Arch Sci (2007) 7:107–127
DOI 10.1007/s10502-007-9055-5

ORIGINAL PAPER

The long-term preservation of identifiable personal data: a comparative archival perspective on privacy regulatory models in the European Union, Australia, Canada and the United States

Livia Iacovino · Malcolm Todd

Published online: 29 August 2007

Abstract This article analyses the extent to which archival exemptions for historical, scientific and statistical research in privacy legislation support preservation in selected European Union countries, and comparable aspects of Australian, American and Canadian law within a legal, ethical and digital archival perspective. The authors recommend that the further processing of personal data under data protection law be given a wider scope of interpretation for archival preservation purposes in both the public and private sector, coupled with the use of researcher and archival codes in relation to access to personal data. They also recommend early appraisal and integration of privacy with freedom of information and archival regimes.

Keywords Privacy laws · Data protection · Personal data · Digital preservation

This article is a substantially revised version of a paper entitled, "Ethical Principles, Accountability and the Long-term Preservation of Identifiable Personal Data: A Comparative Analysis of Privacy Legislation in Australia, Canada, the European Union and the United States", presented at the Association of Canadian Archivists, *Ethics and Accountability in the Archival Sphere*, 29th Annual Conference, Montréal, Québec, Canada May 26–29, 2004. The paper grew out of research conducted for University of British Columbia, *International Research on Permanent Authentic Records in Electronic Systems* Project, InterPARES 2 (IP2), 2002–2006, http://www.interpares.org/ip2/ip2_index.cfm (consulted December 2004). The authors would like to acknowledge the contribution of IP2 policy group researchers in relation to US, Belgian and Canadian material, respectively Terry Maxwell, University at Albany, New York; Hannelore Dekeyser, Katholieke Universiteit, Leuven and Jane Morrison, University of British Columbia, Vancouver.

L. Iacovino (✉)
Centre for Organisational and Social Informatics, Caulfield School of Information Technology, Monash University, P.O. Box 197, Caulfield East, 3145 VIC, Australia
e-mail: Livia.Iacovino@infotech.monash.edu.au

M. Todd
The National Archives—currently on secondment to the Westminster Parliament, Richmond, UK
e-mail: toddmr@parliament.uk

Introduction

Despite global terrorism that has begun to erode privacy rights in a number of countries, there is a move not only to protect identifiable personal information, but also to ensure further legal protection on the basis of perceived sensitivity to certain classes of personal information. These trends include limiting the collection, use and disclosure of sensitive information such as that of racial, ethnic and political persuasion, and placing even higher protection on very sensitive personal data such as health-related information. At the same time, government policies world-wide are encouraging the re-use of personal data in shared networked environments by using unique identifiers to link personal data across jurisdictions and institutions, thus increasing potential privacy abuses in relation to secondary uses (Paterson and Iacovino 2004).

How can records creators and preservers, including archivists and other third parties such as researchers, balance their legal and moral obligations to protect personal information from inappropriate collection, use and disclosure, with its preservation for record reliability and authenticity, essential to societal, corporate and personal accountability? Is the fundamental right to privacy wider than the data protection issue? What about the private sector and the "compatibility" between archival and business purposes? When does privacy cease, for example does it continue after death and for how long? What has been the impact of increased security and terrorism on the collection, disclosure and retention of personal data? How have different jurisdictions tackled these issues? This article addresses these questions within the context of a comparative study in progress on privacy regulatory models and their "archiving" provisions from a legal, ethical and digital archival perspective (Iacovino 2004). It analyses some specific archival exemptions in privacy legislation in representative European Union member countries as at 2003, and comparable provisions of Australian, American and Canadian federal law, as they impact on long-term preservation of personal data in electronic records.

Privacy and the preservation of personal data: legal, archival and ethical perspectives

Privacy is recognised internationally as a human and a legal right and has a strong ethical basis. It is embedded in international conventions and is found in the ethical codes and values of many professions including that of the archivist and the researcher. European-initiated privacy guidelines which have been accepted by many countries are based on Article 17 of *The International Covenant on Civil and Political Rights* 1966, which follows from the Article 12 of the United Nations *Universal Declaration of Human Rights* 1948 (Department of Foreign Affairs 1998). The covenant provides that individuals shall not be subjected to arbitrary or unlawful interference with their privacy and that they have the right to the protection of the law against such interference or attacks. The continuing international support for privacy was re-affirmed by the *World Summit on the Information Society* in 2003, which included the need to prevent the use of information resources and technologies for criminal and terrorist purposes, while respecting human rights and the ethical dimensions of the information society (World Summit 2003).

All recordkeeping participants (record creators, preservers and third parties) have legal obligations to protect information about individuals in records under statutes and common law, which may be distinct from their moral duties. The legal obligations are found in freedom of information, privacy and recordkeeping legislation, and legal duties of confidentiality, contractual and other special relationships, balanced with the correlative rights

of access to information by the record subject or a third party. In addition to legislation, recordkeeping professionals adhere to principles of confidentiality in relation to records under their control through their professional codes and through the implementation of access policies (Ketelaar 1995; International Council on Archives 1996). Many other professionals have a legal and ethical duty of confidentiality that also protects their clients' privacy. Researchers in the fields of genetics, human cloning and human tissue banks have particularly stringent guidelines to comply with. The record subject's informed consent to the collection, use and disclosure of his/her personal information is an essential element of privacy protection and must be obtained by all recordkeeping participants.[1] Therefore, the preservation of and access to personal data depends not only on data protection laws, but also on a wider net of laws and moral codes.

Reliable and authentic records:[2] tension with privacy legislation

Privacy and personal data protection legislation conforms with international privacy principles that personal information should only be collected, used or disclosed for its primary or original purpose, and that its use and disclosure for secondary or other purposes is subject to strict limitations.[3] On the basis of this principle, privacy legislative provisions in many countries mandate the destruction or the de-identification of personal information once its primary purpose has ceased, subject to other legal retention provisions. If records containing personal data are destroyed they will never be available for research or disclosure in the public interest. Destruction and de-identification of records affects the integrity and therefore the quality of research data. However, the interpretation of "other uses" or "further processing" in privacy law varies from one jurisdiction to another, as does when and who does the further processing.

From an archival perspective, a prime responsibility of the archivist is to ensure that records are preserved for other purposes that may not be apparent to their primary immediate ones. The question is whether the central privacy principle is sufficient to satisfy the recordkeeping principle of reliable and authentic records that have other uses not envisaged by their original purpose.[4] From a records continuum perspective, which operates on managing the record throughout its existence as a continuous process, archival purposes are not necessarily considered separate from primary purposes.

A record's authenticity has been defined in terms of its elements of identity, which includes authorship, time of action and the matter in which it participates, as well as its

[1] Consent depends on the capacity of the person to consent "unambiguously", and therefore have moral agency. On consent by a patient in the medical context, see McSherry (2004).

[2] There is another potential tension between a record, *inaccurate* in the sense that it may contain inaccurate personal data, but *authentic* in the sense that at the time of its participation in the creating or any subsequent business process the data was deemed to be correct: see further discussion in this section. The clash of these concerns where there is a legal requirement has not been resolved in many data protection regimes.

[3] The principle, ("Purpose Limitation Principle") that personal information should only be used or disclosed for its primary or original purpose addresses the objective of Articles 6 (1) (b) and 7 of the European Directive 95/46/EC. See Waters (2001).

[4] See Miller (1998) who provides an analysis of why the records of a highly intrusive personal nature were not destroyed after German re-unification but rather covered by specific legislation passed by the Federal German government in order to carry out "corrective justice" through the legal system. The German Law on the State Security Service of the German Democratic Republic (STASI) records justified their retention for the purpose of "settling the accounts" with the former East German regime. At the same time the Law protected the privacy interests of the victims of the STASI surveillance.

integrity or completeness.[5] Personal data in terms of a record's identity and integrity involves addressing the following issues:

- Should personal information be de-identified once its "immediate" use has ceased?
- Should personal information that is inaccurate be destroyed, deleted or amended?
- What is the role of recordkeeping participants, including trusted third parties in protecting privacy and the record's integrity?
- Should third party interests, including that of researchers and archivists, be included in privacy legislative frameworks?

