longer collect all publicly posted tweets on Twitter, but would selectively preserve tweets based on themes and events. This was because the explosive growth of information on Twitter in recent years had overwhelmed storage servers, and the Library of Congress lacked sufficient project management capacity and planning to preserve all Twitter posts [13]. Therefore, archiving itself involves forgetting, and what libraries and archives as memory institutions can preserve is only a portion of all social memory.

When archiving information, libraries and archives have always strived to balance the relationship between public interest and individual rights protection. Even before the right to be forgotten was proposed, private website administrators had requested that libraries and archives delete collected web pages based on privacy, copyright protection, or because the information involved defamation or embarrassment. In 2002, representatives from the Electronic Frontier Foundation, the "Chilling Effects" project, the Council on Library and Information Resources, the Berkeley Law School, and other commercial and non-commercial organizations mentioned at a meeting hosted by the "Archiving Policy Special Interest Group" (an informal group of people interested in digital archiving practices) that requesters could add or modify robots.txt documents on their websites to ensure their web pages would not be collected. The Internet Archive (IA) uses this method, informing website owners that they can add robots.txt documents to prevent IA's crawlers from capturing their web pages [14]. Therefore, balancing public interest and individual rights protection has always been a consideration for libraries and archives as memory institutions when preserving social memory. Whether in the paper era or the digital era, for the purpose of protecting individual rights, abandoning the archiving of certain personal in-

formation has been a consistent practice of libraries and archives as memory institutions.

3.2 Existing Legal Provisions

Existing laws protect data subjects' right to be forgotten while striving to balance this protection with the maintenance of public interest. For example, Article 17(3)(d) of GDPR explicitly stipulates that the right to erasure does not apply to archiving for purposes of public interest, scientific or historical research, or statistical purposes under Article 89(1). As public institutions, libraries and archives generally conduct information archiving based on public interest or for scientific and historical research purposes. Therefore, the law protects and encourages libraries and archives to archive valuable personal information for public interest, which is precisely why many libraries and archives, such as the Library of Congress and the British Library, can undertake projects to archive massive amounts of digital information like Twitter tweets and Facebook posts.

However, according to Article 89(1) of GDPR, when archiving personal information, libraries and archives should also appropriately protect data subjects' rights and freedoms by adopting technical and organizational measures to ensure respect for the principle of data minimization (i.e., personal data must be adequate, relevant, and limited to what is necessary for the purposes of processing). Pseudonymization measures should also be adopted when pseudonymization does not affect the archiving purpose. Therefore, libraries and archives can collect and preserve personal information for public interest purposes, but they must also fully respect information subjects' rights. This is consistent with the practice of recommending private website owners use robots.txt documents to refuse capture and preservation of their web pages, and it is also a professional ethic that libraries and archives must observe when archiving personal information.

3.3 Relevant Judicial Cases

Existing judicial cases demonstrate that courts support and protect the archiving of personal data or information for public interest purposes and will not easily order the deletion of archived personal information from archival databases. This paper lists three relevant cases for illustration:

3.3.1 Case 1: Luzac v. De Volkskrant [15] In 2010, E. Luzac, the founder of a well-known Dutch private school chain, sued the Dutch newspaper De Volkskrant, demanding the deletion of several news articles involving him from the newspaper's archive and website. He claimed that because these articles portrayed him as an untrustworthy businessman, he was unable to obtain bank loans to open new companies. The judge dismissed his lawsuit, arguing that deleting these lawful reports from the archive simply because they contained negative implications would harm the integrity of the newspaper's archive, which

would no longer serve as a reliable witness to the past. This would open the door to rewriting history.

