ARCHEION
2023, T. CXXIV, s. 57–78
ISSN 0066-6041
e-ISSN 2658-1264

DOI 10.4467/26581264ARC.23.011.17871

Parsing privacy for archivists

Trudy Huskamp Peterson

archivesthp@aol.com

ABSTRACT
Protection of privacy is a key issue in determining the extent to which archival materials are to be made accessible to the public. But what is informational privacy; i.e., what are the elements of information found in any type of document or database that must be withheld to avoid intruding on the privacy of an individual? This essay first examines post-World War II international statements that reference privacy. Then it turns to statements referring to privacy issued by the International Council on Archives (ICA), the worldwide professional organization that represents the archival profession to UNESCO. Third is a brief look at several 21st century academic considerations of privacy, one each by a lawyer, a philosopher, and an historian. Finally, it outlines some of the contextual elements that help archivists manage sensitive materials, even without a final definition of informational privacy.

KEYWORDS
privacy protection, access to archival documents, personal data, international conventions and agreements on access to archives, UN human rights conventions, International Council on Archives, International Federation of Library Associations and Institutions

Ochrona prywatności w praktyce archiwalnej

STRESZCZENIE
Ochrona prywatności jest jednym z kluczowych zagadnień podczas ustalania zakresu publicznego udostępniania materiałów archiwalnych. Co bowiem oznacza ochrona informacji dotyczącej życia prywatnego. Przykładowo, które z elementów informacji zawartej w jakimkolwiek rodzaju dokumentu lub bazy danych powinny pozostać nieujawnione, aby uniknąć naruszenia prywatności osoby indywidualnej. W artykule w pierwszym rzędzie przeanalizowano powojenne dokumenty międzynarodowe, odnoszące się do ochrony prywatności. Następnie zwrócono uwagę na dokumenty dotyczące zagadnienia ochrony prywatności, opublikowane przez Międzynarodową Radę Archiwów (ICA), organizację reprezentującą międzynarodowe środowisko archiwalne wobec UNESCO. W części końcowej zawarto przegląd wybranych, opublikowanych w XXI w., prac naukowych, dotyczących ochrony prywatności, których autorzy reprezentują nauki prawne, filozofię i historię. W podsumowaniu Autorka podkreśliła niektóre elementy kontekstu dokumentów archiwalnych, które mogą okazać się pomocne dla archiwistów w toku zarządzania materiałami zawierającymi informacje wrażliwe[1].

SŁOWA KLUCZOWE
ochrona prywatności, dostęp do dokumentów archiwalnych, dane osobowe, międzynarodowe konwencje i umowy dotyczące dostępu do archiwów, konwencje ONZ o ochronie praw człowieka, Międzynarodowa Rada Archiwów, Międzynarodowa Federacja Stowarzyszeń i Instytucji Bibliotekarskich

[1] W tekście zachowano oryginalny, zastosowany przez Autorkę, styl cytowania i bibliografii.

In the aftermath of World War II, the new United Nations adopted the Universal Declaration of Human Rights. Its Article 12 reads:

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

This suggested that all persons reading that Article would know what privacy means. That is simply not true. While privacy as a concept is seemingly universal, what is private and under what circumstances differs widely between peoples and over time. Here are a few personal examples:

1. When I was an archivist with the United States (U.S.) National Archives appraisal project on the records of the Federal Bureau of Investigation (FBI) we project archivists were absolutely barred from seeing income tax return information in the files. The agents who looked at the files before handing them to us would put a brown paper bag over any tax return in the file, and we would simply note on our review sheet that a tax document was included. In Sweden, by contrast, personal income tax information is open to the general public – immediately.
2. On a visit to South Korea, the then-director of the National Archives asked me, "Are you a Christian?". I was uncomfortable with the question and mumbled a response. Such a question is acceptable in Korean culture. But in countries and eras ranging from Nazi-period Poland to Bosnia during the 1990s, not forgetting the Inquisition in Europe, information on the religious persuasion of an individual was a private matter of the gravest consequence.
3. Some years ago, I read an article in the "American Historical Review" about Germany after the Second World War. It appeared that the author had had access to files in the German Federal archives relating to what I considered highly private matters, so I alerted a German archivist to the apparent privacy issue. He replied that the researcher was a bona fide academic and therefore was given access.
4. In the early 1990s, in anticipation of the transfer of records from U.S. to German control, the U.S. and Germany negotiated over access to the records of former Nazi party members that were held by the U.S. in the Berlin Document Center. German law required that the files with private information be closed for 30 years after the death of the individual, while

the U.S. position was that the records with private information would be available at the death of the person. The two nations resolved to treat each copy – the original in Germany and a microfilm in the U.S. – in accordance with national law. Subsequently, a steady stream of researchers came to the U.S. National Archives to use the microfilm records available in the U.S. but closed in Germany.

These examples show how differently national or ethnic groups conceive of what is private and what is not. Even countries that share many common ideas, such as the U.S. and Sweden and Germany, end up with quite different positions on privacy.