Privacy regimes focus on consent to the collection, use and disclosure of personal information in its immediate context, while archival regimes focus on preservation of authentic records for general public disclosure, which may include personal information once it has lost its sensitivity. The retention of personal data ensures that the rights and obligations of those affected by the outcome of a transaction are protected, as well contributes to personal, corporate and collective memory over time (McCalman 2002). Liability arising from incomplete or incorrect information may give rise to damage claims by parties affected. Therefore to prove that incorrect information was provided there needs to be evidence of what was seen by the parties. The deletion of inaccurate personal information can in fact lead to the absence of evidence of the incorrect data used in further action (Laberge 1987–1988). Rather than deleting the inaccurate data, a correction should be made via a notation system.[6]

The role of trusted third parties in protecting privacy is often overlooked in privacy legislation. In the public sector this has been the role of government archival authorities in regulating access and appraisal of records, for example exemptions from privacy legislation for archival authorities or organisations that hold personal data of long-term value. However, in the private sector personal data has yet to develop third party trusted mechanisms.

In the archival sphere, third party archival researcher agreements place the onus of respecting personal information on the researcher. In Europe and Australia human research ethics approvals for research involving human subjects focus on the informed consent of the subjects, which balance the interests of the researchers with the interests of the human subjects.[7] Even voluntary discipline-specific researcher codes of conduct conform to data

[5] The *InterPARES Project* 1 defined record authenticity in terms of the attributes that establish its identity and integrity: International Research on Permanent Authentic Records in Electronic Systems (2001).

[6] Of particular relevance in the light of record integrity is the retention of amended personal information, in Australia's *Freedom of Information Act* 1982 (Cth) s 50(3): "To the extent that it is practicable to do so, the agency or Minister must, when making an amendment under paragraph (2)(a), ensure that the record of information is amended in a way that does not obliterate the text of the record as it existed prior to the amendment". Similarly, the articulation of the 4th Data Protection principle [accuracy and the power to seek rectification] in the UK enactment of Directive 95/46/EC states that the 4th principle is not contravened if the data controller took reasonable steps to ensure its accuracy having regard to the purpose and notation is carried out when the controller is notified by the data subject: *Data Protection Act 1998*, Sch 1(7).

[7] For example informed consent is adopted by the Network of European CNS Transplantation and Restoration (NECTAR) in its ethical guidelines. See Boer (1996). In Australia the *Privacy Act 1988* (Cth) s95 provides that the National Health and Medical Research Council (NHMRC) may, with the approval of the Privacy Commissioner, issue guidelines for the protection of privacy in the conduct of medical research which requires informed consent of data subjects before use of any identified data. Section 95A of the *Privacy Act 1988* (Cth) provides a framework for human research ethics committees to assess proposals to access health information (without the consent of the subject) for research, the compilation or analysis of statistics, or health service management, in order to weigh the public interest in those activities against the public interest in the protection of privacy.

protection legislation.[8] However, researcher codes of conduct for medical and scientific research in particular are often inappropriate when subjects are dead or years have passed since the events concerned (Thomson 2002). The archival notion of "lapse of time" on de-sensitising personal information has been one of the major arguments supporting the eventual disclosure of personal information to third parties in archival regimes. This archival principle is not given due weight in scientific researcher codes of conduct which adopt privacy principles.

Digital archival issues

Preservation of personal data in its digital form, and in particular when used in networked environments, must involve attention to the technical detail of electronic archives without losing a handle on the broader legal and moral issues. These include data matching, that is, the preservation of an identifier, which may identify a person by name, unique number or other means in order to link his/her records across systems and its potential privacy conflict. In the web context, the uncertainty of the extent to which data may identify a person may further deter the preservation of websites or other dynamic records.[9]

Authentication of individuals involves managing personal information that forms part of the identity of a record transaction. Event histories or audit trails of a record's amendment, management and use are also essential for privacy protection, in particular in relation to checking on privacy infringements as opposed to pre-emptive approaches such as authentication. Event histories need to be retained as they form part of the record.[10]

Stronger privacy legislation can however enhance record integrity, for example by minimising unauthorised access to, distribution of and tampering with personal data in electronic networks. In addition "privacy-enhancing technologies"[11] that anonymise personal data for research purposes also support record integrity, if the anonymisation is reversible.

[8] The *Code of Professional Conduct in Socio-Economic Research* (RESPECT) is a voluntary European research code. The RESPECT code is based on a large number of existing professional and ethical codes of practice, together with current legal requirements in the EU. Whilst the RESPECT provisions are voluntary, some of the requirements on which they are based are morally binding on the members of specific professional associations or legally binding on citizens of EU Member States, for example, para. 2.1 Data Protection 2.1.1 h. See The Institute for Employment Studies, University of Sussex, UK et al. (2004). *Micro-Organisms Sustainable Use and Access Regulation International Code of Conduct* (MOSIACC), is an example of a code of conduct for access to and sustainable use of microbial genetic resources. See Desmeth (2000).

[9] For example an Internet Protocol address may constitute personal data if it is reasonably possible to identify the person to whom it belongs. Web harvesting and other automated methods of electronic archiving may have privacy implications, as discovered by the Royal Library of Sweden. See *Sweden and Germany* in section on the EU.

[10] Audit trails are part of "tracking" which is "creating, capturing and maintaining information about the movement and use of records". International Standards Organisation, *International Standard: Information and Documentation—Records Management* ISO 15489-1-2001 Part 1, p. 3.

[11] "Privacy-enhancing products are those that have been designed in a way that aims at accomplishing the largest possible use of truly anonymous data." Commission of the European Communities (2003, p. 16), footnote 26.

European Union, privacy rights and archival exemptions

The European Convention on Human Rights of 1950 as amended in 1998 (European Court of Human Rights 1998) and the OECD *Guidelines on The Protection of Privacy and Transborder Flows of Personal Data* of 1980 (OECD 1980) follow from the principles of *The International Covenant on Civil and Political Rights* 1966. *The European Convention on Human Rights* includes rights related to privacy, family, free expression and fair trial. It was introduced into the law of the United Kingdom in the Human Rights Act 2000, making privacy part of a UK bill of rights.

As a response to technological developments, Directive 97/66/EC (the European Parliament and of the Council 1997) covered the processing of personal data and the protection of privacy in the telecommunications sector. In 1999 the Council of Europe provided guidelines for privacy principles for the Internet (Council of Europe 1999). Directive 2002/58/EC on privacy and electronic communications (the European Parliament and of the Council 2002) has updated Directive 97/66/EC to reflect developments in the markets and technologies for electronic communications services, such as the Internet.

However, the most significant effect on European privacy law has been Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and in the free movement of such data (the European Parliament and of the Council 1995), which took effect in 1998 and required all EU countries to have consistent national privacy laws. Article 6 (1)(b) of Directive 95/46/EC allows further processing for "historical, statistical or scientific purposes", but only when appropriate safeguards are in place. Not all EU Member states have interpreted Article 6 (1)(b) of Directive 95/46/EC in the same way (Commission of the European Communities 2003). Some EU countries use the term "research" rather than "historical", for example Germany, and place the emphasis on scientific research.[12] In most EU legislation there is also further archiving implications in relation to the rectification of inaccurate data by deletion.[13]

Belgium: a continuum model[14]

Belgium's *Personal Data Processing Act* 1992 (PDPA) modified in 1998[15] defines "personal data" as every piece of information regarding an identified or identifiable natural

[12] A brief textual analysis of the articulation of exemptions in EU states by the authors showed that there was no great significance to the use (variously) of the overlapping terms "historical", "archival", "statistical" and "scientific", which may be followed by either "research" or "purposes". "Research" is sometimes an exempt category in its own right.

