BLURRED BOUNDARIES: CAPTURING AND MANAGING PERSONAL INFORMATION IN ARCHIVAL RECORDS IN THE DIGITAL ERA

Dr Elizabeth Lomas, Senior Lecturer in Information Governance, University College London.

ABSTRACT

Over the last decade the role and responsibilities of archivists in managing 'personal' information have shifted dramatically as record creation and capture has moved from paper to digital paradigms. Online collaborative tools have blurred the boundaries between personal and public spaces. In addition ownership is underpinned by a complex network of legislation which comes into play not only dependent upon where the record author sits but on the infrastructure of the software channels through which s/he generates and exchanges information. For example a record author sitting in Europe may generate records through a software company with headquarters in Iceland, hosted within a 'Cloud' in India but with an intended audience in the USA. How then is this set of records passed to the archivist and who owns the records after transfer? This paper will discuss the challenges faced by archivists in acquiring, holding and negotiating access to personal information through time. The discussion is positioned from a UK/European standpoint which provides a particular lens for the work, as Europe has possibly the toughest personal data and privacy legislation in the world. The paper will seek to position this perspective within the context of wider international considerations.

INTRODUCTION

Thank you so much for your invitation to attend and speak at this prestigious event. Today I will be talking about the role and responsibilities of archivists in managing personal papers. This will include some discussion of official recordkeeping as there are not clear cut boundaries between public and private spaces. I will discuss how the expectations placed upon the archivist and archives service have shifted as we have moved from paper to digital paradigms and new legislative frameworks have come into force which require us to alter our practices. I hope to provide you with a sense of the UK and European information management context and how these interconnect to international considerations. The information landscape is still rapidly evolving and this raises many questions which I will posit for our discussion as part of this session.

THE GATEKEEPERS OF THE PAST

When I reflect back to the start of my archival career over 20 years ago and the principles and practices which were in place at this time, they related to a world largely of paper. One of my first positions was as the Archivist of the National Archive of Art and Design at the Victoria and Albert Museum (V&A) in London. I and my colleagues would acquire the personal papers of artists and designers as well as the corporate and charitable records of organisations involved in art and design (Lomas, 2000). In reality, there were not strict divisions between the types of information within these sets of records. Organisational records would contain personal information and personal papers from third parties whilst the papers acquired from artists and designers would often have some business records including commissions and administration for a range of organisations.

These records were most normally accepted as a gift or bequest but also on occasions as long term loans. Loans were accepted, as to make the information available into the public sphere even for a limited time was seen as worthy of the use of public resources in terms of storage and access expenditure. When the Museum acquired these physical records it could assume ownership of the assets it took possession of, subject to the completion of a very simple gift or bequest form returned by the depositor. Rarely were there any disputes regarding ownership. Occasionally the V&A would work to support the national acquisition of items which were the focus of an export case. Within a UK context when 'manuscripts' are fifty years old they can only be loaned or sold overseas provided an export licence is granted. Thousands of individual manuscripts are exported from the UK without public comment (see https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/481913/Export_of_Objects_of_Cultural_Interest_2014-15.pdf). Where a manuscript/archive is deemed by an expert Reviewing Committee to be so closely connected with the UK's history and national life that its departure would be a misfortune, the item(s) is banned from export for a period of time whilst funds are sought to purchase the item(s) for the nation. If funds cannot be raised then the export ban is lifted and the export proceeds. At one time archives were deemed to be of little monetary value but this picture is now changing and therefore there is a growing overseas market for records (Lomas, 1998). The fifty year marker for export considerations means that at present the UK export system has regulated physical items (mainly paper works) and so has not impacted or considered digital information.

The area of legislation we always considered for each acquisition was copyright law as copyright would determine the extent to which the intellectual property rights that resided within the papers could be exploited. Where possible records would be acquired with the copyrights of the archive owner(s) although we accepted that this only ever covered a percentage of the copyright as within any group of papers there would often be writing or photographs from third parties.

The records concerning the Museum's own activities were carefully managed through time (with records management processes) to ensure their preservation as part of the V&A Archives. The V&A is bound by the requirements of the UK's Public Record Acts which require that official records are captured. Whilst there is local government legislation also in place, it should be noted that there is no legislation within the UK determining any requirement to retain personal information for historical purposes (save for that which applies to two very specific types of quasi personal records manorial and tithe records). As such there is an asymmetry between the official and personal archives in existence. The acquisition process for the Archive of Art and Design was somewhat more ad hoc. Acquisitions could only be managed in a systematic way when organisations were still in existence and keen to put in place records management processes. Many archives were acquired when a company closed or on the death of an individual through agreements reached with his/her family. Often the depositors had only a limited knowledge of the archive's full contents as records were rarely accompanied by catalogues. Very occasionally information would be highlighted as either 'confidential' or 'private'. In these circumstances agreement would be reached that the information would be closed for a specified timeframe. In very exceptional circumstances the papers would be placed in acid free packaging and physically sealed with basic descriptions and the criteria for opening placed on the outside of the package. In determining the requirements for closure we listened and discussed this with the depositors as there was no legislative framework relating to access rights. We were the custodians or gatekeepers.

