Legal and Ethical Aspects of Data Privacy

Benefits and Harm of Permanent Retention of Records

By: Stephanie Chinn

Abstract

The abilities provided by nearly infinite storage are a powerful tool for records managers in permanently retaining records and information, but the question must be asked of whether or not these records *should* be kept and for how long. This paper attempts to prompt thoughtfulness in assigning retention schedules based on the benefits of permanency as well as the potential drawbacks, including financial, legal and ethical aspects of the decision.

February 25, 19

Table of Contents

Introduction **2**

What is Permanent Retention? **2**

Permanent Record Retention in Government **3**

Permanent Record Retention in Companies and Business **4**

Permanent Record Retention in Personal Life **4**

Reasons for Permanent Retention **5**

Why not keep it all? **6**

Privacy Acts **8**

Right to be forgotten **9**

Laws and Regulations **10**

Challenges in implementation **12**

Criticism **13**

Conclusion **14**

Introduction

As the sum body of human knowledge continues to expand in the Digital Age, information seekers find that data and records are easier to access than at any time before in human history. A researcher is now capable of accessing materials from literally the other side of the Earth, and even those not on the planet, but instead in orbit in the International Space Station, can access data from around the world in just a matter of minutes, rather than waiting days, weeks, months, or even years to be able to travel to a repository of information or have documents sent to them. Data storage is no longer limited by the cubic feet of shelving available to a facility in some back room or closet; digitization of documents now makes it possible to house entire library systems full of texts in a space smaller than a shoe box. The question data and records managers now face is no longer whether they *can* continue the practice of permanent record retention, but whether they *should* keep those records and for how long. At what point, if ever, is it acceptable to allow certain information to dissolve into the ether and no longer be retained?

What is Permanent Retention?

Permanent Retention as a term is not as easily defined and one might think. The Association of Records Managers & Administrators (ARMA) defines a permanent record as a "record that has been determined to have sufficient historical, administrative, legal, fiscal, or other value to warrant continuing preservation" (ARMA International, 2017). This definition implies long-term preservation, but how long is that really? The Rosetta Stone, inscribed in 196 BC and later rediscovered in 1799 AD, is a granadiorite stele inscribed with a decree written

during the Ptolemaic dynasty in Egypt and is an obvious, though possibly somewhat exaggerated, example of the permanent retention of a document (Rosetta Stones, 2018). Records today are not literally carved in stone for all time, so how long should they realistically be kept? The answer is "it depends."

Permanent Record Retention in Government

Federal records management for the United States government is handled by the National Archives and Records Administration (NARA) who defines permanent records as "Federal records that have been determined by NARA to have sufficient value to warrant their preservation in the National Archives even while they remain in agency custody" (U.S. National Archives, 2018). All federal records are appraised for retention timelines and designated as either temporary or permanent retention based on their proposed records schedule. Those items meeting the specific criteria set forward in Appendix C of the Disposition of Federal Records are identified as permanent records, regardless of physical form or characteristic. These items include records on organizations and functions, formal minutes of boards and commissions, records of internal agency, interagency and nonfederal committees, legal opinions and comments on legislation, formal directives, procedural issuances, and operating manuals relating to program functions, selected evaluations of internal operations, analytical research studies and periodic reports, agency histories and selected background materials, briefing materials, public relations records, publications, selected audiovisual and graphic records, general correspondence or subject files documenting substantive agency programs, selected case files, and other selected data, though this list is not exhaustive. Additionally, in recognition of the fact that many pre-twentieth century records have been destroyed by fire,

flood and neglect, NARA has elected to permanently retain otherwise routine administrative and housekeeping records from that period in an effort to document the organization, functions, and activities of the Government from that time period (U.S. National Archives, 2016a). Records designated for permanent retention by the U.S. Government are to be kept indefinitely, or until such time as they are released for disposition. At that time, they may be either destroyed or re-designated as temporary records following a new records schedule (U.S. National Archives, 2016b).