[13] For example, Austria, *Federal Act Concerning the Protection of Personal Data (Datenschutzgesetz 2000)* s 27 "Right to rectification and erasure. (1) 2 …The obligation to rectify data according to sub-para.1 shall apply only to those data whose correctness is significant for the purpose of the data application [*Datenanwendung*]. … As soon as data are no longer needed for the purpose of the data application, they shall be regarded as illegally processed data and shall be erased *unless their archiving is legally permitted* and unless the access to these data is specially secured. Any further use for another purpose shall be legitimate only if a transmission [*Übermittlung*] of the data for this purpose is legitimate; the legitimacy of further uses for scientific or statistical purposes is laid down in ss 46 and 47." See also s 27 (1): "Every controller shall rectify or erase data that are incorrect or have been processed contrary to the provisions of this Federal Act [*Bundesgesetz*]."

[14] This section has been summarised from notes provided by Hannelore Dekeyser.

[15] Consolidated text of the Belgian law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data as modified by the law of December 11, 1998 implementing Directive 95/46/EC—Unofficial English translation by K. Buyens, updated by Mieke Loncke http://www.law.kuleuven.ac.be/icri/documents/12privacylaw.php (consulted December 2004).

person. Data is identifiable if someone, the data controller or a third party, is able to link the data to a natural person using any reasonable means. The scope of this definition is extremely wide. Under the Belgian law an Internet Protocol address is personal data as it is reasonably possible for an ISP to determine an identifiable person to whom it belongs, even though the archivist may not be able to achieve this.[16] The European Directive 2002/58 on privacy and electronic communications states that the log files of ISPs must be erased or made anonymous when they are no longer needed for the purpose of the transmission. Several exceptions are applicable, amongst others in the interest of national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.[17]

According to the PDPA personal data may only be preserved for as long as necessary to achieve the initial purpose of processing and afterwards all data must be destroyed in principle.[18] An exception to this rule exists for historical, statistical or scientific purposes, in which case preservation is allowed under the conditions set by the Royal Decree of February 13th, 2001.[19] In reality the Royal Decree repeats this principle without imposing any further restrictions. Consequently, the mere preservation of personal data for research does not pose legal problems.

Preservation can form an integral part of the initial processing purposes, which is permitted if the data subjects are informed about this beforehand. Preservation can be a form of "further processing", which is allowed if compatible with the initial processing purposes. Otherwise, the data controller must treat these data just as newly gathered data and inform the data subjects in accordance with the law. However, historical, statistical or scientific purposes are never considered as incompatible with the initial purposes, as long as the conditions set by the PDPA and the Royal Decree of February 13th, 2001 are met whether by the initial data controller or a third party.

As a rule, research should only be conducted on anonymous data, meaning data that cannot be linked in any way to an identifiable person and therefore does not fall within the scope of the PDPA. If anonymous data are insufficient to achieve the research goals, encoded personal data may be used instead, subject to various conditions.[20] When certain

[16] The Netherlands has not taken the strict interpretation of identifiable personal data as in Belgium, and does not consider that in all cases IP addresses are personal data. The Dutch view is that the body processing the personal data has to have the ability to identify the individual via their IP address. An archivist could argue that unlike the ISP he/she does not have additional information to identify a person (Boudrez and Van den Eynde 2002).

[17] Boudrez and Van den Eynde (2002, pp. 75–82) provide an analysis of personal data and the Internet.

[18] "Processing" can be defined as "each action undertaken regarding personal data, including collection, requesting (downloading), storing, availability by means of transmission, etc." The person responsible for data processing is the "data controller", being the one who chooses the purpose and means of processing.

[19] Moniteur Belge, March 13th, 2001, available in French and Dutch http://www.privacy.fgov.be (consulted December 2004).

[20] In practice, many of the issues with the management of personal data contained in records can be mitigated by various permutations of anonymisation, encoding and processing conditional upon procedures by either the controllers or researcher [the last of these issues is discussed below in some detail]. This article concentrates on the tension with fundamental archival principles of authenticity and retaining archives for secondary purposes: the requirement for integrity (International Research on Permanent Authentic Records in Electronic Systems 2001) requires the conceptual stress to be located here. Protecting personal data will often be required at the sub-record level, but needs to be conceptualised in the context of these fundamental issues. Work has continued within InterPARES on these concerns and candidate ways of managing privacy.

categories of sensitive information[21] are involved, more stringent rules apply. It is of minor importance who encodes the data, the initial data controller or a third party, as long as the encoding happens before the research starts. If encoded data is unsuitable for the research goals as well, the original data may be used. The researcher must fulfil the same conditions as before and must obtain the data subjects' explicit consent in writing for the data processing. Again an exception is made when notification is impossible or too burdensome and the Data Commission must be fully informed.[22] Any personal data that has been made public by the data subject himself may be used for research purposes freely. The published research results may not contain any data allowing the identification of the data subjects, unless this information is already public or the data subject consents. A blanket exemption to the conditions set by the Royal Decree is accorded for research conducted by government agencies.

The Belgian approach allows for a continuum view that includes preservation as either part of the original purpose of the data collection or as further processing related to historical archiving.

Italy: historical exemption and codes of conduct

The requirement for the destruction of personal data under privacy law has been modified in Italy by Decree 281/1999 of 30 July 1999, which allows the preservation of personal data for "historical, scientific and statistical research."[23] Although Decree 281/1999 has been repealed by the *Personal Data Protection Code* 196/2003 of 30 June 2003, the provisions dealing with historical, scientific and statistical research have remained substantially the same.[24]

Section 12 of Decree 196/2003 subscribes to the use of deontological and good conduct codes for industry sectors. The processing for historical purposes is covered in a separate section from scientific and statistical research with its own code of conduct. Italy has been the first country in the EU to incorporate a code of conduct and professional practice for the processing of personal data for historical purposes into a national privacy law, in part, in response to a *Recommendation of the Committee of Ministers to Member States on European Policy on Access to Archives* (Council of Europe 2000).[25] The code is based on professional codes of ethics authorised by the Italian Privacy Commissioner with regard

[21] Articles 6–8 PDPA provides extra protection to information related to amongst others political opinions, faith, race or ethnic origin, sexual preference, health and court proceedings.

[22] If the data subject were dead or if the records were over 30 years old this may be a case for '...an exception is made when notification is impossible or too burdensome and the Data Commission must be fully informed.'

[23] In Italy concerns about section 16 of Decree 675/1996 passed to comply with Directive 95/46/EC, which required the destruction of personal data except if needed for similar administrative uses, led to legal changes in 1999 which incorporated section 16 with the preservation of personal data for historical purposes. See Giannetto (2001).

[24] Decreto Legislativo 30 giugno 2003, n. 196, (G.U. 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L)—in vigore dal 1 gennaio 2004—*Codice in Materia di Protezione dei Dati Personali*, ss 16, 98 and 99.