To enable access, in the first instance we would make a description of the acquisition as a whole (the group level) and then subject to resource availability a full catalogue of every item (the physical unit of production) would be made. Access to the archive was granted whether or not a full catalogue had been produced. Items were therefore weighed prior to issuing to researchers in order to minimise the risk of thefts, given that we did not know the full contents of items. This meant that in theory researchers could have accessed personal information which would have compromised or embarrassed an individual. As a publicly funded organisation our goal was to provide access wherever possible – although clearly we would not have intentionally harmed any individual or organisation.

These processes were common to many public archives within the UK. In a Government context records were scrutinised at a more detailed level in order to protect national security. In the early 1990s government information was seldom ever released until 30 years after its creation. This was to protect the career decisions of Ministers and civil servants whilst in post; it was seen to provide a space for enabling free and frank discussion within safe boundaries. Within the context of archives still in private hands access was and still is for the most part determined by the archive owner.

Rarely were there complaints about these processes and liaison with lawyers was exceptionally uncommon. However within a UK context this position changed significantly from the mid-1990s. Two catalysts have necessitated a significant review of archival processes:

- the rise in borne digital information with new tools to access, share and manipulate data in new ways with added commercial and societal value;
- the introduction of new legislation, sometimes as a response to the digital world, which has altered and reinforced perspectives on personal information and access rights relating to information.

In the 21st century these two dimensions have drastically shifted our information landscape and archival practices.

WHERE HAVE ALL THE ARCHIVES GONE? WHO TODAY ARE THE RECORDMAKERS AND RECORDKEEPERS?

With a shift from paper to digital, the nature of a record and the boundaries between its location, ownership and custody have become blurred. The archivist no longer sits as the gatekeeper providing access to information. The role, responsibilities and rights connected to information provision are much more complicated.

Many archivists first engaged with digital technologies as a means to provide access to paper. Initially this occurred through developing online catalogues which provided better search functionality to access the paper records. As the next step digital copies of paper were then provided online. Scanning paper, storing the images and providing access was and is not without costs. Therefore in many instances digital copies are now behind pay walls. In a desire to provide access to information some archives/archivists have signed up to commercial agreements which limit their own freedom in regard to the management and access of information from archives within their care. In hindsight it could have been beneficial for archivists to consider cooperative shared services but then the expectation would have been for information to be made freely available and therefore costs would not

have been covered. Guidance on commercial contracts and past/shared experience has resulted in more robust negotiations relating to more recent digitisation projects.

This shift to online access does now mean that in many instances the archivist/archive service is not in direct contact with a high percentage of users as many will never physically visit the paper archive. Thus the archivist's relationship to many users has altered. Digital formats have challenged paper as they offer the potential for increased search functionality, new uses for information and access to multiple users around the globe. The relationship between the archivist and the user can be enhanced through programmes which allow users to more publicly engage with records through comment, tagging, cataloguing and in some instances uploads of related material. However the question is raised what will happen if no one physically visits the archive? Where digital copies exist The National Archives in the UK has moved some original records from London to salt mines in the North of England. These salt mines provide cheaper storage and amazingly facilitate the right ambient temperatures for paper storage. However, experience has shown that often when digital images exist it can result in increased demand for access to the original record and therefore digital records can add rather than remove service costs. In very rare cases The National Archives has taken a digital copy but not kept the original record. This has been in cases where the original record would not normally have been acquired. Such a decision requires discussion with the Advisory Council on National Records and Archives. Archivists do need to challenge the idea that a digital surrogate replaces an original. In an age of increasing pressure on public finance in the UK context we are asked to review and defend our public value constantly. A critical question is what happens if no one looks at a particular set of original records? Clearly it is important to ensure that collections are managed in line with long term considerations and not linked to short term resource pressures – we know that there are research fashions. However, in Museums there has been a move to deaccession objects and despite earlier ideals that an object once acquired would be kept in perpetuity. Archives are also no longer immune to the idea of deaccessioning despite the fact that it can result in a reluctance by individuals to trust their collections or archives to public care. In 2015 The National Archives did set out a deaccessioning and disposal policy to tackle the issue for archives. This policy encourages the location of alternative places of deposit.

However perhaps the biggest challenge to archives is born digital content which is now the original record. Keeping and managing borne digital records has in my view changed the rules of acquisition and the management of archives through time.

New technologies have changed the way in which key data is created and managed. Across organisations, communities and personal networks, key information is generated through computer mediated communications. Examples include email, SharePoint and a host of Web 2.0 social networking applications, such as Facebook, LinkedIn and wikis. These are critical tools for creating, distributing and saving information. As a result of these tools much more information is created and captured (Brown, Demb and Lomas, 2009). An organisation will still track and control some aspects of these processes within its defined parameters on local networks. However in reality the boundaries between work and home have blurred as technology has enabled flexible working. What is 'business' and what is 'personal' is not always clear cut. An individual will often manage their own personal communications through the convenience of work emails but also through a range of online applications each one of which delivers a different benefit. As the project lead on a research collaboration entitled Continued Communication (2008-2013) the communication preferences in a range of scenarios were surveyed and tested (Ellis, Ridge and Lomas, 2009; Lomas 2013). Different

tools were seen to have different value, for example LinkedIn was valued for reaching professional communities and Twitter for cascading information. Email was overwhelmingly nominated as the favoured tool for work and personal communication. A range of reasons were cited including its ability:

- to reach most audiences;
- to convey both complex and simple messages;
- to evolve communications over time at each participant's convenience;
- to manage a whole range of daily actions including scheduling appointments.