Privacy is a key issue in determining access to archives. Should the archivist of a private media company release unpublished images that show a recognizable dead person whose relatives likely are still alive? Should a government archivist release the 40-year-old report, with critical comments, of a social worker's visit to a family? What should a police archivist do with 20-year-old images from police body cameras taken during a call to a house where a domestic fight is underway? What should a university archivist do if, in the papers of a deceased medical faculty member, there are reports of what today would be unethical medical procedures carried out on pregnant women? What should an archivist in a faith-based institution release of records of adoptions from a home for unwed mothers that closed 30 years ago? What should the archivist release of the donated sizzling love letters of a man to his wife, if the man is dead but the wife is still alive and the deed of gift has no restrictions?

The application of access restrictions based on the need to protect privacy is, therefore, of great concern to historians who work on contemporary topics and want access to archives. They may –and often do – encounter materials closed for reasons of privacy. To understand those closures and the reasoning behind them requires a look into the considerations of the concept of privacy that were current in the second half of the 20th century and the early decades of the 21st[2].

Is there an international norm on privacy? This essay first examines post-World War II international statements that reference privacy. Then it turns to statements referring to privacy issued by the International Council on

[2] This essay concerns solely information privacy, not the issues of physical intrusion into body and home.

Archives (ICA), the worldwide professional organization that represents the archival profession to UNESCO. Third is a brief look at several 21st century academic considerations of privacy, one each by a lawyer, a philosopher, and an historian. Finally, it outlines some of the contextual elements that help archivists manage sensitive materials, even without a final definition of information privacy.

I. International inter-governmental statements

A. Universal Declaration of Human Rights, Covenant and Conventions

The United Nations Charter mandated the creation of a Commission on Human Rights, and the UN's Economic and Social Council created and charged the Commission to come up with a recommendation and report "regarding […] an international bill of rights". The Commission worked for two years on a Universal Declaration, which was adopted by the United Nations (UN) General Assembly on 10 December 1948. (The Commission specifically wanted it to be a universal and not just a UN Declaration)[3].

The final version of Article 12 on privacy reflected contributions from many of the 58 countries that made up the new United Nations, but the basic language came from Latin American countries that, at the same time as the Declaration was being drafted, were writing the Organization of American States' American Declaration of the Rights and Duties of Man, known as the Bogota Declaration. The Bogota document, adopted six months before the Universal Declaration, stated "Every person has the right to the protection of the law against abusive attacks upon his honor, his reputation, and his private and family life" and "Every person has the right to the inviolability and transmission of his correspondence"[4]. The UN drafting committee for the Universal Declaration's Article 12 used

3 J. Morsink, *The Universal Declaration of Human Rights. Origins, drafting and intent,* Philadelphia 1999. See especially Chapter 4, sections 1 and 2, for discussion of Article 12. This discussion is based on Morsink's analysis.

4 American Declaration of the Rights and Duties of Man, O.A.S. Res. XXX, adopted by the Ninth International Conference of American States (1948), http://hrlibrary.umn.edu/oasinstr/zoas2dec.htm (accessed 2023-06-30).

draft language from the Bogota Declaration and language drawn from national constitutions. Examples of constitutional language included:

- Argentina: "The domicile is inviolable, as also epistolary correspondence and private papers".
- Bolivia: "Every house is an inviolable asylum" and "epistolary correspondence and private papers are inviolable".
- Yugoslavia: "The dwelling is inviolable" and "the privacy of letters and other means of communication is inviolable".

The drafters found similar phrases in the constitutions of Egypt, Iraq, Lebanon, Belgium, Denmark, and Luxembourg.

As the drafting got underway, the U.S. proposed the text, "No one shall be subjected to arbitrary or unauthorized searches of his person, home, papers and effects or to unreasonable interference with his person, home, family, relations with others, reputation, privacy, activities or property. The secrecy of correspondence shall be respected". Panama suggested, "Freedom from unreasonable interference with his person, home, reputation, privacy, activities, and property is the right of everyone. The State has the duty to protect this freedom". The Chinese delegation offered, "No one shall be subjected to unreasonable interference with his privacy, family, home, correspondence or reputation". The Soviet Union proposed, "No one shall be subjected to arbitrary interference with his privacy, family, home, correspondence, honor and reputation". And a delegate from the Philippines argued that reputation needed to be added to the protected elements as "[t]here were parts of the world where the former practices of Nazi Germany and Japan were being carried out. Reputations were ruined beyond repair by systematic defamation in the press and by other methods. Some safeguard against such attacks should be included".

In these draft offerings, privacy, reputation, and correspondence are all mentioned, as if they are separate but related issues. Notice, too, that in all the quotes from national constitutions and in the proposed languages, no definitions of privacy are offered. In his detailed study of the drafting of the Declaration, Johannes Morsink found no evidence of an attempt to define privacy. The drafters appear to have thought that privacy as a concept was obvious. While the Nazi *government's* intrusion into privacy clearly forms the background to the development of the attitudes reflected in Article 12, the final language does not exclude the intrusion by one *citizen* or *private entity* upon the privacy of another

and, in fact, specifically requires the state through "protection of the law" to protect citizens, one from another.