[25] *Recommendation No. R (2000)13 of the Committee of Ministers to Member States on European Policy on Access to Archives*, as well as the Italian Constitution, European Conventions on Human Rights and Freedom, and the International Code for Archivists, provided the framework for the Code of Conduct and Professional Practice Regarding the Processing of Personal Data for Historical Purposes. See Giannetto (2001).

to processing of personal data to be applied equally to researchers and archivists. It includes limited legal sanctions for violations.[26]

The sections in Decree 196/2003 dealing with processing for historical purposes are section 101 which states that personal data collected for historical purposes cannot be used for administrative purposes that are unfavourable to the subject, except if used for purposes in relation to section 11 (which covers the correct processing of personal data), that documents containing personal details can only be used for historical purposes if relevant and indispensable for those purposes, or they may be used if the data have already been disclosed in the public domain either directly by the data subject or by his/her actions. Section 102 deals with the issuance of a deontological and good conduct code to be promoted by the Privacy Commissioner for both public and private persons, including scientific and professional associations interested in using personal data for historical purposes, with particular reference to the collection, use and disclosure of health, sexual or other private matters to be handled with care, and the researcher informing the data subject who may be affected before disclosure. Section 103 specifically relates to the consultation of documents preserved in archives by deferring to Decree 490/2004 (Cultural and Environmental Heritage Code), in relation to access to records held in state archives, historical records of public entities and private archives.[27]

Sections 101–103 of 196/2003 clearly draw from archival and FOI regimes, as well as codes of ethics, and are therefore of particular relevance to arguing the archival case for the preservation and access to personal data on the basis of archival principles built into legislation.[28]

Sweden and Germany: freedom of information and privacy regimes

Sweden has a long history of open access with freedom of information laws going back to 1766.[29] In the Swedish *Personal Data Act* 1998 s 3, personal data is defined as "all kinds of information that directly or indirectly may be referable to a natural person *who is alive*." There is also a specific provision to allow personal data to be retained for longer than necessary for its original purposes. Section 9 provides that "personal data may be kept for historical, statistical or scientific purposes for a longer time than stated in the first paragraph (i)." Para (i) states that "personal data is not kept for a longer period than is necessary having regard to the purpose of the processing". However, in 2001 the Swedish Data Inspection Board discontinued the Swedish National Library's web archiving project because it involved the processing of personal data. The Board argued that specific legislation was required for the collection of personal information from a website for historical and cultural purposes, thus interpreting historical, statistical or scientific purposes narrowly (Boudrez and Van den Eynde 2002, p. 76).

[26] Code of Conduct and Professional Practice Regarding the Processing of Personal Data for Historical Purposes (*Codice di Deontologia e di Buona Condotta per i Trattamenti di Dati Personali per Scopi Storici*, 28 febbraio 2001, Gazetta Ufficiale, Serie Generale, n. 8, 5 aprile 2001). See Article 13 Breaches of the Rules of Conduct.

[27] It should be noted that only private archives that are declared to be of noteworthy historical interest are covered by the Act on Cultural and Environmental Heritage; other private records held in private collections or institutes are excluded from the ambit of this act, but not from the data protection act.

[28] 196/2003, ss 101 (1), (2) and (3); Art. 102 (1), (2), a, b, c. Art. 103 (1).

[29] Constraints of space have prevented direct consideration of the Scandinavian countries' advanced state in both FOI and eGovernment terms.

The Federal archives legislation in Germany is a good example where the effects of the implementation of the Directive remain problematic. The implementation of the Directive, the amendment to the previous *Bundesdatenschutzgesetz* (not enacted until 2003), explicitly does not affect either the *Bundesarchivgesetz* or any extant specific laws affecting the processing of personal data. However, the *Bundesarchivgesetz* explicitly cannot override an obligation arising from other legislation to destroy documents.

There are further issues in German federal law that remain unresolved and they relate to access to information and the point at which custody and responsibility for electronic archives is transferred to archival institutions. "Responsibility" in this context relates to the authentication of archival records and the making of access decisions, which might—incidentally or otherwise—involve the release of personal data. The first issue has provoked lively professional discussions amongst archivists and governmental organisations. The second has only not come to a head because the federal government, unlike a quarter of the state governments, has no freedom of information legislation.[30]

Spain and the United Kingdom: specific archival exceptions and clarifications

Directive 95/46/EC in both Spain and the United Kingdom are relatively straightforward transpositions of the original text that show slight differences in the detail of how archival processing is permitted. The Spanish law specifically reserves what the Directive calls *compatibility* of purpose where the transfer of data is allowed for research, scientific and historical purposes to public administrations.[31] The UK law leaves this to the principle of compatibility,[32] but makes two interesting provisions, ostensibly to promote the integrity of records and to recognise archival processing involved in giving access as of a lesser order than other types.[33]

The UK enacted a FOIA 2 years after the Data Protection Act and the concern has been to keep the regimes as separate as possible: information is either subject to one or the other.[34] It is worth noting that the overall effect on public policy of these two regimes has been to harmonise the processing of digital and analogue material.

[30] The Ministry of the Interior decided in late 2001 not to transpose a draft federal Freedom of Information measure into law.

[31] Organic law 15/1999 on the protection of personal data https://www.agpd.es/upload/Ley%20Org%E1nica%2015-99_ingles.pdf (consulted July 2007).

[32] Clarification recognising the compatibility of the retention of national archives deriving from the business activities of public record bodies by the then Public Record Office was requested and gained at an early stage from the then Data Protection Commissioner (now Information Commissioner).

[33] Data Protection Act 1998, see: http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm, consulted July 2007. This does not, however, resolve the tension between the integrity of archives and the proportionality of processing required by the first of the data protection principles. Archival processing can be held to be compatible with other purposes, but the possibility of it being disproportionate remains to pose a serious challenge to either archival selection policies or the integrity of records. This is an issue only likely to be resolved by case law. The possible clash with macro appraisal is discussed in the next section "General Observations on the EU Framework".

[34] With both personal and non-personal data normally existing and access to them having to be arbitrated at a level below that of the record (or record aggregation), this is also symptomatic of the more widespread challenge posed by privacy to the integrity of records and archives noted in the introduction.

France and the bureaucratic tradition[35]

The French have made more than one legislative initiative enacting the Directive 95/46/EC,[36] apparently symptomatic of different approaches to reconciling conflicting jurisprudence and policy. The latest has specific articles designed to permit public archival purposes and specifically amends archival legislation to do this. Following on from the UK example, the French have also acknowledged some archival processes as being explicitly more permissible than others. This time it is preservation activity that is singled out, *le conservation* being a subset of processing but one explicit in the law and distinct from other types.[37] France has also used the formula of non-profit archival activities rather than specifically public sector ones as the criterion for establishing compatibility of purpose and/or applying the scientific, historical and statistical exemption.[38]

The most striking characteristic of the French law, though, remains the strictness of its privacy stipulations and the lack of a freedom of information tradition.[39] In addition, the French terminology for *les archives*, covering as it does what in many other jurisdictions would be referred to as *records* until or if not identified as archives might be taken as evidence of the application of a continuum viewpoint.[40]

General observations on the EU framework and personal data preservation

Broad generalisation about the impact of Directive 95/46/EC from an archival standpoint is difficult. The Directive tries to provide for similar protections for citizens and a single market within which data processing is harmonised to a degree leaving much detail to be worked out by member states under the principle of subsidiarity. The Directive uses several phrases or concepts, which member states have interpreted differently in fitting into existing jurisprudence, as the above examples will attest.

The most striking and oft repeated phrase is the requirement "subject to appropriate safeguards." Another is the precise articulation of the principle of compatibility. Many member states could have made broader use of the Directive's derogation powers[41] or could have made them more specific in their application to archives or archival processes (such as preservation activity) that may only involve incidental processing of the personal data.

[35] The authors are grateful to Isabelle de Lamberterie for her kind assistance with the preparation of this part of the article. For more detailed exposition of the French position than is possible here, refer to de Lamberterie (2004), and for analysis of the read-over of this subject into the area of identification and authentication technologies, also de Lamberterie (2002).

[36] The *Loi informatique et libertés* of April 2000 has been superseded by the *Loi No. 2004-801*.

[37] Thus, *le conservation* is a subset of *le traîtement* and enjoys a data subject access exemption under Article 32 (iii).

[38] It is not entirely clear at the time of writing how this is to operate in practice, although the text of the new law seems to allow for the possibility of retention in non-public sector archives.

[39] Two measures from the late 1970s established in law the *droit de mémoire* and the *droit de l'oubli* which were in fine counterpoint, but left a number of issues to be resolved by the implementation of Directive 95/46/EC. The first is part of the archival legislation and naturally concentrates on the collective memory. The second relates to the specific right of individuals not to be imprisoned by their own past.

[40] The French usage is similar to that defined by the draft International Council on Archives' terminological database at: http://www.staff.www.uni-marburg.de/~mennehar/datiii/intro.htm, consulted February 2005. There is no established French word for *record*, although some practitioners are trying to establish the concept of *le records management* at the time of writing.