As a result of email, conversational information which might once have been lost is captured. Email can be structured and managed and certain metadata is automatically captured such as the author and date but often one email will deal with multiple issues despite that fact that it may be being used to replace more structured official record sets. In the UK a number of official enquiries have demonstrated this shift in recordkeeping. The Hutton Inquiry which investigated the UK government's evidence and decisions in respect of going to War in Iraq relied on accessing information from email accounts. Moss (2005) discusses the poor recordkeeping and accountability which existed and the extent to which key decisions were tracked in email and indeed in the private diaries of individuals. We have seen in the recent case of Hillary Clinton's use of a personal email account for USA Government business how even those in key positions of accountability can distort their official and personal recordkeeping. In some respects this is not new, as I mentioned previously physical papers often were not neatly divided between work and home lives. However in the digital domain the choices between how and where to communicate have become more fractured with many more channels for communication being selected. The Continued Communication research found that people were making quick decisions on where and how to communicate based on the considerations tabled in Figure 1.

Figure 1: Communication requirements

Communication considerations	**Explanation**
Reach	The physical distance through space that a tool can send a message and the audience potential
Size	The amount of data/information/representations that can be transmitted
Capacity of channel	How much data/information/representations can be transmitted per unit time through the infrastructure
Resource	The cost of transmitting, e.g. the energy expended in transmitting the message
Speed of creation	How quickly the message can be composed
Infrastructure/ equipment requirements	Pertains to the physical structures that need to be in place in order to transmit the message, including any specialist equipment needed
Interoperability	The ability for a message to be accessed across different devices and platforms
Complexity	How easy it is to learn and then use the tool to communicate the message

Control structure/style	How well you are able to form the message as you would like – will it retain tone, clarity etc?
Comprehension	How easy the message is conveyed and understood across the communication channel
Authenticity/ integrity	Capable of ensuring that the message's context and contents will be protected.
Data ownership	The ability to retain rights over the message, to ensure that it is not used for other purposes and can be effectively deleted as required
Privacy	The ability to ensure that the message is viewed only by intended recipients
Security	Pertains to protection against hackers, malware etc

Reproduced from Ellis, Ridge and Lomas, 2009.

Legal cases have revealed this trend to capture key information through a wide range of computer mediated communication tools, e.g. a report by Patzakis (2012) concluded that there was a growing trend for computer mediated communications to form part of the evidence submitted in both civil and criminal cases.

When information is created and captured through computer mediated communications this raises a number of questions and challenged for the archivist. The data ownership and the reality of the record is complicated as it is no longer a single fixed physical entity. The message/information content may be authored by an individual in a personal or employed capacity. That message is created and captured through a piece of software and storage infrastructure. Aspects of the software, storage and authorship may then reside in different parts of the world. For example a record author sitting in Europe may generate records through a software company with headquarters in Iceland, hosted within a 'Cloud' in India but with an intended audience in the USA. This infrastructure enables the information to be transmitted and presented through time by bringing together these components. However some parts of the supply chain may alter, corrupt or break through time. Where the components are brought together the original content/record may be reused, mashed up or linked to other data with other contributors authoring interwoven content to create a new record. To maintain the information through time migrations may be required. Certainly more active management is required from the point of creation and capture which in Europe have led to the rise of the Records Continuum as a management model in preference to the Lifecycle model (Upward, 2005). Whether or not the information is private or public and who owns the information will depend upon the contracts entered into with software and storage providers, the way in which the information is labelled/badged and where and how the information is distributed as it may be considered to have been 'published' or 'made public' depending upon platforms and settings on those platforms. It will also be dependent on the legislative regimes that relate to different parts of the process given that this may encompass legislation from different countries.

This raises a number of questions for the archivist:

- Can there be archival records in a digital age?
  Given the need to migrate digital information through time can there ever be such a thing as an 'original archival record'? An original bitstream can be stored. This is the original record in the eyes of the computer but this was not the way in which the

author saw or understood the content. To understand the record then requires a new skillset for the archivist/user.

- How should we appraisal digital information?
  So much more information is generated and this does require new approaches to appraisal. New systems are being trialled. For example, the USA National Archives and Records Administration has decide to top slice the Government email systems and take the records of key users rather than consider content, the Capstone approach (https://www.archives.gov/records-mgmt/email-management/sample-capstone-approach.pdf). It can be argued that this 'big buckets' approach to appraisal (ie decision making at a very high level) may be seen to provide a transparency for retention and disposal of information which is a better fit for less structured information. In the UK Government records are deleted from email servers after only six months in an attempt to force users to file emails into structured record systems. These are Government records and personal data is captured only as a bi-product. To appraise and capture personal data represents a different challenge. Digital technology potentially allows us to capture a far wider range of individual perspectives and to access it much more effectively than paper paradigms. As such, in 2010 US Library of Congress decided to acquire all of Twitter's tweets from 2006-2010 (https://www.loc.gov/today/pr/2013/files/twitter_report_2013jan.pdf). This captured not only American but international tweets. A 'copy' of these records could be acquired whilst still providing users with access to their tweets on Twitter. Given that digital records are more readily copied it is possible that archives can enter into contracts with individuals far sooner. For example, it would be possible to mirror an author's email systems in order to automatically capture copies of all emails sent and received in real time. Much more research needs to be done on rethinking retention and appraisal techniques particularly in a personal context. We are still at a cross roads in terms of what can be automated. New computer capabilities will enable the granular management of information dependent upon sophisticated rules. However, what can be acquired and how and when it can be used is also dependent on legislative considerations.