The inclusion of the word "arbitrary" in Article 12 signaled that, if legally warranted, some invasions of privacy and correspondence could be made. The delegate from Saudi Arabia explained, "The right of every individual to be free from State interference in his private life must be regarded as sacred as long as that right was not used as a cloak for activities which were essentially detrimental to the general good, or which endangered its general welfare and security". The drafters clearly understood that a government would hold at least some information that an individual would consider private, but they said nothing about a right to information about either what the government was doing or what information it had on you as an individual.

Soon after the Universal Declaration was adopted, efforts began to complement it with the "hard legal form of an international treaty" to bind State parties to respect the basic civil and political rights of individuals[5]. This culminated in the adoption and entry into force in 1976 of the UN Covenant on Civil and Political Rights. Its Article 17 reiterated the privacy statement of the Declaration, with no further explanation. In 1988 the UN Human Rights Committee published "General Comment No. 16: Article 17 (Right to Privacy)" of the Covenant, which said the right to privacy "is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons", clarifying in advance of the explosion of social media that businesses and other private entities are also to observe the privacy rights of persons. "Correspondence should be delivered to the addressee without interception and without being opened or otherwise read", it declared. And the Comment explained, "The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law", placing the burden on the State to ensure that the right is protected through "legislative and other measures"[6].

---

5 Ch. Tomuschat, "International Covenant on Civil and Political Rights," United Nations Audiovisual Library of International Law, https://legal.un.org/avl/pdf/ha/iccpr/iccpr_e.pdf (accessed 2023-06-30).

6 The Comment also said: "Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited", never foreseeing that individuals might choose to use devices that automatically surveil them. See idem.

During the following two decades, the United Nations adopted several conventions that include a privacy element:[7]

- The UN Convention on the Rights of the Child, entered into force in 1990, referenced privacy in Article 16, without further definition: "1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honor and reputation. 2. The child has the right to the protection of the law against such interference or attacks"[8].
- The International Convention on the Protection of All Migrant Workers and Members of Their Families entered into force in 2003. Its Article 14 says: "No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and members of his or her family shall have the right to the protection of the law against such interference or attacks"[9].
- The Convention on the Rights of Persons with Disabilities, in force in 2008, said in Article 22: "1. No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication or to unlawful attacks on his or her honour and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks. 2. States Parties shall protect

---

7 The United Nations Declaration on the Rights of Indigenous Peoples curiously refers to privacy only in terms of private religious sites; Article 12(1): "Indigenous people have the right to manifest, practice, develop and teach their spiritual and religious traditions, customs and ceremonies; the right to maintain, protect, and have access in privacy to their religious and cultural sites; the right to the use and control of their ceremonial objects; and the right to the repatriation of their human remains", https://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP_E_web.pdf (accessed 2023-06-30).

8 Convention on the Rights of the Child adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989 entry into force 2 September 1990, in accordance with article 49, https://www.unicef.org/child-rights-convention/convention-text# (accessed 2023-06-30).

9 International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families Adopted 18 December 1990 by General Assembly Resolution 45/158, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-protection-rights-all-migrant-workers (accessed 2023-06-30).

the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others"[10].

In sum, the Universal Declaration and the subsequent Covenant and Conventions do not get us very far towards an understanding of what is information privacy. It is clear that the personal correspondence of an individual, in the possession of that individual, should generally be protected from intrusion and not be made public unless the person chooses to do so. And the 2008 Convention shows that medical information falls within the privacy penumbra, as understood by the UN nation-states.

B. International Guidelines in the 1980s

During the 1970s, the rapid adoption of computers in government agencies and private businesses led to a series of studies and recommendations on data protection. The Organization for Economic Co-Operation and Development (OECD) was established in 1961. By 2023 it had 38 member countries with 6 "accession candidate" countries and 5 non-member "key partner" countries and served as a major international economic think tank. In the late 1970s OECD commissioned a group of experts to develop guidelines on the transborder flow of data. The guidelines were adopted in 1980, with OECD noting in the preface "that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties and in reconciling fundamental but competing values such as privacy and the free flow of information"[11]. The Annex to the Guidelines defines "personal data" as "any information relating to an identified or identifiable individual (data subject)". And it specifies that the Guidelines apply to data in both the public and private sectors. The OECD Guidelines were enormously influential. They had a specific economic focus: they aimed to prevent domestic legislation, such as the data

[10] Convention on the Rights of Persons with Disabilities adopted 13 December 2006 by Sixty-first session of the General Assembly by resolution A/RES/61/106, https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities (accessed 2023-06-30).

[11] Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en (accessed 2023-06-30). The Guidelines were updated in 2013.

protection and privacy acts that were being developed in Europe and North America during the 1970s, from harming the flow of information necessary for commerce.

By 1981 the United Nations Human Rights Commission's sub-commission on discrimination and minorities was studying "guidelines for computerized personal files, particularly as they affected the privacy of the individual"[12]. Revised throughout the 1980s, the "guidelines for the regulation of computerized personal data files" were adopted by the UN General Assembly in 1991[13]. The guidelines do not offer a definition of privacy or private information, simply referring to "information about persons" or "personal data".