[41] Particularly those under Articles 6[1](b) and (d) and—possibly—7.

Many of the enacted exemptions for archival purposes take the view that it is possible to identify a point when all non-historical processing of personal data has ceased. This at once supports a continuum view of the desirability of identifying the various requirements of the record throughout its existence and denies the possibility of historical purposes being contemporaneous with others if personal data processing is to be allowed.[42]

The extent to which record creators and preservers can rely on article 6 (1)(b) of Directive 95/46/EC for archival preservation of identifiable personal data is questionable if "historical" and other research or archival exemptions have been enacted narrowly to constitute "further processing" of personal data that is not allowable.

A strict interpretation of Article 40 of the EU Directive allows Member states to exempt some processing on the grounds of public access for research purposes and whether the organisation wishing to continue using the information is doing so for a profit motive or not. The archives and library sectors are specifically mentioned. This could be very helpful to the archival case, albeit dependent on a clear dividing line between the private and not-for-profit and government sectors.

In the British legislation this is subsumed within the generic legal concepts of processing and compatible purposes and Mme de Lamberterie makes a plea for French law to take advantage of this for the French research communities (de Lamberterie 2004).

Many of the national examples above major on the position of public archives, while in most member states there is a need to demonstrate compatibility between archival and other business purposes if private archives are to flourish.[43] Public authorities with integral or official archival facilities will find it easier to argue that they comply with this proviso, especially where these have a statutory basis. A commercial company or a private archive is going to find this much harder to establish, and generally preservation strategies are much weaker in the private sector.

Policies on "macro" appraisal, for example, run an enhanced risk of executing a disproportionate retention of personal information.[44] Will this influence archival authorities to sanction the destruction of personal data? As it is likely to be only a policy of an archival authority rather than enshrined in statute, the compatibility of this with the original purposes as well as its proportionality must also remain an open question.[45] Will this place

[42] Further work on the challenges presented by the privacy agenda to various archival methodologies have continued within the InterPARES 2 project.

[43] For example, in Belgium the storage of personal data for later processing by the body responsible for the records has to be compatible with its original purpose, while later processing of records for historical purposes by another body (e.g. the archives) has to take account of the reasonable use and their public nature (Boudrez and Van den Eynde 2002, pp. 81–82).

[44] Archival literature contains a great deal of discussion of the possibilities of appraising the value of either records or business functions at a high level and assigning value—in terms of retention particularly—accordingly. In the digital environment in particular, archivists from a number of different theoretical schools mainly agree that whatever the criteria, this is an inexorable trend. From a privacy perspective, this raises a logistical problem: records of a business function often have predictable patterns of personal data incidence especially where the data relates to the participants in the transaction and therefore having moral responsibilities noted earlier in the records management process. Incidental references, however, would in an earlier age have been picked up as a by-product of a more detailed appraisal process, including sensitive personal data. A separate routine may be now required to confirm the level and type of incidental personal data. This is particularly important as regards sensitive personal data. So, if the intention of macro-appraisal is to conserve appraisal resources, the privacy agenda says otherwise.

[45] Perceived clashes between statutory regimes that have not been completely worked through can come down simply to the chronological sequence: viz. did the supreme legislative authority pass the privacy measure before the archival?

appraisal with the record creators who could argue their appraisal decisions on the basis of their relationship with "original purposes"?

Many jurisdictions have regimes for public archives that assume by statutory default that all records are to be kept unless there is the authority of the National Archivist (or some other legal person) to destroy them. How is this to be resolved with the requirement to cease in many cases to process the personal data? Basically the incidence of personal data as an integral part of the record (and possibly essential to its being seen as authentic) means that there is another statutory default running in the opposite direction.

In general, the common purpose of the archival mission with statistical, scientific and other research communities works well in member states' legislation. Pausing briefly to consider the secondary use of statistical records for archival purposes, it is interesting that no member state apart from Finland appears to have made a specific exemption for archiving census data.[46] The challenge for archivists must be that many research and statistical purposes can proceed without the individuals being identifiable in most circumstances. Integrity and authenticity in the archival senses, however, cannot be compatible with anonymisation. To the scientific community the balance between accuracy and authenticity may be differently drawn, thus it is more acceptable to the scientist for a research dataset to be anonymised than for an archivist.[47]

Researcher and data controller codes of practice

The production of a deontological code of conduct for archivists and researchers as the Italian response to the Recommendation of the Council of Europe, Committee of Ministers seems to be a unique example. Article 27 of Directive 95/46/EC actually prefers codes of practice binding data controllers (such as an archives) rather than researchers. An example of the latter is the draft under discussion between the UK Society of Archivists, The National Archives and the Information Commissioner.[48] The EU *First Report on the Implementation of the Data Protection Directive* lamented the lack of progress made in sector codes of practice covering the whole European single market, noting that only three valid requests had been received for, respectively, the direct marketing, headhunting and telecommunications sectors (Commission of the European Communities 2003). This was

[46] Under s 18 of the *Personal Data Act* 523/1999 and even then subject to objection from the data subject. Outside the European Economic Area, many countries including New Zealand retain their census data. In Australia census data since the first census in 1911 have been destroyed on the basis that data accuracy would be compromised if data subjects knew that their confidentiality has been compromised. A long campaign to reverse the trend in Australia was exacerbated by the privacy lobby. Until 2001 the raw census data was destroyed once statistics had been extracted. *Census information Legislation Amendment Act 2000* (Cth) allowed those participating in the 2001 Census to "opt-in" to have their return retained by National Archives of Australia with an embargo of 99 years to satisfy privacy concerns.

[47] Except where the research, as occasionally in the life sciences, demands the tracking of identity across time and perhaps cannot be achieved by anonymising or coding personal identifiers. It remains to be seen whether the activities under analysis in the scientific case studies in InterPARES 2 will show considerable concern about the privacy of data subjects (including incidental ones) and whether the scientific community sets the same store by authentic records in the sense of their completeness or integrity. ISO 15489 deconstructs "Authenticity" as a factor of "Reliability", "Useability" and "Integrity". The InterPARES 2 intellectual framework substitutes "Accuracy" for the last of these, not least to foster the dialogue with the scientific community.

[48] http://www.archives.org.uk/professionalissues/reviseddataprotectioncodeofpracticeversion6.html consulted July 2007.

despite there being a procedure in place for their agreement at European level.[49] At the same time the report noted encouraging examples of national codes in Germany, the Netherlands and Spain. Although one example of a sector code relates to the press—freedom of press expression is also subject to a specific exemption under the Directive—only the Dutch scientific research code relies on the exemption in Dutch law for historical, statistical and scientific purposes (see Article 10[2] of the Personal Data Protection Act 2000).[50] There are no specific archives sector codes mentioned in the report.

National security: immunity from fundamental right of privacy?

In Europe, the privacy right is separate from and goes far beyond data protection. For example, a judgement in a German case from 1978 adjudicated in the Court of Human Rights included the following statement:

> States may not..., in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate... the danger (is that) of undermining or even destroying democracy on the ground of defending it (Commission of the European Communities 2003, p. 5)

Aside from being unthinkable in the contemporary United States, it is also indicative of the breadth of the fundamental right to privacy in the European Union. Directive 95/46/EC explicitly *cannot* have any impact in the areas of defence and security. Yet there are signs that the privacy right is undergoing some startling development: the principles of proportionality and reasonableness evident in the data protection principles seem to be being pushed back into an area that might have been assumed to be covered by "blanket" security provisions.

Discussions between the EU and the US on passenger name records (PNR) in response to demands from the US Department of Homeland Security have gone to the level of the retention period of the passenger data, the mechanisms for letting the Americans have access to the data, and the fields that will be permitted and those that will not (e.g. ethnic origin and religious persuasion, two of the sensitive personal data categories). The US originally asked to retain the data about EU citizens for 50 years; the final period agreed was 3½ years. It should be noted that exemptions for historical records in the data protection regimes might be unlikely to have much impact if the fundamental right to privacy is invoked.