3.3.2 Case 2: David Webb Case in Hong Kong [16] The plaintiff in this case had filed for divorce, and the court issued three judgments in 2000, 2002, and 2002, which were accessible in the Legal Reference System (LRS). These three judgments did not anonymize the names of the plaintiff, her ex-husband, and her children, and the three judgments could be retrieved in the LRS by entering the plaintiff's name. The plaintiff requested in 2010 and 2012 that the Chief Justice of the Hong Kong Supreme Court delete these three judgments from the system, but the Chief Justice held that the principle of open justice requires court judgments to be publicly accessible. These three judgments could not be deleted from the judicial system's website, but could be processed by pseudonymizing the names of the plaintiff, her ex-husband, and her children in the three judgments in the system. This processing is consistent with GDPR provisions, as the court held that deleting this information would harm public interest, but pseudonymization could be adopted because it would not affect the purpose of archiving and providing these judgments to the public.

3.3.3 Case 3: Wegrzynowski and Smolczewski v. Poland [17] The two plaintiffs in this case had filed a civil lawsuit in the Warsaw Regional Court against two journalists from the Rzeczpospolita daily newspaper for defamation due to their inaccurate reporting. The Warsaw Regional Court supported their claim, ruling that the two journalists had failed to take necessary measures to verify the accusations against the two plaintiffs in the newspaper reports, and ordered the journalists and the newspaper's editor-in-chief to donate to charity and publish an apology in the newspaper. However, the plaintiffs discovered that this critical report remained accessible on the newspaper's website and could be retrieved through the Google search engine. They requested that this report be deleted from the newspaper's website, but this request was not supported by the Warsaw Regional Court, leading them to sue in the European Court of Human Rights (ECtHR). In 2013, the ECtHR issued a judgment dismissing the plaintiffs' claim. The ECtHR held that web archives, including those maintained by the media, are protected by the right to freedom of expression. The media's primary function is to act as a public watchdog, but it also has the duty to preserve and provide access to archives containing previously published news. The ECtHR also acknowledged the Warsaw Regional Court's view that judicial institutions cannot participate in rewriting history by ordering the deletion of all traces of publication from the public domain. It also considered the feasible remedy proposed by the Warsaw Regional Court—inserting a comment on the webpage informing the public of the outcome of the previous civil litigation—as worthy of consideration.

In the above cases, newspapers, courts, and other institutions archived valuable personal information based on public interest. When citizens requested the deletion of this information based on personal interests, these requests were not

supported by the courts, which held that personal interests must yield to public interest in such cases.

In summary, the proposal and establishment of the right to be forgotten will not hinder libraries and archives from archiving information based on public interest, nor will it prevent libraries and archives from archiving and preserving valuable personal information.

4. Impact of the Right to be Forgotten on Information Access in Libraries and Archives

Although the right to be forgotten will not hinder information archiving in libraries and archives, the proposal and establishment of the right to delisting within this right may affect information access in libraries and archives, resulting in certain archived information being unavailable or restricted from access. This is primarily because the retrieval systems of libraries and archives may also be considered search engines, and some countries' libraries and archives have already established information take-down policies that reflect respect for the right to be forgotten.

4.1 Definition of Search Engines

Based on existing court judgments, the right to delisting primarily targets large commercial search engines such as Google, Bing, and Yahoo. However, courts have not explicitly defined search engines. In the case of Google Spain SL v. Agencia Española de Protección de Datos, the Court of Justice of the European Union (CJEU) held that the characteristic activity of search engines is "collecting data, then retrieving, recording, and organizing this data within the framework of their indexing programs, storing this data on their servers, and making this data available to users through the form of listing search results" [18]. J. Kerr also notes that the CJEU adopted a relatively broad interpretation of what constitutes a search engine, considering search engines to be any service with retrieval characteristics that can connect users to websites based on their selection of search terms, including internal search engines that only operate within websites [19]. According to the CJEU's interpretation, the online retrieval systems of libraries and archives could also be considered search engines. If a data subject believes that personal information involving them is inappropriate, irrelevant, or excessive, they could also require libraries and archives to prevent such information from being displayed when searching using their name, making it potentially impossible for other users to find this information.