Also during the 1980s, Interpol, the International Criminal Police Organization, became involved in the question of privacy and data protection. While revising the Headquarters agreement for Interpol, the UN General Assembly mandated the creation of an independent body to monitor the implementation of Interpol's data protection practices. Interpol then adopted a formal statement of its compliance with the UN guidelines on data protection. Interpol noted, however, that the protection of the data it held that was sent to Interpol by national police authorities was the responsibility of the sender: "as it is only the custodian of the police information that it receives from member countries, Interpol is required to handle such information in accordance with the demands of those countries"[14].

In the late 1980s UNESCO funded a study by the International Council on Archives on archival appraisal of records containing personal information. In that study, personal information was defined as "any information about an identifiable individual that is recorded in any format", leaving open the question of what of that information should be accorded privacy protection and, indeed, what is privacy in an archival context[15].

---

12 Report of the Sub-Commission on Prevention of Discrimination and Protection of Minorities on its 34th Session, Geneva, 17 August–11 September 1981, E/CN.4/1512, https://digitallibrary.un.org/record/29890 (accessed 2023-06-30).

13 Guidelines for the Regulation of Computerized Personnel Data Files. Resolution adopted by the UN General Assembly 1991, https://digitallibrary.un.org/record/105299 (accessed 2023-06-30).

14 S. El Zein, *Reconciling Data Protection Regulations with the requirements of judicial and police co-operation, 21st International Conference on Privacy and Personal Data Protection. Hong Kong Convention and Exhibition Centre China 13–15 September 1999*, http://oigouvernance.blogspot.com/2013/11/reconciling-data-protection-regulations.html (accessed 2023-06-30).

15 T. Cook, *The Archival appraisal of records containing personal information. A Ramp Study with Guidelines*, UNESCO, April 1991, PGI-91/WS/3, https://unesdoc.unesco.org/ark:/48223/

C. Principles for the Protection and Promotion of Human Rights through Action to Combat Impunity

A major step in stating an international right to information privacy came with the publication of the Principles for the Protection and Promotion of Human Rights through Action to Combat Impunity by the United Nations Commission on Human Rights. Distinguished French legal scholar Louis Joinet developed the principles (often called the "Joinet Principles"), which included five principles on the "preservation of and access to archives bearing witness to violations". Accepted by the UN Commission on Human Rights in 1997, they were revised by American University law professor Diane Orentlicher in 2005[16].

The Principles obligate a State "to preserve archives and other evidence concerning violations of human rights and humanitarian law and to facilitate knowledge of those violations"[17]. The Principles then address the tension between access to archives to combat impunity and privacy for victims and other individuals (Joinet/Orentlicher tacitly excludes from the "other individuals" category those persons who are implicated in human rights violations). The Principles offer a set of categories for access, based on the relationship of the person to the information sought. They are:

- Victims and their relatives get access to records that would assist them in rights claims.
- Persons implicated get access for their legal defense.
- Historical researchers gain access "subject to reasonable restrictions aimed at safeguarding the privacy and security of victims or other individuals"[18].

---

pf0000090644 (accessed 2023-06-30). I was a member of the "group of experts" whose deliberation formed the basis for the study.

16 "The Administration of Justice and the Human Rights of Detainees: Questions of the impunity of perpetrators of human rights violations (civil and political). Revised final report prepared by Mr. Joinet pursuant to Sub-Commission decision 1996/119", United Nations Commission on Human Rights, Sub-Commission on Prevention of Discrimination and Protection of Minorities, E/CN.4/Sub.2/1997/20/Rev.1,1997-10-02; updated by E/CN.4/2005/102, 18 February 2005, and E/CN.4/2005/102/Add.1, 8 February 2005, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G05/109/00/PDF/G0510900.pdf?OpenElement (accessed 2023-06-30). I reviewed the principles relating to archives for the 2005 revision.

17 Ibidem, principle 3.

18 Ibidem, principle 15.

- Courts and non-judicial commissions of inquiry, as well as investigators reporting to them" get access to "relevant archives" but "in a manner that respects applicable privacy concerns, including in particular assurances of confidentiality provided to victims and other witnesses as a precondition of their testimony"[19].
- A balancing test between access and privacy is required for access to "the files of commissions of inquiry", with access "balanced against the legitimate expectations of confidentiality of victims and other witnesses testifying on their behalf"[20].The Principles further warn that at the outset of the work of commissions of inquiry, the commissions "should clarify the conditions that will govern access to their documents, including conditions aimed at preventing disclosure of confidential information while facilitating public access to their archives"[21]. Further, "information that might identify a witness who provided testimony pursuant to a promise of confidentiality must be protected from disclosure"[22].
- Addressing "specific measures relating to archives containing names" defined as "information that makes it possible, directly or indirectly, to identify the individuals to who they relate", the Principles state that a person is entitled to know when his or her name appears "in State archives"[23].