This may be a defining development. Although the European Commission entered the agreement with the US in the teeth of opposition from the European Parliament, the Section 29 Working Party created by 95/46/EC and some national privacy Commissioners, we ought not to forget that passenger name records of migration, nor that certain information retained under security blankets for long periods in the past have been released to become rich sources of archival information. The question of whether privacy/data protection and freedom of information reduce the chance for these data to survive is open to conjecture.

[49] The authors have nonetheless discovered the existence of sectoral codes intended to be Europe wide or even global, such as the RESPECT code mentioned in footnote 8.

[50] Unofficial translation at: http://www.dutchdpa.nl/downloads_wetten/wbp.pdf, consulted July 2007.

Privacy regimes and the preservation of personal data: Canada, Australia and the United States

The interrelationship of archival, privacy and freedom of information legislative regimes, and the question of which laws take precedence affects the archival case for preserving personal data. The Canadian, Australian and American regimes are a case in point.

Canada[51]

Canada has separate privacy laws for the public and private sectors. The public sector is governed by the *Privacy Act* and *Access to Information Act* 1983. Provisions in the *Privacy Act 1983* and specifically for the federal archives, now Libraries and Archives Canada, provide exceptions for research or statistical purposes, as long as the records have been disclosed by a government body to the national archives for archival purposes, or to a person under specific conditions or transferred to Libraries and Archives Canada by a government authority.[52] The Act does not apply to private records in the national archives.[53]

Canada introduced federal privacy law for the private sector in 2000 largely in response to the EU Data Protection Directive and developments in electronic commerce (Cook 2002). The *Personal Information Protection and Electronic Documents Act* (PIPEDA) 2000 integrates the Canadian Standards Association's (CSA) *Model Code for the Protection of Personal Information* as Schedule 1 and provides exceptions for archives and research to the consent, use and disclosure principles.[54] Principle five states that "[p]ersonal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes." PIPEDA's electronic documents' sections also have the potential to affect the authenticity and reliability of electronic records, in that they relate to access, usability, metadata and authentication.[55]

The *Privacy Act* adequately covers disclosure to the Archives, and further disclosure by the Archives, but leaves the retention of personal information to the minister in charge of

[51] This section is an extract from a paper by Jane Morrison, March 2004. It only covers the federal sector.

[52] Canada, *Privacy Act* 1983, s 8(2) (3). Section 6(2) defines the provisions for access to and correction of active records: "[a] government institution shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible."

[53] Canada, *Privacy Act 1983* s 69(1). Unlike Australia and the US, Canada has to account for "total archives", which is the longstanding tradition of public archival institutions acquiring private records, which until recent changes would not have been covered by Federal privacy law.

[54] Canada, *Personal Information Protection and Electronic Documents Act* (PIPEDA) 2000 s(3) "an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is…(*f*) for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed; (*g*) made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation; (*h*) made after the earlier of (i) one hundred years after the record containing the information was created, and (ii) 20 years after the death of the individual whom the information is about[.]".

[55] Canada, *Personal Information Protection and Electronic Documents Act* (PIPEDA) 2000 s 37.

the institution. PIPEDA has weaker provisions for archival activities. In most of its exceptions, archival purposes have to be assumed to be part of statistical, scholarly study or research purposes, or journalistic, artistic or literary purposes. By adopting the CSA *Model Code* privacy principles (particularly limiting retention) without adequate archival exceptions, the Act encourages records destruction and de-identification.

Australia

In Australia, at the federal level and in most of its states, archival and freedom of information legislation has included provisions on disclosure and protection of personal information that predate privacy acts.[56] Subsequent to the introduction of privacy law, Australian archival and FOI laws have generally taken precedence.[57] Consequently, the general approach in Australian privacy acts has been to create rights, but to implement them through archival and FOI laws.[58]

Australian privacy laws have been extended in recent years to the private sector with many significant exceptions and to specific contexts such as health. As in Canada, the impetus for extending privacy legislation in Australia arose from the October 1998 EU Directive restricting personal information from member countries to other countries unless adequate privacy safeguards were in place. Rather than enacting new legislation, the federal government extended its existing public sector legislation to the private sector through the *Privacy Amendment (Private Sector) Act* 2000. By incorporating national privacy principles (NPPs) into the Principal Act, the *Privacy Act* 1988 regulates how privacy is handled in the private sector nationally.[59] Most state privacy legislation follows the Commonwealth model.[60]

[56] Privacy provisions in Freedom of Information legislation in Australia include for example *Freedom of Information (Miscellaneous Amendments) Act* 1999 (VIC), s 33(1). Privacy legislation in Australian states is as follows: *Invasion of Privacy Act* 1971 (QLD) covers credit reporting agencies and listening devices. The *Privacy and Personal Protection Information Act* 1998 (NSW) applies to the public sector only and excludes state-owned corporations and state investigative agencies. *Information Privacy Act* 2000 (VIC) imposes privacy obligations in respect of the management of personal information across the Victorian public sector. South Australia, Tasmania and Western Australia have versions of Information Privacy Principles (IPPs) as administrative instructions but these do not have the force of law. The *Australian Capital Territory Government Service (Consequential Provisions) Act* 1994 applies the *Privacy Act* 1988 (Cth) to the Australian Capital Territory. Separate privacy legislation for health information is found in: *Health Records (Privacy and Access) Act* 1997 (ACT); *Health Records Act* 2001 (VIC); the Health Information Privacy Act 2002 (NSW).

[57] For example, the Commonwealth public records regime applies to personal information in records that are over 30 years old. In the *Privacy Act* 1988, s 6 (f), Commonwealth records that are defined by s 3(1) of the *Archives Act* 1983, as in the open access period for the purposes of that Act are exempted even if they are not in archival custody. Records are defined as in the open access period in s 3 (7) of the *Archives Act* 1983: "A record is in the open access period if a period of 30 years has elapsed since the end of the year ending 31 December in which the record came into existence."

[58] The Australian Law Reform Commission's review of the *Freedom of Information Act* 1982 (Cth) in 1995 concluded that the Act had been the main vehicle for access and amendment of personal information rather than the Privacy Act, and that the destruction of incorrect personal information was generally not implemented (Australian Law Reform Commission 1995; Waters 2001).

[59] The existing privacy principles in the *Privacy Act* 1988 (Cth) have continued to cover the public sector in the Commonwealth and the Australian Capital Territory, while each state has been expected to have its own privacy act for the public sector.

[60] New South Wales has not followed the Commonwealth model. In the *Privacy and Personal Protection Information Act* (NSW) 1998 s 29 (5) applies to the public sector which issues privacy codes of practice for classes of information, an agency or class of agency, or activity, for example for research, which cover all public sector agencies, including private records deposited in designated archives.

The national privacy principles that affect long-term preservation include the deletion and/or de-identification of personal data once it has served its primary purpose, data accuracy provisions, storage, access, alteration of records, and limits on use and disclosure (Iacovino 2001). In relation to compatibility between archival and other business purposes the objects clause of the *Privacy Amendment (Private Sector) Act* 2000 "recognises ... the right of business to achieve its objectives efficiently" which could include preservation processes such as migration.[61] For public records, personal data that does survive beyond its primary purpose is subject to Commonwealth and state archival legislation which continues to protect personal information for the lifetime of the person by restricting information that has continuing sensitivity usually beyond 30 years.[62] In the private sector there is no exemption for records of a profit-making private archive or a business entity wishing to provide access to older records containing personal information as found in the *Archives Act* 1983 (Cth), unless they are *deposited* in a designated public institution.[63]

Unlike the EU and Canadian federal sphere where privacy law is generally limited to living persons, in Australia there has not been a clear determination on when privacy ceases, for example does it continue after death and for how long, and, if there is a duty of confidentiality does it die with the person? As there is no sunset clause on certain classes of personal information, for example medical information about a deceased person, it appears it may never be disclosed (Savulescu and Skene 2000). However, in some state privacy laws, limits of time are placed on the protection of privacy.[64]

In Australia there are no general exemptions in privacy legislation for access to personal information for historical, scientific, or statistical research, except for health information or temporary public interest determinations. Under the *Privacy Act* 1988 s 80A "temporary public interest determinations", the Privacy Commissioner can make a Public Interest Determination allowing for derogation from a National Privacy Principle, which could be requested for particular records regardless of age for research within specified guidelines. In the *Privacy Act* 1988 s 95, a disclosure of health information for statistical or research

[61] *Privacy Amendment (Private Sector) Act* 2000, s 3 Objects, (b) (iii).