- Who owns the archival record, how and when can it be used?
  Given the complex structures for generating record there are issues around who can/should own which parts of the record(s)? As the record is now dispersed across geographic boundaries the legislative regimes which apply are exceptionally complicated. To what extent the archivist can have certainty over ownership will differ depending on the acquisition arrangements. To establish ownership the archivist may need to negotiate not only with the author of the content but others in the digital supply chain dependent upon where and how the content has been generated. We do not have international agreement on legislative requirements and yet this does impact on what and how information can be managed through time. This can both limit and delimit the parameters of the discussion. Critical in an archive context where there are public resources at play is when and how the information can be legitimately accessed. This can be complicated as when data is acquired from a software developer it is necessary to understand the contracts users have entered into and how the contracts have changed at particular points in time. Many social media platforms allow authors to tailor their settings. Furthermore legal requirements depend not necessarily on one software company's headquarters but where its data is located and where the individual authors reside. Just as copyright legislation is slowly progressing

towards international standards so too could other information legislative regimes. However there remain very different national perspectives on the balance between privacy and access.

- Who are the creators and custodians of the information
  The information landscape is complicated. To navigate these boundaries archivists do need to work with a range of information experts. In addition, we can work more closely with users. In fact some of the boundaries between users and archivists are now perforated. We have seen a move in the last twenty years to the establishment of community archives. In addition, the digital domain has enabled us to break down the boundaries between archivist and user, which means we can engage to better manage records through mutually evolved collection policies and management. In digital spaces we can all be participants in the archiving process as record makers and recordkeepers.

These questions need to be answered and understood in the context of the legislative regimes that govern the management of information. However equally there are some moral parameters that can be amended in legislation over the longer term if we as an information profession are clearer in presenting an international voice on information societal needs, opportunities and challenges. This involves reviewing the existing information legislation and what are and should be our fundamental information rights.

WHAT ARE OUR FUNDAMENTAL INFORMATION RIGHTS?

In establishing agreement on information privacy, access, ownership and specific archival considerations we need to look towards established human rights agreements which do contain components related to information agendas. In1948 the *Universal Declaration of Human Rights* (UDHR) set out by the United Nations General Assembly in Paris on 10 December 1948 laid out fundamental human rights which encompassed rights relating to free speech, ownership and privacy. The UDHR was drafted by representatives with different legal and cultural backgrounds from all regions of the world, and ratified by the United Nations General Assembly in Paris on 10 December 1948. The United Nations continues to hail this as a common standard to live by for all peoples and all nations. The rights related to privacy, property and speech have a bearing on the management of information and are therefore worth citing in full.

> Article 12 defines a right for privacy:
> "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."
>
> Article 17 defined property rights:
> "Everyone has the right to own property alone as well as in association with others. No one shall be arbitrarily deprived of his property."
>
> Article 19 confirms the rights to freedom of speech
> "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

However, what each of these articles means in practice is determined by laws and the exercise of justice at more localised regional and national levels. At an international level there has been an acceptance that moral norms differ and therefore the application of the Convention in practice is complicated. Within the USA these principles are conveyed in fairly absolute terms. However, in a USA context the right to freedom of speech is of paramount importance as it is enshrined within the American Constitution and therefore whilst there are confidentiality laws for business and privacy laws for individuals, the case law has come down on the side of greater openness than in European contexts.