What is not covered in the Principles is a definition of privacy. The caution about information provided with a promise of confidentiality is reasonably clear, although it is sometimes hard to identify in files exactly which statements are covered by an implied as opposed to an explicit promise. For example, does the mere appearance of someone's name in a file as someone who talked to a commission require protection?

The question of duration is also not covered. Understandably, the Principles (like the Universal Declaration) have a presentist orientation. But what happens when the records of such a commission are 30 years old? 50? 100? Here we return to the cultural distinction between a society that considers the actions of ancestors equal to the action of today's generations and a society like the United

---

19 Ibidem, principle 16.

20 Ibidem, principle 17.

21 Ibidem, principle 8(f).

22 Ibidem, principle 10(d).

23 Ibidem, principle 17(b). For further information on the Principles, see F. Haldeman and T. Unger, eds., *The United Nations Principles to Combat Impunity: A Commentary,* Oxford University Press, 2018.

States where the principle of "no privacy for the dead" is generally accepted. Still, by clarifying that there are different categories of users and that they have different rights of access, the Joinet/Orentlicher Principles made a significant step forward to an international understanding of privacy, particularly in an archival context.

D. The 21st century and the UN Special Rapporteurs

During the first two decades of the 21st century a good many declarations and conventions with a privacy component were issued by regional inter-governmental groups, such as the European Union's important General Data Protection Regulation. But the next major truly international action was the 2015 decision by the UN Human Rights Council to appoint a UN Special Rapporteur (SR) on the right to privacy. The Council cited the "global and open nature of the Internet" as a driving force behind the creation of the post, noted that "certain types of metadata, when aggregated, can reveal personal information and can give an insight into an individual's behaviour, social relationships, private preferences and identity", and affirmed "that the same rights the people have offline must also be protected online, including the right to privacy". This seems to be nearing a statement of the categories of personal life that could be grouped as privacy concerns. The Special Rapporteurs have issued a series of statements and reports, ranging over such topics as health-related data, gender impacts of data release, big data analytics, and privacy for children. The first SR, Joseph Cannataci, suggested "metrics for privacy" for states to use to judge their privacy position, but these are of little help to archivists faced with specific questions of information privacy. In the summer of 2022 SR Ana Brian Nougrères issued a report analyzing seven international documents to ascertain the "principles underpinning privacy and the protection of personal data", but neither SR has specifically considered the issues of archival materials that also contain important privacy information[24].

[24] The Office of the High Commissioner for Human Rights, Special Rapporteur on the right to privacy, https://www.ohchr.org/en/special-procedures/sr-privacy (accessed 2023-06-30).

II. International archival statements

Aware that archivists in the post-Cold War era were struggling to implement practices to identify and protect materials containing private information, the international archival community began adopting significant policy statements relating to information privacy.

First, in 1996 the International Council on Archives adopted an international archival Code of Ethics[25]. Its Principle 7 reads, "Archivists should respect both access and privacy, and act within the boundaries of relevant legislation. Archivists should take care that corporate and personal privacy as well as national security are protected without destroying information, especially in the case of electronic records where updating and erasure are common practice. They must respect the privacy of individuals who created or are the subjects of records, especially those who had no voice in the use or disposition of the materials".

Also in the early 1990s, the ICA established a group of experts to discuss problems related to archives of former regimes and make recommendations for their management. Funded by UNESCO and issued in 1997, the experts' report recognized the right to historical and scholarly research in records of repressive regimes, but warned that "[a]ccess to such documents must take into account the need to protect the victims of repression. Appropriate measure must be taken to protect third parties mentioned in the document". If "individual privacy and the right to historical investigation are opposed" in a demand for access, copies of the records with "names of victims or third parties deleted" may be provided[26]. Published the same year as the influential Joinet Principles, together the two statements focused attention on privacy issues that arose when managing the records of repressive regimes and away from the broader situations in which questions of information privacy arise.

In 2012 ICA adopted "Principles of Access to Archives". Principle 4 reads, "Institutions holding archives ensure that restrictions on access are clear and

---

25 International Council on Archives, ICA Code of Ethics, https://www.ica.org/en/ica-code-ethics (accessed 2023-06-30).

26 A. Gonzalez Quintana, "Archives of the Security Services of Former Repressive Regimes: Report prepared for UNESCO on behalf of the International Council on Archives," Paris: UNESCO, 1997, https://unesdoc.unesco.org/ark:/48223/pf0000140074 (accessed 2023-06-30).

of state duration, are based on pertinent legislation, acknowledge the right of privacy and respect the rights of owners of private materials"[27]. As the chair of the drafting committee, I can report authoritatively that we intentionally, specifically, did not attempt a definition of privacy, avoiding the contentious variations we knew existed. However, the Access Principles were supplemented in 2014 by "Technical Guidance on Managing Archives with Restrictions", which provides a sample access policy for an archival institution. The sample suggests that an archives announce that "Materials containing information, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy of a living person", should be restricted until a specific set of conditions are met[28]. It further explains that the materials to be restricted in this category would contain "information about a living person which reveal details of a highly personal nature which if released, would constitute a clearly unwarranted invasion of privacy, including but not limited to information about the physical or mental health or the medical or psychiatric care or treatment of the individual, and which personal information is not known to have been made public previously."