4.2 Information Take-Down Policies of Libraries and Archives

Currently, libraries and archives in some countries, such as the United Kingdom and Australia, have established information take-down policies that stipulate under specific circumstances, the public can apply to have certain information

removed from libraries' and archives' online retrieval systems and no longer provided for access. The author analyzed the information take-down policies of the British Library, The National Archives (UK), the National Library of Scotland, the National Archives of Scotland, and the National Library of Wales, finding that these institutions' current policies all specify circumstances under which information removal can be applied for, generally including: when providing information online violates copyright law; when information contains sensitive personal data; when information contains obscene or defamatory content; and when information has been incorrectly published online. The provision allowing application for removal when "information contains sensitive personal data" is consistent with the purpose of establishing the right to delisting, and the National Archives of Scotland's 2018 information take-down policy explicitly states that under GDPR, files containing personal or sensitive personal information may result in such information being removed [20].

Therefore, the establishment of the right to delisting will affect information provision and access in libraries and archives, resulting in certain personal information being unavailable through retrieval systems or unsearchable by name. However, it should be noted that the right to delisting primarily grants data subjects the right to restrict and terminate the dissemination of personal data they believe is detrimental to their interests. Therefore, the removal of information from retrieval systems does not mean the information is deleted from the collections of libraries and archives. For information removed from online retrieval systems, libraries and archives generally store it in specialized databases and provide some explanation on their websites regarding the reasons for its removal. According to the survey by V. Dressler and C. Kristof, when information is taken down from websites, some libraries' catalogs include corresponding explanations, and some libraries create "tombstone" pages to inform users that the information has been removed, also informing users that the removed information is preserved in a separate archive. Some institutions call this archive a "dark archive," where access to preserved archives is restricted or prohibited [9]. Therefore, the right to delisting may result in certain personal data or information in libraries and archives being unavailable or restricted from access, but it will not lead to the deletion of this information. Moreover, information removed from online retrieval systems is not permanently closed to everyone; libraries and archives must determine based on specific circumstances whether some information may be allowed for use by certain individuals under legal provisions, or whether the reasons for removal no longer exist, in which case the information can be restored for retrieval and access.

Furthermore, the establishment and protection of the right to delisting may also lead libraries and archives to proactively refrain from providing access to certain personal information, primarily due to operational cost considerations. As mentioned above, one condition for exercising the right to delisting is the determination that the personal information is inappropriate, irrelevant, or excessive. According to the 2014 Google Spain judgment, this determination is generally first made by the data controller, i.e., the search engine. Therefore,

if a data subject applies to libraries and archives based on the right to be forgotten to prevent their personal information from appearing in search results, libraries and archives must generally first determine whether to approve this application, which increases operational costs. For example, between May 30, 2014, and April 31, 2019, Google processed applications from 502,648 applicants involving 3,231,694 web pages, with an average of 47,000 applications per month since January 2015, requiring thousands of hours of human review [21]. In the review process, balancing individual rights and public interest is not easy for libraries and archives. If data subjects do not agree with the handling results of libraries and archives, they may file lawsuits, causing litigation burdens for these institutions. These factors may lead libraries and archives to proactively refrain from providing access to certain personal information to reduce operational costs.

5. Implications and Recommendations

The establishment and protection of the right to be forgotten will not hinder information archiving in libraries and archives. However, to achieve a balance between the right to be forgotten and public interest, libraries and archives need to particularly observe the following principles when archiving information:

(1) **Principle of Data Minimization**: Personal information/data to be archived must be relevant, necessary, and adequate for archiving purposes. Personal information/data beyond these requirements should not be archived. Determining whether archived personal information/data is relevant, necessary, and adequate depends primarily on the archiving purpose. Therefore, when conducting information archiving, libraries and archives must collect and preserve personal information closely aligned with their archiving purposes.