[62] For example privacy continues to be protected through the *Archives Act* 1983 (Cth) under s 33 (1) g: "Information or matter the disclosure of which under this Act would involve the unreasonable disclosure of information relating to the personal affairs of any person (including a deceased person)."

[63] *Privacy Act 1988* (Cth) s 6(1) Interpretation "'record'…*does not include*: (d) a generally available publication; or (e) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or (f) Commonwealth records as defined by subsection 3(1) of the Archives Act 1983 that are in the open access period for the purposes of that Act; or (fa) records (as defined in the Archives Act 1983) in the custody of the Archives (as defined in that Act) in relation to which the Archives has entered into arrangements with a person other than a Commonwealth institution (as defined in that Act) providing for the extent to which the Archives or other persons are to have access to the records; or (g) documents placed by or on behalf of a person (other than an agency) in the memorial collection within the meaning of the Australian War Memorial Act 1980; or (h) letters or other articles in the course of transmission by post." *Information Privacy Act* 2000 (VIC), s 11 (1) (b)–(d), *Health Records Act* 2001 (Vic) s 15 and the *Health Records and Information Privacy Act* 2002 (NSW) s 4(3) c "personal information", provide exemptions for private records that are more than 30 years old, if they are deposited in a public institution as defined by their respective legislation. In the case of *Information Privacy Act* 2000 (VIC) and *Health Records Act* 2001 (VIC) private records held by any "not-for-profit" organisation are exempted regardless of age.

[64] For example, the *Privacy and Personal Protection Information Act* 1998 (NSW) s 4.3 (a) "personal information" does not include "information about an individual who has been dead for more than 30 years." In the case of personal health information in a state archive, the *State Records Act* 2000 (WA) s 49(2) sets a hundred year limit to protecting personal medical information from disclosure, while the French archival law is set much longer at 150 years (see De Lamberterie 2004).

purposes must comply with Guidelines prepared by National Medical Research Council and be approved by the Federal Privacy Commissioner.

Sui generis health records laws passed in Victoria, NSW and the Australian Capital Territory have provisions regarding the secondary and long-term retention of personal health information. For example, *Health Records Act* 2001 (VIC), HPP 4.2 provides that a health service provider must not delete health information relating to an individual, even if it is later found or claimed to be inaccurate, unless permitted by law, or not contrary to a law. Information can be deleted related to a child once the individual attains 25 years or, in any case, 7 years after the last occasion on which a health service was provided to the individual. Health information held by other organisations is treated the same as other personal information in relation to retention.

Therefore, although on the surface Australian privacy laws do not have exemptions to the principle of "further processing" or "secondary uses" on the basis of research, history and statistics, the deference to archival and freedom of information legislation taking precedence (at least in the Commonwealth and Victoria), as well as the use of public interest determinations, and a broad reading of secondary purposes, provide a balanced approach to the long-term preservation of personal data and its protection in the public sector, but are far less clear in the private sector.

United States[65]

The United States has followed a different model from that of Australia and Canada in response to the EU Directive of 1995. It did not respond through legislation but negotiated a "safe harbour framework" with the European Commission in 2000 for the transfer of personal data from Europe to US, under which US organisations voluntarily subscribe to predetermined privacy obligations (Hughes 2001).

It was not until 1965 that the United States Supreme Court articulated a national right to privacy.[66] Historically, individual states have often led the way in the development of more effective records privacy protection.[67] The Privacy Act of 1974 (5 U.S.C. s 552a) prohibits disclosure of individual information to a federal agency or person, except with written approval by the affected person.[68] Under the Privacy Act, only records authorised as relevant to accomplish an agency's purpose under statute or Presidential order can be kept. Section 552(e)4 covers procedures for access, storage, retrieval, retention and disposal. The provisions of both privacy and freedom of information laws are incorporated in the federal Office of Management and Budget (OMB) Circular A-130, which was promulgated as a result of the Paperwork Reduction Act of 1980 (PL 95-511). OMB Memorandum No. M-99-18, written in 1999, expands the provision of privacy protection to web-based documents. FOI has created an affirmative responsibility to release certain types of

[65] Extracted from a paper by Terry Maxwell with additions by the authors.

[66] *Griswold v. Connecticut* (381 U.S. 479).

[67] Stronger state privacy protection may be constrained by overuse of federal pre-emption. Pre-emption is the practice whereby a higher level of government blocks the ability of governments at a lower level from enacting either weaker or stronger privacy controls.

[68] There are, however, several exceptions to this rule. Disclosures by record keepers can occur when federal agencies require information to perform their duties, for statistical research, for certain law enforcement activities, for health and safety purposes to determine a person's last known address, for Congress, and via a court order. Individuals may have access to their own records, and can request amendments to correct inaccuracies, which are relevant to record integrity, if in fact the record is amended by deletion.

documents. However, amendments in 2003 prohibit agency processing of FOI requests from foreign entities.[69]

The United States has also opted for a number of *sui generis* privacy laws.[70] The Health Insurance Portability and Accountability Act (HIPAA), 1996 (PL 104-191) covers both public and private organisations that produce and use health information. However, long-term accessibility of the records is not addressed.

In contrast to the EU, Australia and Canada, the United States has not sought to regulate the information practices of private organisations. However, in certain industries, particularly those engaged in financial, health care, and telecommunications services, government bodies have been given some oversight and access capabilities but these acts provide weak privacy protection.[71] In addition, recent legislation targeting terrorism and drug enforcement[72] have led to broad exemptions in financial and telecommunications acts for law enforcement and counter terrorism investigations.[73]

Conclusion

From the research to date it can be concluded that the EU Data Protection Directive 95/46/EC introduced not total harmonisation, but an extremely full and detailed regime that required many member states to revamp substantially their privacy provisions, but there are important differences in how the archival perspective has been addressed. In some EU jurisdictions there are examples of the fundamental right of privacy overriding the data protection exemption, while in the US increased security fears have led to the opposite trend. Cross-jurisdictional sharing of personal data in the web environment threatens the efficacy of the broader privacy regulatory framework, which in some countries has included freedom of information and archival legislation and the protection from disclosure by professionals and archivists well before the passing of data protection legislation. In the case of the Australian, American and Canadian situation there are very different perspectives that arise from the interrelationship of their public records regimes and the much later, and as yet very immature, private sector privacy regulation.

The recommendations arising from this study include promoting the addition of archival and researcher ethics codes into the privacy legislative framework, as has been done in Italy. That this has not been achieved elsewhere in the European Union is partly owing to the complexity of the issues and the contradictions in other policy areas that need to be balanced. Privacy needs to be integrated with freedom of information and archival regimes,

[69] *Intelligence Authorization Act* of 2003 (PL 107-306).

[70] *Family Educational Rights and Privacy Act* of 1974 (34 CFR Part 99), or FERPA, protects the privacy of student educational records for all schools receiving federal funding.

[71] *Fair Credit Reporting Act* (PL 91-508), *Fair and Accurate Credit Transactions Act* of 2003 (PL 108-159), *Right to Financial Privacy Act* (12 USC 3401 et. Seq).

