10

Right to Information

Elizabeth Shepherd

'Right to information' (RTI), 'access to information' (ATI) or 'freedom of information' (FOI) has been adopted by countries around the world to enable the rights of citizens to freedom of opinion and expression, which is a prerequisite for human rights. In 1948, the United Nations Universal Declaration of Human Rights Article 19 stated the fundamental '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' (United Nations, 1948, sec.19). In 1966, the International Covenant on Civil and Political Rights also declared that the right to freedom of expression 'shall include freedom to seek, receive and impart information and ideas of all kinds' (United Nations, 1966, sec.19). The right to information has frequently been linked to trust in public discourse and to enabling accountable and open government. Access to information establishes a right for individuals to seek information held by public authorities, often in a manner defined by the law, and generally subject to exemptions for such things as national security, defence, international relations, police investigations and privacy (Shepherd, 2015, 717).

Recordkeeping professionals in corporate and public organisations provide access to records for internal business use to support current activities, as well as ensuring access to records needed over the longer term for the study of cultural heritage and the history of communities and families. In addition, in the accountability domain, records can be used to hold individuals, officials and corporations to account, both internally and externally. Providing access to reliable records is commonly cited as a necessary prerequisite for

accountability, transparency, and good governance. Transparency International (Pope, 2003, 19) asserted that 'when we campaign for greater access to information we must at the same time campaign for improved records management. There seems little point in having access to information that is chaotic and unreliable'. Archives have been called 'arsenals of democratic accountability' (Eastwood, 1993; Iacovino, 2010) and this chapter will examine the recordkeeping role in providing access to records so that individuals can exercise their 'right to information'. It will consider four different aspects of access to information: national archives and records legislation; secrecy and privacy; responsive release of information by governments under freedom of information; and proactive release of information under open government policies. It will reflect upon whether these aspects together provide citizens with 'a right to information' and therefore whether such a right can be said to exist in practice. Unofficial routes to information access, such as whistleblowing or unauthorised disclosure by activists, will not be covered in this chapter.

ACCOUNTABILITY, TRANSPARENCY, GOOD GOVERNANCE AND RECORDKEEPING

Three terms are commonly associated with the right to information: accountability, transparency and good governance. As Herrero asserts (2015, 4), 'Access to Information is not only a fundamental human right but also a key instrument contributing towards transparency and accountability to build more open institutions'. We can think about accountability as the 'requirement to perform duties, including financial and operational responsibilities, in a manner that complies with legislation, policies, objectives and expected standards of conduct' (IRMT, 2009, 5). Meijer (2001) identifies three phases in the process of accountability (the information phase, the discussion phase, and the sanction phase). He sets

out the accountability processes which follow from a ‘trigger’ event, which encompass identifying an accountable person, outlining the situation or action for which the public authority needs to account, specifying the accountability forum or setting within which the process of accountability takes place, identifying the relevant criteria for making a judgement, and setting out and implementing sanctions. Records can document the accountability events and causes, and allow sanctions to be implemented and audited, although Hurley (2005) cautions that ‘effective recordkeeping is a necessary, but not a sufficient, condition for accountability’. Hurley identifies some recordkeeping roles required for accountability, including regulatory and enforcement functions and service and enabling functions. For O’Neill (2002) reductive accountability leads to an audit culture, whereas intelligent accountability leads to good governance.

Transparency is a wider concept which includes making public affairs open to public scrutiny so as to enable citizens to understand the actions of their governments. Florini tells us that transparency is a continuum, ‘at one extreme, nothing is hidden. All government files are open to inspection by anyone wanting to see them, and meetings are always public. At the other, secrecy reigns supreme’ (2002, 4). Transparency is therefore a prerequisite for, but not the same as, accountability (Florini, 2007). Chapman and Hunt express the relationship thus: ‘a commitment to transparency forms an essential part of the process of accountability’ (2006). Transparency represents a policy and culture of openness which allows parties equal access to information thus improving information asymmetries between the state and its citizens, although the practical implementation varies considerably from democratic to more authoritarian states.

FOI is often considered a necessary part of transparency, given that such scrutiny cannot easily be conducted without access to the official records of policy-making and its execution. However, O’Neill (2002) presents a more nuanced argument given the growth of

public distrust in politicians and the state, despite greater openness and transparency, leading her to suggest that transparency and openness are not unconditional goods, as they are so often presented, and saying 'transparency certainly destroys secrecy: but it may not limit the deception and deliberate misinformation that undermine relations of trust' (O'Neill, 2002, lecture 4, sec.1). As O'Neill points out, digital technologies spread information and misinformation equally efficiently. In other words, access to trusted information may be more important than transparency, and trusted information derives from records which are authentic, reliable, accessible and useable.