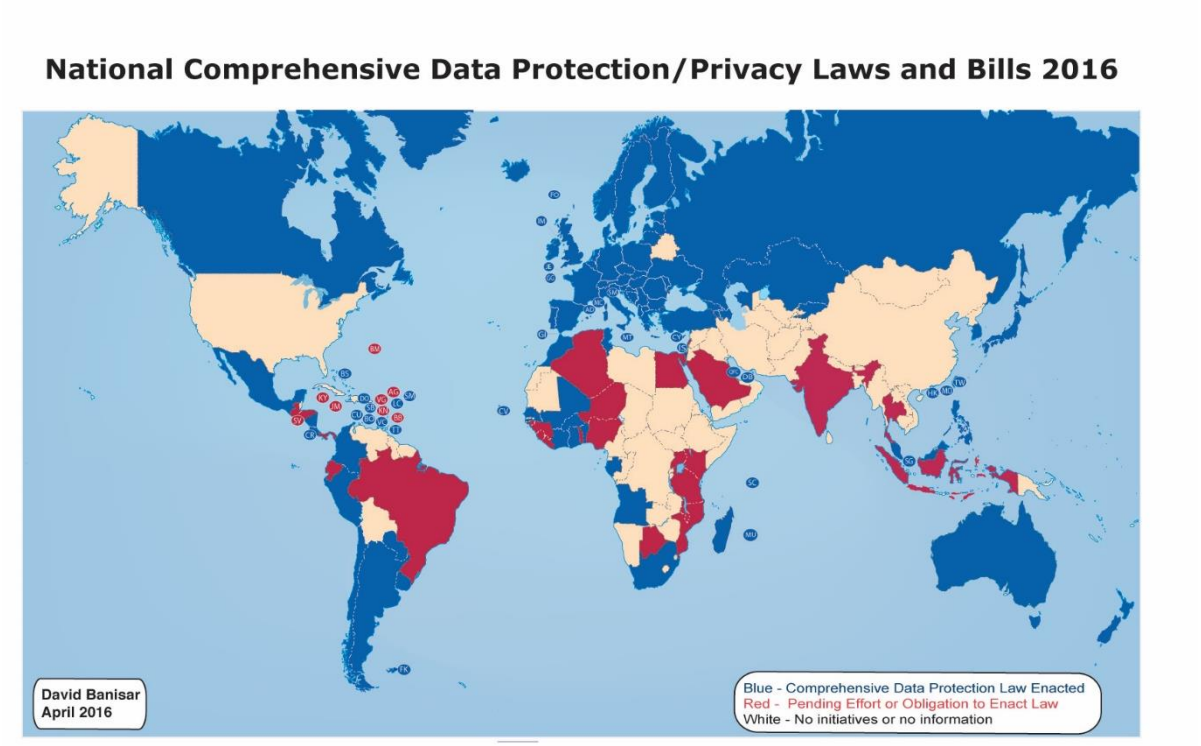
Within the EU context the principles of the UN Convention were ratified by a European Convention on Human Rights which came into force in 1953. The European Conventions qualified the Rights set out by the UN. For example the right to privacy exists provided that individuals are acting in accordance with law and that the rights to privacy are not undermining the functioning of a democratic society. This means that there exists a blurring of the boundaries between the state's right to interfere with citizens' privacy. Within the EU as separate nation states we do not agree on privacy parameters. Within French legislation there is a much greater division between public and private life. As such France's President Mitterand's extramarital affair and his health scares were kept secret during his lifetime. However after his death they were made public partly through legal actions. In France, organisations cannot monitor employee email whereas in the UK this is legitimate provided there is a known monitoring policy in operation. From the 1960s legal remedy in respect of the EU Convention can be sought through the European Court of Human Rights but this is slow and expensive. However it has had some impact at national levels. Those cases heard at this level have influenced national decisions. For example, Princess Caroline of Monaco won a landmark ruling from the European Court of Human Rights to protect her right to privacy. The decision prevented the media from publishing images of her private life. This has influenced national decisions. In the UK context we see as a result a number of superinjunctions (or 'gagging order') being imposed by the courts which have prevented the UK media publishing stories on the private lives of celebrities. Google has had to respect these decisions. Google search engines in the UK block this information. However, as a UK citizen sitting in London I can still go to the USA Google search engine and locate this information although I cannot disseminate it. Thus the European and USA positions remain in conflict as there are different tipping points between privacy and access.

David Banisar provides a mapping which he updates regarding different information rights laws. This delivers a high level visualisation of those countries who provide privacy (Figure 2) and privacy (Figure 3) regimes (http://home.broadpark.no/~wkeim/foi-list.htm).

Over two thirds of the world's nations do have legislation across these domains. However whilst the map includes many countries it is to be noted that the picture is neither complete nor uniform. For example both the UK and Brazil provide some privacy and access regimes but the legislation differs significantly. In fact every nation has their own legislative and differing framework despite the existence of the UDHR.

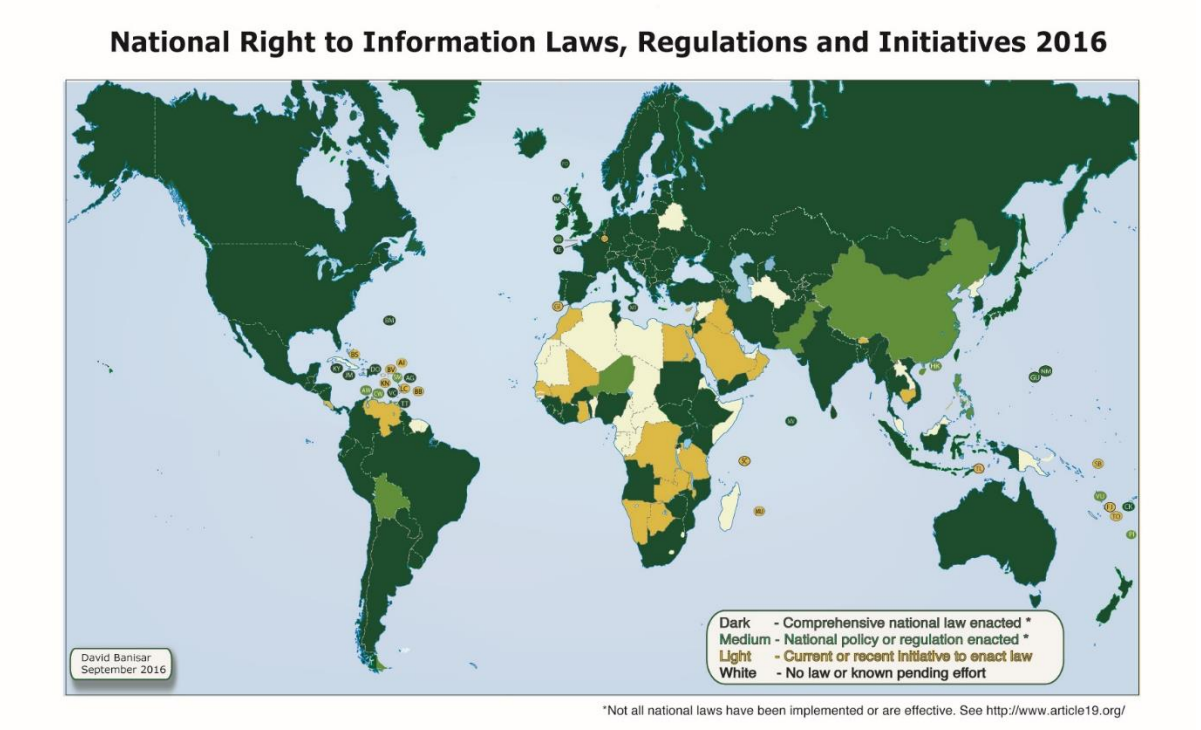
Within the EU there is a patchwork of legislation which delivers privacy and ownership legislation as well as remedy against defamation or libel most of which operates at a national level. Also at a national level is some specific legislation which deals with information held on computers or certain specified types of information. At an EU level in addition to the human rights legislation is specific legislation on protecting personal data.