[72] The *Patriot Act* of 2001 (PL 107-56) expanded the authority for law enforcement and intelligence agency information interception and sharing of wire, oral and electronic communications related to terrorism and computer fraud and abuse. The *Homeland Security Act* of 2002 (PL 107-296) promotes exchange of information regarding terrorism among federal, state, and local agencies and private organisations, but must comply with applicable Federal law on privacy.

[73] The *Telecommunications Act* of 1996 (PL 104-104) s 222c, while extending the prior requirements for privacy of Customer Proprietary Network Information (CPNI), required affirmative customer approval (opt-in) for sharing personal information, except in the case of authorised law enforcement purposes, or for direct business purposes of the carrier or their contractors.

and more needs to be done to promote the preservation of archives by private sector organisations. Even early appraisal decisions may not always get around privacy concerns, but consideration of these issues early is essential for the archival policy agenda, and the Belgian model supports this approach. The research to date also confirms that privacy laws impose limitations on the use of identifiable as well as de-identified data for research purposes. Special arrangements for access to anonymised data that can be re-identified are important access management issues that need to be streamlined. Addressing the deletion of identifying data as a record integrity issue should improve the quality of data available for research purposes. For the future good of archives it is vital that all recordkeepers—creators and preservers—ensure a wide scope of interpretation be given to what is deemed to be permitted "further processing" of personal information where these are additional to the primary purpose of the creator, and that the moral dimension of protecting privacy is not excluded from the regulatory framework.

References

Australian Law Reform Commission (1995) Open government: a Review of the Federal Freedom of Information Act 1982, report 77. Australian Government Publishing Service, Canberra

Boer GJ (1996) Ethical guidelines for the use of human embryonic or foetal tissue for experimental and clinical neurotransplantation and research. Network of European CNS Transplantation and Restoration (NECTAR) Netherlands Institute for Brain Research, Amsterdam, http://www.nesu.mphy.lu.se/nectar/eth.1.html Consulted July 2007

Boudrez F, Van den Eynde S (2002) Archiving websites. State Archives of Antwerp, Antwerp-Leuven

Commission of the European Communities (2003) Report from the commission, First Report on the Implementation of the Data Protection Directive (95/46/EC), COM (2003) 265 Final: http://www.eur-lex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf Consulted July 2007

Cook T (2002) Archives and privacy in a wired world: the impact of the personal information act (Bill C-6) on archives. Archivaria 53:94–114

Council of Europe (1999) Committee of ministers. Recommendation No. R (99) 5 for the Protection of Privacy on the Internet: https://www.wcd.coe.int/com.instranet.InstraServlet?Command=com.instranet.CmdBlobGet&DocId=396824&SecMode=1&Admin=0&Usage=4&InstranetImage=62835 Consulted July 2007

Council of Europe (2000) Committee of ministers. Recommendation No. R (2000) 13 on European Policy on Access to Archives: https://www.wcm.coe.int/ViewDoc.jsp?id=366245&Lang=en Consulted July 2007

De Lamberterie I (2002) Les Actes Authentiques Electroniques: Réflection Juridique Prospective. La Documentation Française, Paris (France)

De Lamberterie I (2004) La Protection des Archives dans la Société de L'information. In: Cornu M, Fromageau J (eds) Archives et Patrimoine. L'Harmattan, Paris, pp 135–162

Department of Foreign Affairs and Trade (1998) International covenant on civil and political rights. Australian Treaty Series, 1980, no. 23. Reprint, Australian Government Publishing Service, Canberra

Desmeth P (2000) Elaboration and diffusion of a code of conduct for the access to and sustainable use of microbial resources within the framework of the convention on biological diversity, BCCM: http://www.belspo.be/bccm/mosaicc/docs/code.pdf Consulted December 2004

European Court of Human Rights (1998) Council of Europe, European Convention on Human Rights, as amended by Protocol No. 11. European Treaty Series, No. 5: http://www.coe.int/T/E/Human_rights/echr_eng.pdf Consulted December 2004

European Parliament and the Council of the European Union (1995) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data: http://www.ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf, http://www.ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf Consulted July 2007

European Parliament and the Council of the European Union (1997) Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector: http://www.eur-lex.europa.eu/LexUriServ/site/en/oj/1998/l_024/l_02419980130en00010008.pdf Consulted July 2007

European Parliament and the Council of the European Union (2002) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector: http://www.eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_201/l_20120020731en00370047.pdf Consulted July 2007

Giannetto M (2001) Principi Metodologici e Deontologie Professionali nel Codice Degli Archivisti e Degli Storici. In: La Storia e la Privacy, Dal Dibattito alla Publicazione del Codice Deontologico. Atti del Seminario di Roma 30 novembre 1999. Ministero per i Beni e le Attività Culturali, Direzione Generale per gli Archivi, Roma, pp 55–90

Hughes G (2001) Our rapidly expanding privacy obligations. Law Inst J 75:55–61

Iacovino L (2001) Identity, trust and privacy, some recordkeeping implications in the context of recent Australian privacy legislative initiatives. In: Convergence, joint national conference. Conference proceedings. Australian Society of Archivists and the Records Management Association of Australia, Hobart, pp 71–90

Iacovino L (2004) Provisions in European Union National Privacy Laws regarding historical/archival/research exemptions by country (Table). Policy Cross Domain Research Team, InterPARES 2 (internal document)

The Institute for Employment Studies, University of Sussex, UK et al (2004) RESPECT project: http://www.respectproject.org/code/respect_code.pdf Consulted December 2004

International Council on Archives (1996) The international code of ethics for archivists, 6 Sept. 1996: http://www.ica.org/sites/default/files/Ethics-EN.pdf Consulted July 2007

International Research on Permanent Authentic Records in Electronic Systems (InterPARES 1) Project (2001) Authenticity task force, final report, 28 October 2001. Appendix: Requirements for Accessing and Maintaining the Authenticity of Electronic Records: http://www.interpares.org/documents/atf_draft_final_report.pdf Consulted December 2004

International Standards Organisation (2001) International standard: information and documentation—records management ISO 15489-1-2001 part 1. ISO Geneva

Ketelaar E (1995) The right to know, the right to forget? personal information in public archives. Arch Manuscripts 23:8–17

Laberge D (1987–1988) Information, knowledge and rights: the preservation of archives as a political and social issue. Archivaria 25:44–50

McCalman J (2002) Privacy and the past. In: Papers presented at, privacy: balancing the needs of researchers and the individual's right to privacy under the new privacy laws. National Scholarly Communications Forum, Round Table 14, Canberra: http://www.humanities.org.au/Events/NSCF/Documents/PDF/McCalman.pdf Consulted July 2007

McSherry B (2004) Ethical issues in healthconnect's shared electronic health record system. J Law Med 12:60–68

Miller J (1998) Settling accounts with a secret police: the German law on the stasi records. Europe-Asia Stud 50:305–350

OECD (1980) Guidelines governing the protection of privacy and transborder flows of personal data: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html Consulted July 2007

Paterson M, Iacovino L (2004) Health privacy: the draft Australian national health privacy code and the shared longitudinal electronic health record. Health Inf Manag J 33:5–11

Savulescu J, Skene L (2000) Who has the right to access medical information from a deceased person? Ethical and legal perspectives. J Law Med 8:81–88

Thomson C (2002) Can the principles of research ethics protect privacy? In: Privacy: balancing the needs of researchers and the individual's right to privacy under the new privacy laws. National Scholarly Communications Forum, Round Table 14, National Archives of Australia, Canberra: http://www.humanities.org.au/Events/NSCF/Documents/PDF/Thomson.pdf Consulted July 2007

Waters N (2001) A comparative analysis of australian privacy laws with special reference to the concept of 'adequacy' for the purposes of the European Union data protection directive. In: Papers presented to The New Australian Privacy Landscape, Faculty of Law, Continuing Legal Education, The University of New South Wales, Sydney

World Summit on the Information Society (2003) Declaration of principles and plan of action, WSIS-03/Geneva/Doc/4-E, WSIS, Geneva: http://www.itu.int/wsis/docs/geneva/official/dop.html Consulted December 2004