Permanent Record Retention in Companies and Business

Like the U.S. Government, many companies have designated certain records as being of sufficient historical value to the company that they should be kept indefinitely. Unlike the government, these businesses tend to recognize the possibility of the company terminating its existence, either through bankruptcy or some other form of dissolution and permanent records are generally understood to be those retained so long as the company or division is in existence, often described using the phrase “in perpetuity” or referring to the life of the company (LOC). Even that length of time is not always enough for some records, such as tax and other accounting records. There may be legal requirements that necessitate maintaining these records beyond the life of the company, extending even further than “permanent” record retention (Serber, 2016).

Permanent Record Retention in Personal Life

Retention schedules for personal records vary widely due to the very fact that they are handled on a personal level by individuals who are far less likely to create formal record

retention policies than governments or companies, and also far less likely to follow those policies if they are created. An individual may keep permanent records for the lifetime of the person it pertains to, or even far longer if those records are handed down from one generation to another, as in the case of genealogical records and other items of historical significance to family members. Generally speaking, it is recommended that individuals maintain records for no longer than ten years maximum except for proof of title or ownership and medical records. These items should be retained permanently with ownership records being archived after an asset is sold and medical records being actively maintained for the lifetime of the individual (PrivacyRights.org, 2018).

Reasons for Permanent Retention

There are many reasons that an organization or individual would want to retain a record permanently. These records are often designated as having a high enduring or archival value and are sometimes referred to as being 'significant' or 'major' in order to separate them from those that need only be retained temporarily while active. Using these terms, even if only in thinking about the records, can help to form that distinction. Significant records set a precedent or have considerable economic, environmental or social impact. They may lead to or document a major change in policy or capture some other unique event or point in history that would be of interest in the future. Alternatively, thinking about what would happen if a record were lost or destroyed may help to identify how long it should be retained. Records that may be required for legal or medical purposes in the future should be retained, as well as those of a unique or historical nature (Drechshage, 2016).

Research records may need to be maintained if they contain scientific or mathematical data proofs or otherwise contribute to the overall body of human knowledge. Just as historically significant records must be retained to tell the story of our society, scientific research must be retained to show the path of investigation and progression of overall knowledge.

Additionally, there may legal reasons for permanently maintaining some records. Many jurisdictions have what are commonly referred to as Sunshine Laws as an extension of the U.S. Freedom of Information Act (FOIA) of 1967. The FOIA requires federal agencies to disclose any information requested under the Act "unless it falls under one of nine exemptions which protect interests such as personal privacy, national security, and law enforcement" based on a presumption of openness for the operations of such agencies (Freedom of Information Act, 2018). Local Sunshine Laws require that meetings of governmental agencies and departments be open to the public that they serve, and these laws require specific records to be retained and available for public inspection.

Why not keep it all?

While digital records take up far less physical storage space than printed documents, they do still require space and resources to maintain. The price of digital storage can quickly add up when dealing with large numbers of records. Since digital files degrade with use, files designated for permanent retention in a repository that are still being actively used should be backed up with both user-level copies and archival-level files. Back-ups are preferably stored off-site, in a different physical location to reduce risk of loss due to a physical failure or disaster, and many repositories rely on cloud storage or automated file duplication to a secondary

location. User-level files can be more compressed for faster downloads and repeated uses, where archival-level files will typically have lower compression rates and larger files sizes. Archival-level files may be stored in a dark-archives backup copy of the repository and are preserved for future use, typically with no current access. Checksums can be used to ensure fixity of data within digital files. Sometimes called a hash sum, this is a numerical value assigned to a file based on the number of set or unset bits in a file (Technopedia.com, 2018). This value will not change unless the file itself is altered or degrades. Monitoring the checksum of a digital file will give early warning if an error appears in a user-level copy and it can be replaced with a new copy based on the archival-level file. Storage and monitoring of permanently retained digital files requires an ongoing financial commitment for equipment and resources.