Figure 2: Mapping of worldwide data protection and privacy laws by David Banisar



Reproduced with the kind permission of David Banisar.

Figure 3: Mapping of worldwide information access regimes by David Banisar



Reproduced with the kind permission of David Banisar.

EUROPEAN UNION APPROACH TO PERSONAL DATA

Within the context of the EU personal information is any information relating to a living individual and this is governed by data protection legislation. It must be noted that it has in rare instances been extended to cover the information of deceased persons, e.g. in cases brought by families about deceased persons where for example the medical information has a family bearing. The UK has had data protection legislation in place since 1984. The legislation was established to enable personal information relating to living individuals generated on computers to be shared for trading purposes. In 1995 an European Union directive (Directive 95/46/EC) was passed which established the parameters relating to the good management of personal information relating to living individuals, regardless of its format. The Directive related not only to public organisations but private concerns including companies, charities and any entity processing personal data. The Directive was then enacted through national legislation which in the case of the UK was the Data Protection Act 1998. This legislation extended its reach to include paper and digital records. The legislation was significant as it challenged the processes for enabling access to information within archives, particularly where the contents were unknown. Although personal information was not caught by the legislation unless it was deemed to be part of a 'relevant filing system' the meaning of this has been challenged on a number of occasions.

The Data Protection Act 1998 has eight key principles. At the heart of the legislation is the concept that all personal data relating to living individuals must be obtained and processed fairly and lawfully. In other words the processing must be in line with the reasonable expectations of the individual it concerns. A special exemption was made for 'research purposes' to enable archives to retain personal information without explicit consent. Where information is deemed to be 'sensitive' then stricter justifications for processing must be met. Sensitive data is classified as information concerning:

- racial or ethnic origin;
- political opinions or other beliefs;
- trade union membership;
- sexual life;
- mental or physical health;
- offences committed or allegedly committed; and
- details of proceedings for offences committed or allegedly committed.

The categories of sensitive data reflect EU citizen concerns regarding information which they deem should be private and confidential. This list potentially differs from concerns on other continents. Individuals have the right to request access to their own personal information and very few exemptions to these access rights exist. Under the current legislation individuals can ask that inaccurate, damaging or distressing information is amended, blocked, erased or destroyed.

Information must be managed securely and safely. Best practice requires organisations to consider conduction privacy impact assessments, e.g. for new IT systems that manage personal data. Critically personal data must only be transferred outside the European Economic Area if that country ensures an adequate level of protection. As a result of this requirement Safe Harbour agreements were negotiated establishing the arrangements for appropriate levels of protection outside of the European Economic Area, e.g. agreements were established with Argentina, Canada, Guernsey, the Isle of Man and the USA. However

in the latter case there has been a significant challenge concerning sharing data with the USA through the case of Max Shrems.

Max Shrems is an Austrian lawyer. As a student Shrems became interested in Facebook's apparent ignorance of EU data protection laws and therefore undertook research on the subject. A request to Facebook for his own personal data revealed hundreds of pages including posts which he thought had been removed. Following the revelations from Edward Snowden in 2013 that the USA security services does monitor social media information he was concerned about access to and the use made of his information. He complained to the Irish Information Commissioner. Facebook's EU headquarters are in Ireland and therefore this was the legislative domain in which Shrems has in effect signed a contract for using Facebook. Shrems failed to get a satisfactory resolution with the Irish Information Commissioner and therefore he progressed his case to the European Courts. He was attempting to stop Facebook's EU data being transferred to the USA on the basis that USA legislation and Facebook specifically do not provide sufficient protections to prevent third party interference. In 2015 as a result of this action the Court of Justice of the European Union found that the USA Safe Harbour Agreement is not suitably robust and data transfer should be reviewed. The impact of this decision called into question more generally the sanctioned use of USA software by EU organisations in cases where personal data is managed. New arrangements regarding the privacy of EU data in the USA have now been negotiated and continue to be the subject of discussion. Aspects of Shrems' legal battle remain ongoing in Ireland and also in Austria where Shrems invited Facebook users to join his case as a class action relating to deletion rights.

The EU direction of travel in terms of legislation is towards greater privacy and additional rights for data subjects regarding their personal data. Although in the UK there has been moves towards 'deemed consent' which requires people to opt out rather than opt in to data usage. However in May 2016 a new Data Protection General Regulation was passed which strengthens privacy legislation and personal data rights. This comes into force in May 2018. Despite the UK decision to vote to leave the EU, as the UK is likely to still be a member of the EU in 2018 when the legislation comes into effect it will automatically apply in the UK. This Regulation includes the 'right to be forgotten' although there is a derogation for archival purposes. The definition of archival purposes and archival services are still under discussion. In addition this means that a greater percentage of information may be lost before it makes it into a formal archive service. However, potentially archives should be providing a better consultation service regarding the retention of personal data for historical reasons. In addition this does present challenges about how we achieve deletion in a digital age where information is held and embedded in multiple locations.