Next, in 2016 ICA issued as a "working document" a set of "Basic Principles on the Role of Archivists and Records Managers in Support of Human Rights". The commentary to its Principle 11 says, "Uncritical opening of archives may result in violations of the privacy of individuals and may result in retaliation

---

27 Principles of Access to Archives, Adopted by the AGM on August 24, 2012, https://www.ica.org/sites/default/files/ICA_Access-principles_EN.pdf (accessed 2023-06-30).

28 These restrictions are that the materials may be disclosed only:

i. "To the named individual or his authorized representative, provided that access will not be granted if the records are restricted pursuant to any other general or specific restrictions; or
ii. If the individual or his legal representative agrees to its release; or
iii. To those officers and employees of the office of origin or its successor in function who have a need for the information in the performance of their official duties; or
iv. To the Donor of the materials or to the Donor's designee, pursuant to the provisions of the Donor's deed of gift; or
v. To researchers for the purpose of statistical or quantitative medical or psychiatric research when such researchers have provided the ***** Archives with written assurance that the information will be used solely for statistical research or reporting and that no individually identifiable information will be disclosed by the researcher's work".

See: Principles of Access to Archives. Technical Guidance on Managing Archives with Restrictions 2014-02-01, p. 16–17, https://www.ica.org/sites/default/files/2014-02_standards_tech-guidelines-draft_EN.pdf (accessed 2023-06-30).

against them. Archivists and records managers balance the right to truth with the need to protect the privacy of identifiable persons"[29].

Finally, in 2020 ICA with the International Federation of Library Associations and Institutions issued a joint "Statement on Privacy Legislation and Archiving", commenting on "the emergence of a new, tougher, generation of privacy laws around the world". It argued that restrictions to archival materials should be "applied strictly based on the spirit and letter of any relevant law, including privacy legislation, interpreted according to professional understanding and judgment. Such restrictions clearly include situations where the information could facilitate identity theft, or where it is unfair, irrelevant, or causes unreasonable harm (for example in the context of «right to be forgotten» legislation)"[30]. The statement is not altogether clear: what could be closed as "irrelevant" information?

As a whole, these five statements make a little progress in helping to determine what information privacy interests are, but they are not wholly satisfactory as workday guidance.

III. Academic views

Lawyers, philosophers, sociologists, historians and others all have tried to define privacy. The literature is enormous, dating from the late nineteenth century and presenting distinct viewpoints. Scholars in the 21st century continue to have robust discussions on the nature of privacy.

A report by the UN Special Rapporteur on privacy quoted legal scholar Daniel Solove, a specialist in privacy law, as identifying six general conceptions of privacy among academic thinkers: "(1) The right to be let alone; (2) limited access to self – the ability to shield oneself from unwanted access by others; (3) secrecy – the concealment of certain matters from others; (4) control over personal information – the ability to exercise control over information about oneself; (5) personhood – the protection of one's personality, individuality, and dignity;

[29] Basic Principles on the role of Archivists and Records Managers in support of Human Rights, https://www.ica.org/en/basic-principles-on-the-role-of-archivists-and-records-managers-in-support-of-human-rights-0 (accessed 2023-06-30).

[30] IFLA-ICA Statement on Privacy Legislation and Archiving 2020, https://www.ifla.org/publications/ifla-ica-statement-on-privacy-legislation-and-archiving/ (accessed 2023-06-30).

and (6) intimacy – control over, or limited access to, one's intimate relationships or aspects of life". Solove argued that all these conceptions were inadequate in one or more way and suggested instead that privacy "should be conceptualized contextually as it is implicated in particular problems. When we protect privacy, we protect against disruptions to certain practices"[31].

Solove's contention is supported by a concept called "contextual integrity", which argues that people do not need complete privacy; they need privacy within certain social norms. Philosopher Helen Nissenbaum posited four variables in the question of contextual integrity: the context of a flow of information, the capacities in which the individuals sending and receiving are acting, the type of information, and how the information is transmitted[32]. Historian Lawrence Cappello, agreeing with Solove, further argued that information has three stages-collected, processed and disseminated – and wrote that "in the struggle to find an appropriate privacy balance for information, the battle over collection has been lost" and information processing "is the new key battleground"[33].

The European Court of Human Rights in the 2008 case of *S. and Marper v. the United Kingdom* adopted a position similar to that of these three scholars when it wrote that "in determining whether the personal information retained by the authorities involves any [...] private-life aspects [...], the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the result that may be obtained"[34].

This approach – viewing privacy as a matter in context – avoids the slippery problem of definition and points toward pragmatic practice instead of dogmatic definition.

---

31 D.J. Solove, "Contextualizing Privacy," *California Law Review,* 2002, 1087–1156. Quoted in Joseph A. Cannataci, "Visit to the United States of America: Report of the Special Rapporteur on the right to privacy," A/HRC/46/37/Add.4, 20 January 2021.