Furthermore, retaining records unnecessarily opens an organization to the responsibility of producing those records when requested. Records that are maintained beyond the legal requirements prompt a need for additional staffing for the storage and organization of these records, as well as exposing the organization to the possibility of additional information requests that must be complied with.

In addition to rightful requests for information, maintaining more records than is necessary in permanent storage opens an organization to possible information security breaches. While every organization should have in place policies that to safeguard against data breaches, the reality is that hackers and other criminals will continue to exploit security vulnerabilities and data breaches do happen. The only way to truly ensure that records cannot be stolen is to not keep them to begin with. This is just one more reason that organizations

should evaluate what records are truly necessary for permanent retention as part of building and evaluating a permanent records retention strategy.

Privacy Acts

Additionally, privacy concerns must be considered when deciding whether or not to keep records. For example, the American Library Association (ALA) considers a patron's right to privacy to be a major pillar of the ALA Library Bill of Rights. Violating that privacy can have a significant chilling effect on a library user's willingness to exercise their right to read and impair free access to ideas. "True liberty of choice in the library requires both a varied selection of materials and the assurance that one's choices are not monitored" (American Library Association, 2017). As a result of these foundational beliefs, the ALA recommends that libraries limit the degree to which personally identifiable information about patrons is monitored, collected, disclosed and distributed, even in compliance with local, state, and federal law. Libraries are not required to collect or maintain information about library users, though many do on a temporary basis as long as a record is active and then remove them afterwards. For example, the library maintains a record linking a patron to an item that they checked out as long as they have possession of that item. When the item is returned and it is no longer necessary to keep the record active, the specific record linking that patron with that item can then be removed in order to preserve the patron's privacy.

Beyond values-based privacy rights, there are legal requirements for maintaining privacy of personal records, primarily based on ethical guidelines. The Privacy Act of 1974 prohibits the disclosure of a record about an individual from a system of records without the written consent of the individual. There are some exceptions built into this Act, but generally speaking, it

ensures that information collected about an individual by a federal agency must remain private unless authorized by that individual. Individuals also have the right to examine the information collected about them and to make corrections if necessary, which could prompt changes to permanently retained records. For this reason, a good records management plan will include guidelines for updating records that are no longer considered active as part of a commitment to maintaining accuracy of permanent records.

Education and Health records must also legally be kept private. The Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA) set forth guidelines for maintaining privacy of the associated records, even from family members. From the inception of FERPA in 1974, educational institutions receiving government funding from any applicable program must maintain the privacy of the education records of students unless written permission is provided for disclosure of those records, except in the case of minor children, whose educational records may be released to their parents/guardians in certain cases (Family Educational Rights and Privacy Act, 1974). Similarly, HIPAA sets forth rules protecting the privacy of Personal Health Information and each healthcare entity must provide the individual with a notice explaining its privacy practices. Except in specific cases when required by law, such as reporting suspected child abuse to state child welfare agencies, the healthcare entity must have written permission in order to release Personal Health Information to any other entity, including the individual's family, insurance company, or other medical professionals (Health Insurance Portability and Accountability Act, 2003).

Right to be forgotten

These Acts do not constitute the only legal privacy rights allowed to individuals. In recent years, the digital age and the rising popularity of internet use has brought forth an expansion of existing data privacy regulations in the form of the right to be forgotten. The theory behind this newly defined right is based on the difficulty of escaping one's past on the internet. The core provision of this right was articulated by the European Commissioner for Justice, Fundamental Rights and Citizenship, Viviane Reding on January 22, 2012 when she noted that "If an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system" (Stanford Law Review, 2012). In other words, it is "the right to silence on past events in life that are no longer occurring" (Pino, 2000). 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" and is distinct from the right to privacy. The right to privacy deals with information that is not generally known, while the right to be forgotten allows an information to remove information that was publicly known at one time in an effort to deny third parties further access to the information (Weber, 2011).

Laws and Regulations

Because so many records are available online and can be accesses from nearly anywhere, it is important to take into account the various laws of different jurisdictions, including those of countries other than the United States. Many jurisdictions are struggling with privacy rights and legally and ethically controlling access to personal information in the digital age. The result has been an influx of international laws regarding the right to be forgotten.