A key impact of the data protection legislation has been the challenge of managing access versus privacy when personal data is concerned.

ACCESS TO INFORMATION

Within the EU personal data rights govern a wide range of organisations. However, access rights exist for the most part only in relation to public authorities. There are a number of campaign groups seeking to extend these boundaries and develop manifestos on openness given the important role information does provide in underpinning the functioning of a mature ethical society (e.g. http://www.opengovernment.org.uk/). In terms of legislation the EU has legislated for access to environmental information in the context of public bodies through the Aarhus Convention. Environmental information is seen to concern natural capital

and its use or misuse can impact locally and globally. It also covers the built environment. Separately EU nations have made their own decisions regarding legislating for access to information more generally.

In the UK the key piece of legislation is the Freedom of Information Act 2000 which provides the access regime for information held by UK public sector bodies). Scotland also has a separate piece of legislation the Freedom of Information (Scotland) 2002 Act which covers Scottish public sector bodies. These Acts are intended to promote a culture of openness and accountability amongst UK public sector bodies by providing people with rights of access to the information they hold. The legislation is retrospective.

Under the terms of the legislation all persons who make a request for information to a public authority must be informed whether or not the organisation holds the information requested. They need not see the actual record only a version of the information.

As well as providing information when requested, the Act also places a duty on all public bodies to be proactive in the release of official information. To this end, public bodies must adopt and maintain a publication scheme that details the classes of information it will regularly publish. The publication scheme is a guide to the types of information routinely published by the organisation, and therefore consists of classes of information rather than a list of individual documents.

Information can be withheld from release where certain exemptions are deemed to apply, these include commercial confidentiality, information classified as personal information under the terms of data protection legislation, information supplied under a legal duty of confidence and information supplied under the terms of legal professional privilege. Some exemptions are subject to a public interest case being established, i.e. it being in the public interest that the records are withheld. When records are deemed to be historical records – which has now been changed to twenty years old whereas previously this was set at thirty years – some exemptions fall away, e.g. commercial confidentiality. However national security and the personal data rights remain and are considered absolute exemptions, i.e. no justification is required.

As the personal data rights are absolute exemptions the personal data is normally withheld under the person it concerns has died. This can be legally challenge. In a court scenario it is considered whether the release of personal data would cause ‘damage’ or ‘distress’ and what the public interest in the release would be. There would need to be a very strong public interest in the release in order to override the personal data considerations. However, archivists are risk averse and on that basis err on the side of closure when there are conflicting concerns. It is clearly easier to close records and then review them upon challenge whereas once opened the position is somewhat irreversible. However whereas once a public sector archivist would shut records of private owners simply upon that individual(s) request this is no longer the case. Private owned information is only personal data if it is information very specifically about a living individual. Requests for access to information which is not deemed to be personal data may be subject to release. This therefore would include information about a private owners family members if those persons are deceased. A small number of private owners have therefore withdrawn records that were previously held on loan by public sector archives.

Corporations and charities are required to deposit key records such as accounts and annual reports which are then available but these organisations need not answer information requests as it would be deemed too burdensome. At a surface level individual accountability in the UK is fairly minimal as there is no mandatory ID system. Tax information must be provided but unlike the Norway legislative system this information is exempt from public scrutiny. However there are concerns about Government surveillance which in the UK align more to US processes than other European national models. In 2000 the Regulation of Investigatory Powers Act was passed and there have been attempts to extend this. Telecommunication companies are required to keep all user records for specified periods. Legislation of this nature has been described as 'a snooper's charter'. Within the UK there is a surveillance culture in terms of extensive CCTV surveillance in public places. This is generally supported as a mechanism for reducing crime. However Edward Snowden's revelations do impact on public perceptions regarding surveillance. The extent of monitoring has come into question in the library domain in the USA and UK where it has been claimed that Government agencies have wanted access to readers' information. Librarians have claimed this is an invasion of privacy and freedom as it is to be argued that you are not what you read, ergo to read a book about terrorists does not make the reader a terrorist.

New agreements and international cases have changed the nature of information holding. Confidentiality and privacy are complex domains and the parameters move. Perhaps the most notable archival case in recent years is that of the oral history Belfast Project in Boston College library which collected Irish Republican Army and Loyalist perspectives on the so called 'Troubles' in Ireland. The accounts were sealed and assurances given that they would not be released until after the death of the individual unless that individual consented. However as part of a murder inquiry by the British Government despite being deposited in the USA a number of these accounts were successfully subpoenaed (King, 2014). This has undermined the process of assurances for retained records confidentially which will impact history. Whilst this was a criminal investigation we know that attitudes to crime do change through time and indeed nations already differ in perspectives to crime. Therefore it is debatable whether the records should have been released. However this case demonstrated that national contexts can be overridden. No longer can immoveable assurances be given in regards to confidentiality.

INFORMATION AS AN ASSET

Information is now recognised as an asset with a capital value. A survey by Western Digital this month, reported in the Daily Telegraph, claimed that the average consumer values their own data at £3241 with men putting a higher value on their personal information than women http://www.telegraph.co.uk/technology/news/12012191/How-much-is-your-personal-data-worth.html. Yet relatively few people pay for data services which increases the opportunities for companies to get users to sign up to harvesting data provided a service is free. Personal perspectives on what individuals will pay in terms of information services are changing. However from a commercial standpoint it is clear that certain kinds of information bear a price tag, e.g. insurance companies have sold accident data to personal injury lawyers and the data of pregnant women has been deemed of value to retail concerns.