32 H. Nissenbaum, "Privacy as Contextual Integrity," *Washington Law Review,* v. 79, February 4, 2004, pp. 101–139, https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf (accessed 2023-06-30).

33 L. Cappello, *None of Your Damn Business: Privacy in the United States from the Gilded Age to the Digital Age,* University of Chicago Press, 2019, pp. 266–267.

34 European Court Of Human Rights, Case of S. and Marper v. The United Kingdom (Applications nos. 30562/04 and 30566/04), para.67, Judgment, Strasbourg 4 December 2008, https://rm.coe.int/168067d216 (accessed 2023-06-30).

IV. Archivists and privacy information in context

Archivists deciding on release of privacy information stand within two contexts: within an employing organization, responding to the directions given them by law or internal rule (for instance, a regulation adopted by a faith-based organization, a rule created by a civil society entity) and as acting a surrogate for the person whose information is embodied in the document. In the first context, the archivist has no decision to take except to follow the law and regulation. However, in the second context, asserting a privacy interest in the document is exercising the power to decide on matters of significant personal interest on behalf of another.

A separate set of disclosure rules governs release of materials to the person who is the subject of the item or file, someone with legal responsibility for a person, or a party in litigation – each will have unique access to the information. However, when the release is to the general public, including to an historian, the archivist, standing in the shoes of the subject person, thinks not about the concept of privacy itself but whether the release of that particular information might invade the person's privacy. Here context is everything: the name of a person in a public database of telephone number is one thing, but that same name in a list of persons undergoing drug rehabilitation is quite another.

So how can archivist think through the context in which the information in embedded? By asking questions and considering context such as these:

Creator and recipient. The difference between an item in any format created by the person and the item created by another organization or individual about that person is significant, as is the identity of the immediate custodian of the document. A sexually explicit email within the personal materials donated by the person who made or received it is one context; that same email picked up by police surveillance and found within a file on suspected subversives is very different.

Age of the information. Most court cases that involve privacy questions relate to information about living persons; i.e., usually within 50 to 70 years of when the invasion of privacy occurred. In archives, items that contain information, even medical information, may be releasable after the person is dead or after a period passes after the person is dead, a period that varies by nation

and culture. Laws that seem to close archives containing personal information in perpetuity trouble this consideration.

Cultural group. Closely related is whether the information in the item is related to an individual, family, clan, or other group. Cultural differences are key here, and interests of such groups can extend the time that the information must be sequestered. For example, information about the religious and tribal rights of Indigenous people may require closure indefinitely, with exceptions only as negotiated with the group.

Cultural norms. The types of information a culture may deem sensitive include (among others) marital status, birth legitimacy, medical conditions, welfare status, religious affiliation, and personal and family financial information. Whether photographs of the dead can be released is affected by cultural sensibilities, for example. When the information relates to a person in a culture other than that of the archivist, especially careful consideration of the larger implications of release is required.

Risk to person. Whether the release of the information would put an individual at risk, mortally or through discrimination, damage, harassment, or embarrassment must be considered. For instance, the release of the name of a person who provided information to a commission investigating corruption could lead to reprisals against that person or the person's family.

Public status. If the person about whom the information applies is a living public figure, some information that would be protected for an average period might be made public because of the great public interest in the information on a celebrity.

Previous disclosure. If there has been official public disclosure (not leaked) of the information, including disclosure by the person, and especially if the person is aware that the information was made public and did not take action against the disclosing party, the further release of the information is unlikely to cause an invasion of privacy.

Conclusion

International statements that refer to privacy have not included a universally acceptable definition of privacy beyond generalities. The post-Cold War developments in human rights and archival institutions have emphasized the

rights of persons named in records, particularly those of repressive regimes, and produced some guidance on handling sensitive personal information. Other texts by international organizations have skirted the issue of definition of privacy entirely, recognizing the diversity in approaches, both across cultures and across time. Recent academic thinkers have suggested that a global definition of privacy is not necessary, that a pragmatic approach, looking at specific legal and policy problems in a specific context, will do. As Daniel Solove pithily observed, "All generalization is an imperfection"[35].

For the archivists, information privacy is not absolute. Context is key to understanding the potential harm that release of information can reasonably be expected to cause. Information carelessly disclosed about a person can lead to ruined reputations, disrupted family life, and even murder.

Answers to the questions and the decisions about access to information that has a privacy component can be exceedingly difficult to find. Sincere, competent professionals can reach different conclusions. But the crux of dealing with the information privacy concept is professional cognitive empathy, the ability to momentarily stand in the shoes of another and to decide.

Bibliography

Cappello L., *None of your damn business. Privacy in the United States from the gilded Age to the digital age*, Chicago 2019, pp. 266–267.

Cook T., *The archival appraisal of records containing personal information: A RAMP study with guidelines*, Paris 1991, PGI-91/WS/3, https://unesdoc.unesco.org/ark:/48223/pf0000090644 (accessed 2023-06-30).