Depending on the jurisdiction, those laws can have very different requirements that have far-reaching implications.

One of the most commonly discussed legal requirements for the right to be forgotten in recent years is due to a new regulation in the European Union. The European Union adopted the General Data Protection Regulation (GDPR) in April 2016 with an enforcement date beginning May 25, 2018. The regulation was intended to "enhance data protection rights of individuals and to improve business opportunities by facilitating the free flow of personal data in the digital single market" (Council of the European Union, 2015). The final regulation addresses the export of personal data outside of the European Union (EU) and the European Economic Area (EEA) by requiring that controllers of personal data place appropriate technical and organizational measures in place to implement data protection principles. It requires that organizations use the highest possible privacy settings by default in an effort to ensure that data is not made public without explicit consent of the individual and that the information cannot be used to identify a specific individual without additional information that is stored separately. Individuals have the right to revoke this consent at any time. In practice, this means that no more than two specific pieces of data about any individual may be stored in the same file, either physical or digital, at any given time to be completely certain that a data breach will not compromise security. Organizations must report any data breaches within 72 hours of discovery if any data or records are compromised.

Organizations that are not compliant could face hefty fines, and it is still unclear how far-reaching this law truly is in practice. GDPR does not only apply to organizations located within the European Union, but also to organizations outside of the EU and EEA if they offer

good or services to or monitor the behavior of European Union citizens. All companies that process or hold personal data of individuals residing in the European Union must comply with GDPR, regardless of where the company is located, potentially implicating companies who do not do business in the EU but have customers who are citizens. Fines for companies found to be non-compliant with GDPR can range from 2-4% of the company's annual global turnover to €20 million, or over $22.6 million (EUGDPR.org, 2018).

Challenges in implementation

There are obvious challenges to implementing and enforcing laws governing the right to be forgotten in areas outside the initiating sovereign state. Unless explicitly agreed to in international treaties, citizens and organizations are not legally required to follow laws and regulations outside of the rule's associated jurisdiction. As a result enforcement options for newly founded right to be forgotten laws and regulations are still unclear in cases where companies do not operate or have holdings inside of the governing sovereign state (Levin Institute, 2016). In the case of GDPR, which claims authority of all organizations dealing with EU citizens, even if they do not operate inside of the European Union, enforcement is questionable and still largely untested. Globalization of the internet in the digital age has changed the interpretation of international economic laws and only time will tell how sovereign states and other trade unions will react to efforts to enforce laws not ratified by their citizens. For now, many companies are opting to implement security requirements, even if they are not required to do so and erring on the side of caution in regards to requests for removing personal information.

Criticism

Laws and regulations governing the right to be forgotten on the internet affect search engines as well, even if they are not directly hosting the information to be removed. When the draft version of a European Data Protection Regulation was released in 2012, Google quickly formed and Advisory Council of professors, lawyers, and government officials from around Europe to provide guidelines for decisions on removal requests in the search engine. By May of 2014, Google had removed nearly 1.4 million URLs from its results pages in the EU, but noted that the information could still be easily found through non-European search engines. In July 2015, an accidental data leak revealed that over 95% of removal requests were from citizens attempting to protect personal and private information. Criticism came when the members of the other requests were analyzed and found to be criminals, politicians, and public figures that were requesting the removal of links to information many outsiders deemed to be publicly relevant, calling into question the balance of weighing an individual's right to privacy with the public's right to know (Brindle, 2015).

The initial response to requests for information removal are handled internally by organizations, leading to varying policies on what should and should not be removed. If denied, an individual requesting the removal of information has the right to appeal to their local data protection agency (Dean, 2015). Reasons for takedown requests have varied widely, as well as the final decisions by data protection agencies. The resulting uncertainty may easily prompt a chilling effect on intellectual freedom on an international level as search engines are forced to essentially censor results rather than remain neutral providers of data. The regulations, governing rights that are deliberately left broadly defined in an effort to accommodate new

technologies in the future, are still new enough that case law has not concretely defined how narrowly they will be applied in practice (Stanford Law Review, 2012).