> "By and large, the story of web advertising and ad companies and networks is a story of organizations aggressively and unapologetically tracking and intruding on people for years."
> https://utcc.utoronto.ca/~cks/space/blog/web/AdblockingAndMorality

This month the UK information commissioner started to investigate WhatsApp data sharing with Facebook its parent company which has clearly been instigated for commercial advantage but may conflict with individual ownership rights. As well as information potentially having a price tag there are significant costs to properly managing information particularly personal information. From 2008 the UK Information Commissioner Richard Thomas started to describe personal data in interviews as a toxic asset being both a 'toxic liability' as well as an 'asset'.

There are clear tensions regarding the appropriate use and reuse of information and the boundaries between a range of services. In the UK, the reuse of public sector information is now formally regulated and this impacts as to how archives are reused through time. Archives have not traditionally been money making concerns but as there are increasing pressures on public finances the archives does need to more actively consider the parameters of commercial exploitation. So this raises a further question what can and should archive services charge for and commercially exploit?

IN CONCLUSION

Information is an asset but also a source of responsibility. Archives did historically hold data behind defined walls but in a digital age the boundaries are blurring. As resources are depleted there may be new commercial pressures and conflicts for archivists to face. Archivists need to be clearer on their moral parameters so they can defend themselves from resource pressures but take advantage of commercial considerations as appropriate. We can benefit from the increased recognition that information is an asset. Whilst it is a significant challenge to manage records through time and over dispersed locations, it is important that we both recognise and seize a leading role in terms of the many opportunities that exist. These include:

- the opportunity to acquire, appraise and catalogue/tag records in new ways through automation and greater user engagement.
- the opportunity to access and reuse information in exciting new ways.
- the opportunity for archives to have a commercial and social role in the use and reuse of information.
- the opportunity to engage with a wide range of information professionals in harnessing and solving the grand challenges that face us.
- the opportunity to underpin and evolve a moral information rights landscape and thus to play a lead in shaping international information rights law.

Creating international understanding on the appropriate use of information will be a long journey. However archivists have longstanding international collaborative networks – we are good at talking, sharing expertise and reaching consensus. Therefore we can play a key role in shaping nations' moral consciences about the appropriate use and reuse of information. So I would like to end with the call for us to re-envisage our own professional codes of ethics in order that we have a clear moral compass to lead the international information rights agenda and shape new legislation.

Thank you for listening to me today.

References

Brown, M., Demb, S. R. and Lomas, E. (2009) Continued communication – maximising the potential of communications: the research and outputs of a co-operative inquiry, Delivered as

a keynote by E. Lomas. *Proceedings on the International conference on managing information in the digital era*, Botswana, 14-16 October 2009, pp.3-21.

Ellis, B., Lomas, E. and Ridge, M. (2009) 'Continued communication – maximising the business potential of communications through Web 2.0'. *Proceedings of Online Information*, London, 1-3 December 2009, pp.17-23.

Iacovino, L. and Todd, M.(2007) '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. Archival Science, 7(1), pp.107-127.

King, James (2014) 'Say nothing': silenced records and the Boston College subpoenas', *Archives and Records*, 35(1), pp.28-42,

Lomas, E. (1998) 'The Ones That Get Away? Archives and Export Legislation in the UK', published in *Business Archives Principles and Practice*, 75, pp.13-30.

Lomas, E. (2000) A guide to the Archive of Art and Design. London and Chicago: V&A and Fitzroy Dearborn Publishers.

Lomas, E. (2013) *An autoethnography exploring the engagement of records management through a computer mediated communication co-operative inquiry*. Northumbria University.

MacNeil, H. (2005) 'Privacy, liberty and democracy', in Behrnd-Klodt, M. and Peter Wosh, P. eds., *Privacy and confidentiality reader: archivists and archival records*. Alpha Publishing House: Chicago, pp. 67–81.

Moss, M. (2005b) 'The Hutton Inquiry, the President of Nigeria and what the Butler hoped to see', *English Historical Review*, 120 (487), pp.577-592.

Patzakis, J. (2012) *Overcoming potential legal challenges to the authentication of social media evidence*. Pasadena: X1Discovery.

The National Archives (2015) *Deaccessioning and disposal: guidance for archive services*. OPSI: London. Available at: http://www.nationalarchives.gov.uk/documents/Deaccessioning-and-disposal-guide.pdf (Accessed 1 September 2016).

Todd, M. (2006) 'Power, identity, integrity, authenticity, and the archives: a comparative study of the application of archival methodologies to contemporary privacy', *Archivaria*, 61, pp.181-214.

United Nations General Assembly (1948) *Universal Declaration of Human Rights*. United Nations: Paris. Available at: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf (Accessed 1 September 2016).

Upward, F. (2005) The records continuum. In: McKemmish et al. (2005) *Archives: recordkeeping in society*, p.205. Centre for Information Studies, Charles Sturt University: New South Wales.

Wisser, K.M. & Blanco-Rivera, (2016) ‘Surveillance, documentation and privacy: an international comparative analysis of state intelligence records, *Journal of Archival Science* (2016) 16(2), pp.125-147