(2) **Principle of Ensuring Personal Information/Data Integrity**: As seen in the case of Wegrzynowski and Smolczewski v. Poland, even when some inaccurate information or reports are archived, courts will not support requests to delete such information. However, libraries and archives need to ensure the integrity of archived information. From a records management perspective, complete records should include both content and metadata. According to ISO 15489 5.2.3, record metadata includes information about the record's content, structure, creation and use context, relationships with other records or metadata, and business activities and events involving the record during its existence. In Wegrzynowski and Smolczewski v. Poland, the Warsaw Regional Court proposed inserting information about the civil judgment in dispute on the page of the contested report, which would add metadata to the file of the disputed report to ensure the integrity of information reflecting the entire event. Similar practices are reflected in a 2015 case of the Constitutional Court of Colombia, which involved an online magazine that mentioned the name of a person accused of slave trafficking but who had not been convicted.

> The court held that the magazine did not need to delete this information, but only needed to update the report and inform readers that the person had not been convicted [22], i.e., to add corresponding metadata to make the information more complete. Therefore, libraries and archives must also observe the principle of ensuring archived information integrity when archiving information. Ensuring the integrity of archived information can further achieve the adequacy of personal information/data. This is a professional requirement for libraries and archives as memory institutions to preserve social memory, and it is also an important measure to balance individual rights and public interest.

Given the impact of the right to be forgotten on information provision and access in libraries and archives, these institutions need to establish and improve a whole-process review mechanism: (1) **Information Provision and Access Review Mechanism**, i.e., reviewing whether information to be provided for access involves personal privacy or sensitive personal information, which can be considered ex ante review; (2) **Information Removal Review Mechanism**, i.e., reviewing citizens' applications for information removal and making corresponding handling decisions, which can be considered interim review; and (3) **Removed Information Restoration Review Mechanism**, i.e., periodically reviewing removed information to determine whether the circumstances leading to removal have changed and whether such information can be provided for access again, which can be considered ex post review. Libraries and archives need to formulate review standards and procedures for these mechanisms and establish dedicated review teams and members. To ensure transparency throughout the process, libraries and archives need to publicly disclose these review standards and procedures. Additionally, for information removal applications, libraries and archives may adopt pseudonymization. "Pseudonymization" refers to replacing personal data characteristics with other symbols such that data subjects cannot be identified without using additional information. "Pseudonymization" differs from "anonymization," which is a technical rule for concealing personal characteristics to make them no longer identifiable. Data processed through anonymization is no longer personal data and can be used and traded without the consent of personal data subjects [23]. When receiving information removal applications, libraries and archives can pseudonymize some information and provide the pseudonymized information for use, while storing additional information used to identify data subjects in other databases. In practice, the circumstances under which pseudonymization can be applied should be determined based on specific situations. For example, pseudonymization is generally not applied to public figures, but is required for minors. The general principle is that pseudonymization should not impair the purpose of information archiving. To help users obtain needed information, library and archive staff should provide users with more search suggestions and assistance.

This paper primarily discusses the impact of the right to be forgotten on information archiving and access in libraries and archives as memory institutions, and proposes some principles and mechanisms. However, many issues

warrant further research, such as how to formulate review standards for the series of review mechanisms, under what specific circumstances personal information "pseudonymization" can be implemented in practice, whether information "pseudonymization" will affect the evidentiary value of such information or even threaten public trust in libraries and archives as trusted memory preservation institutions, and how libraries and archives can timely collect relevant metadata given the dynamic nature of record/information metadata to ensure the integrity of relevant personal information. Additionally, if certain information archived by libraries and archives cannot be provided for access due to protection under the right to delisting, the information obtained by the public may be incomplete, which may affect the construction of social memory or academic research.

References

[1] IFLA statement on the right to be forgotten [EB/OL]. [2021-06-01]. https://www.ifla.org/node/10272.

[2] ICA Congress Abu Dhabi, United Arab Emirates 19-22 October 2021 (rescheduling) Call for proposals and papers [EB/OL]. [2021-02-16]. https://www.ica.org/en/call-for-proposals-and-papers-ica-abu-dhabi-congress-closed.

[3] TRETIKOV L. European court decision punches holes in free knowledge [EB/OL]. [2021-02-16]. https://blog.wikimedia.org/2014/08/06/european-court-decision-punches-holes-in-free-knowledge/.