Conclusion

Napoleon Bonaparte is famously quoted as once stating “History is the version of past events that people have decided to agree upon.” The study of history is based on the records that our society chooses to leave behind, both in large organizations and in the everyday lives of individuals. Records being created today may not still be available thousands of years from now, even if they are referred to as “permanent” but these records still maintain the history of the organization or individuals they are a part of. It is this responsibility to future information needs, and not the availability of storage and resources that demands consideration of whether or not a record should be kept or allowed to be lost to time. Records should be carefully evaluated for both the pros and cons of permanency before deciding on a retention schedule.

Bibliography

American Library Association. (2017, April). Privacy. Retrieved from http://www.ala.org/advocacy/privacy

ARMA International. (2007). *Glossary of records and information management terms* (3rd Edition). Lenexa, KS: ARMA International.

Brindle, B. (2015, March 4). How can Google forget you? Retrieved from https://computer.howstuffworks.com/how-can-google-forget-you.htm

Council of the European Union, President. (2015, June 11). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Retrieved from http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

Dean, J. (2015, May 13). Google could face legal action over 'right to be forgotten' rejections. *The Times*. Retrieved from https://www.thetimes.co.uk/article/google-could-face-legal-action-over-right-to-be-forgotten-rejections-v6spmk2gz0s

Drechshage, A. (2016, September 19). GRDS records, will you be my significant or other? Retrieved from https://grkblog.archives.qld.gov.au/2016/09/20/grds-records-will-you-be-my-significant-or-other/

EUGDPR.org. (2018, August). GDPR FAQs – EUGDPR. Retrieved from https://eugdpr.org/the-regulation/gdpr-faqs/

Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (1974). Retrieved from https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Freedom of Information Act (FOIA). (2018). Freedom of Information Act. Retrieved from https://www.foia.gov/about.html

Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104–191 (1996). Retrieved from https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm

Levin Institute, State University of New York. (2016). International Law | Globalization101. Retrieved from http://www.globalization101.org/category/issues-in-depth/international-law/

Pino, G. (2000). *The right to personal identity in Italian private law: Constitutional interpretation and judge-made rights* (SSRN Scholarly Paper No. ID 1737392). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=1737392

Privacy Act of 1974, Pub. L. No. 93–579, § 552a, 5 U.S.C. (1974). Retrieved from https://www.justice.gov/opcl/privacy-act-1974

PrivacyRights.org. (2018, June 12). Personal record retention and destruction plan. Retrieved from https://www.privacyrights.org/consumer-guides/personal-data-retention-and-destruction-plan

Rosetta Stone. (2018). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Rosetta_Stone&oldid=871278209

Stanford Law Review. (2012, February 13). The right to be forgotten. Retrieved from https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/

Surber, R. (2016, March 24). What does a permanent retention period really mean? Retrieved from https://www.zasio.com/what-does-a-permanent-retention-period-really-mean/

Technopedia.com. (2018). What is checksum? Retrieved from https://www.techopedia.com/definition/1792/checksum

U.S. National Archives and Records Administration. (2016a, August 15). Disposition of federal records - Appendix C. Retrieved from https://www.archives.gov/records-mgmt/publications/disposition-of-federal-records/appendix-c.html

U.S. National Archives and Records Administration. (2016b, August 15). Frequently asked questions about records scheduling and disposition. Retrieved from https://www.archives.gov/records-mgmt/faqs/scheduling.html

U.S. National Archives and Records Administration. (2018, August 1). Agency permanent records. Retrieved from https://www.archives.gov/records-mgmt/scheduling/permanent-records

Weber, R. H. (2011). The right to be forgotten: More than a Pandora's box? *Journal of Intellectual Property, Information Technology and E-Commerce Law*, *2*, 120–130. Retrieved from https://nbn-resolving.org/urn:nbn:de:0009-29-30849