El Zein S., *Reconciling data protection regulations with the requirements of judicial and police co-operation. 21st International Conference on Privacy and Personal Data Protection. Hong Kong Convention and Exhibition Centre China 13–15 September 1999*, http://oigouvernance.blogspot.com/2013/11/reconciling-data-protection-regulations.html (accessed 2023-06-30).

European Court Of Human Rights, Case of S. and Marper v. The United Kingdom (Applications nos. 30562/04 and 30566/04), Judgment, Strasbourg 4 December 2008, https://rm.coe.int/168067d216 (accessed 2023-06-30).

[35] D.J. Solove, op. cit.

Gonzales Quintana A., Archives of the security services of former repressive regimes. Report prepared for UNESCO on behalf of the International Council on Archives, Paris 1997, https://unesdoc.unesco.org/ark:/48223/pf0000140074 (accessed 2023-06-30).

Haldeman F., Unger T. (eds.), *The United Nations Principles to Combat Impunity. A Commentary*, Oxford 2018.

Morsink J., *The Universal Declaration of Human Rights. Origins, drafting and intent*, Philadelphia 1999.

Nissenbaum H., "Privacy as Contextual Integrity," Washington Law Review, v. 79, February 4, 2004, pp. 101–139, https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf (accessed 2023-06-30).

Organization for Economic Co-Operation and Development, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en (accessed 2023-06-30).

Organization of American States, American Declaration of the Rights and Duties of Man, O.A.S. Res. XXX, adopted by the Ninth International Conference of American States (1948), http://hrlibrary.umn.edu/oasinstr/zoas2dec.htm (accessed 2023-06-30).

Solove D.J., "Contextualizing Privacy," California Law Review, 2002, 1087–1156.

Tomuschat Ch., *International Covenant on Civil and Political Rights*, United Nations Audiovisual Library of International Law, 2008, https://legal.un.org/avl/pdf/ha/iccpr/iccpr_e.pdf (accessed 2023-06-30).

International Council on Archives

Basic Principles on the Role of Archivists and Records Managers in Support of Human Rights, https://www.ica.org/en/basic-principles-on-the-role-of-archivists-and-records-managers-in-support-of-human-rights-0 (accessed 2023-06-30).

Code of Ethics, https://www.ica.org/en/ica-code-ethics (accessed 2023-06-30).

International Federation of Library Associations – International Council on Archives. Statement on Privacy Legislation and Archiving 2020, https://www.ifla.org/publications/ifla-ica-statement-on-privacy-legislation-and-archiving/ (accessed 2023-06-30).

Principles of Access to Archives, Adopted by the AGM on August 24, 2012, https://www.ica.org/sites/default/files/ICA_Access-principles_EN.pdf (accessed 2023-06-30).

Principles of Access to Archives. Technical Guidance on Managing Archives with Restrictions 2014-02-01, https://www.ica.org/sites/default/files/2014-02_standards_tech-guidelines-draft_EN.pdf (accessed 2023-06-30).

United Nations

Convention on the Rights of the Child adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989 entry into force 2 September 1990, in accordance with article 49, https://www.unicef.org/child-rights-convention/convention-text# (accessed 2023-06-30).

Convention on the Rights of Persons with Disabilities adopted 13 December 2006 by Sixty-first session of the General Assembly by resolution A/RES/61/106, https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities (accessed 2023-06-30).

Guidelines for the Regulation of Computerized Personnel Data Files. Resolution adopted by the UN General Assembly 1991, https://digitallibrary.un.org/record/105299 (accessed 2023-06-30).

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families Adopted 18 December 1990 by General Assembly Resolution 45/158, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-protection-rights-all-migrant-workers (accessed 2023-06-30).

United Nations Commission on Human Rights. Report of the Sub-Commission on Prevention of Discrimination and Protection of Minorities on its 34th Session, Geneva, 17 August–11 September 1981, E/CN.4/1512, https://digitallibrary.un.org/record/29890 (accessed 2023-06-30).

United Nations Declaration on the Rights of Indigenous Peoples, https://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP_E_web.pdf (accessed 2023-06-30).

United Nations Human Rights Council. The Administration of Justice and the Human Rights of Detainees, Question of the impunity of perpetrators of human rights violations (civil and political). Revised final report prepared by Mr. Joinet pursuant to Sub-Commission decision 1996/119, E/CN.4/Sub.2/1997/20/Rev.1,1997-10-02; updated by E/CN.4/2005/102, 18 February 2005, and E/CN.4/2005/102/Add.1, 8 February 2005, https://search.un.org/search?sort=relevance&collection=ods&currentPageNumber=1&q=Revised+final+report+prepared+ by+Mr.+Joinet+&row=10&start=1 (accessed 2023-06-30).

United Nations Office of the High Commissioner for Human Rights:

Special Rapporteur on the right to privacy, https://www.ohchr.org/en/special-procedures/sr-privacy (accessed 2023-06-30).

Special Rapporteur on the right to privacy, visit to the United States of America, 20 January 2021, A/HRC/46/37/Add.4, https://digitallibrary.un.org/record/3899160 (accessed 2023-06-30).