[4] DE BAETS A. A historian's view on the right to be forgotten [J]. International review of law, computers & technology, 2016, 30(1/2): 57-66.

[5] HENTTONEN P. Privacy as an archival problem and a solution [J]. Archival science, 2017(17): 285-303.

[6] DE ROSNAY M D, GUADAMUZ A. Memory hole or right to delist? Implications of the right to be forgotten for Web archiving [J]. Social science research on the Internet, 2017(6): 1-22.

[7] WYBER S. The right to be forgotten and libraries [J]. Journal of information ethics, 2018, 27(2): 81-97.

[8] ZHANG Tao. Conflict and balance in the application of the right to be forgotten in web information archiving [J]. Archives science study, 2020(5): 126-133.

[9] DRESSLER V, KRISTOF C. The right to be forgotten and implications on digital collections: a survey of ARL member institutions on practice and policy [J]. College & research libraries, 2018, 79(7): 972-990.

[10] DETERWANG NEC. The right to be forgotten and informational autonomy in the digital environment [C]// GHEZZI A, PEREIRA G, VESNIC-ALUIE.

The ethics of memory in a digital age. Palgrave macmillan memory studies. London: Palgrave Macmillan, 2014: 82-101.

[11] ZANFIR G. Tracing the right to be forgotten in the short history of data protection law: the "new clothes" of an old right [C]// GUTWIRTH S, LEENES R, DE HERT P. Reforming European data protection law. Law, governance and technology series. Dordrecht: Springer, 2015(20): 227-249.

[12] Judgment of the court (Grand Chamber) 24 September 2019 [EB/OL]. [2021-02-16]. https://curia.europa.eu/juris/document/document_{print}.jsf;jsessionid=FF2068A68B302A60C

[13] Library of Congress will no longer archive every Tweet [EB/OL]. [2021-02-16]. http://www.npr.org/sections/thetwo-way/2017/12/26/573609499/library-of-congress-will-no-longer-archive-every-tweet.

[14] The Oakland archive policy [EB/OL]. [2021-02-16]. https://www2.sims.berkeley.edu/research/conferences/policy/AA_B_{{{54}}_{{2014}}}.pdf.

[15] Dutch newspaper De Volkskrant can keep negative articles in internet archive [EB/OL]. [2021-02-16]. https://www.pcpd.org.hk/english/enforcement/decisions/privacy_{{{commiss

[16] Administrative appeal no. 54/2014 between David M Webb and Privacy Commissioner for personal data [EB/OL]. [2021-02-16]. https://www.pcpd.org.hk/english/enforcement/decisio

[17] Wegrzynowski and Smolczewski v. Poland [EB/OL]. [2021-02-16]. https://globalfreedomofexpression.columbia.edu/cases/wegrzynowski-smolczewski-v-poland/.

[18] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos [EB/OL]. [2021-04-09]. http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pa

[19] KERR J. What is a search engine? The simple question the Court of Justice of the European Union forgot to ask and what it means for the future of the right to be forgotten [J]. Chicago journal of international law, 2016, 17(1): 219-242.

[20] Records reclosure and take-down policy [EB/OL]. [2021-02-16]. https://www.nrscotland.gov.uk/files//record-keeping/record-keeping-policies/nrs-records-reclosure-and-take-down-policy-june-2018.pdf.

[21] BERTRAM T, BURSZTEIN E, STEPHANIE C, et al. Five years of the right to be forgotten [C]// Proceedings of the 2019 ACM SIGSAC conference on computer and communications security. New York: Association for Computing Machinery, 2019: 959-971.

[22] Corte Constitucional de Colombia, Sentencia T-277/15 [EB/OL]. [2021-02-16]. http://www.corteconstitucional.gov.co/relatoria/2015/t-277-15.htm.

[23] GAO Ying, DU Juan. Legal regulation of data anonymization in the big data era [J/OL]. Information studies: theory & application, 2021. [2021-02-20]. https://kns.cnki.net/kcms/detail/11.1762.G3.20210529.1757.002.html.

Note: Figure translations are in progress. See original paper for figures.