Transparency has been described as 'the key to better governance' (Hood and Heald, 2006) which is often seen as a benefit of open government policies. The World Bank (2007, i) defines governance as 'the manner in which public officials and institutions acquire and exercise the authority to shape public policy and provide public goods and services'. Anticorruption measures including 'reforms to strengthen the accountability and transparency of state institutions' promote good governance (World Bank, 2007, v). Open government takes this idea a step further by asserting a participatory democratic approach 'in which the influence of the people could be brought to bear at all stages of the decision making' (Robertson, 1999, 21). Openness 'goes beyond access to documents to cover such items as opening up of processes and meetings of public bodies…concentrating on processes that allow us to see the operations and activities of government at work' (Birkinshaw, 2010, 29).

Recordkeeping throughout the continuum plays a significant part in providing accountability, transparency and good (or more open) government. In Meijer's phase model of the accountability process (2001), records allow for the production of information and evidence which support the investigatory phase of the accountability process, records are created to document the discussion phase and they capture the decisions made about sanctions, which in turn allow citizens to check that sanctions were properly enforced.

Without reliable recordkeeping, accountability would not be a trusted process and it would not be auditable. Historical accountability can be provided through key recordkeeping activities, in particular archival appraisal, that is, the selection of records for permanent preservation. There are various analyses in the archival science literature (including Hurley, 2002, 2005; Avery and Holmlund, 2010) of the recordkeeping role in accountability following statutory obligations for the selective preservation of records, even sometimes in cases when the record creators sought to destroy records. When the accounting firm, Arthur Andersen, unlawfully destroyed records relating to the firm's relationship with the collapsed energy giant, Enron, in 2002 apparently with no recordkeeping intervention, accountability was impeded. The so-called Heiner Affair in Australia in 1990 developed when the newly elected Queensland Government shredded the records accumulated by a retired magistrate, Noel Heiner, who had been investigating alleged abuse at a youth centre, a scandal which the government believed (rightly) would damage its reputation and which it sought to conceal. Since the records were subject to public archives law, they could not be destroyed without the permission of the State Archivist, which was sought and given, leading to a crisis in the Council of Australasian Archives and Records Authorities and the Australian Society of Archivists over ethics and professional accountability. Should the archivist only be concerned with historical value when undertaking appraisal or also with the value of records for accountability and transparency in the present? Should the archivist follow the interests of their employer or pursue some greater idea of professional and public accountability?

Transparency and accountability by making public affairs more open to scrutiny rely on the systematic creation and capture of records, their proper organisation so that they provide evidence of transactions, their selection and preservation for an appropriate length of time in a trustworthy recordkeeping system, and their retrievability when needed. Good governance is encouraged by more open systems. Trust in government and openness are

enhanced by responsive release of records under legislative regimes such as FOI and proactive release by government of open information about the conduct of public business. If information released is to be trusted it must originate in a trustworthy recordkeeping system. The rest of this chapter will explore the legal and policy frameworks and the recordkeeping role in the creation, preservation and provision of access to records and data which together constitute an essential underpinning of the right to information.

ACCESS TO PUBLIC RECORDS: NATIONAL ARCHIVES AND RECORDS LEGISLATION AND SERVICES

Following the upheaval of law, administration and governments in 19th century Europe, came the emergence of national identity, sovereign nation states and national archives. Citizens were given the right to access public archives for the first time: as Duchein (1992) said, 'the notion that research in archives was a civic right was increasingly recognised'. *L'archives nationales* was established in France by state decree in 1794. *Archivo Historico Nacional* was founded in Spain in 1866. In the UK, the Public Record Office (PRO) Act 1838 established for the first time in law public access to central legal and court records, extended to executive records from government administrative departments under an Order in Council in 1852 (Shepherd, 2009). Centralised provision for public access to public records ('created by a government or a department of government in the course of the business of government') was made in the new searchrooms built in Chancery Lane, London from 1851 onwards. The Public Record Office Act 1877 established a system for the transfer of records from government departments to the PRO and allowed records dated after 1715 and 'not of sufficient public value to justify their preservation' to be destroyed (UK Committee on Departmental Records, 1954, 17). Schedules of records for destruction were

drawn up by a Committee of Inspecting Officers. A further Act of 1898 extended the destruction date back to 1660. National archives legislation in many countries in 19th century Europe established a public right of access to records of governments for the first time.

By 1950, the record generating activities of two World Wars, the extension of the state machinery, and 'the invention of such devices as the typewriter and the duplicating machine' exposed weaknesses in the public records systems established in the UK and in other countries (UK Committee on Departmental Records, 1954, 5). For example, 120 miles of records in UK government Departments awaited transfer to the PRO. A Committee was established, chaired by Sir James Grigg (UK Committee on Departmental Records, 1954, 2, 6), 'to review the arrangements for the preservation of the records of government Departments', on the premise that 'the making of adequate arrangements for the preservation of its records is an inescapable duty of the Government of a civilized state'. Its main recommendations were enacted in the Public Records Act 1958. The 1958 Act took a big step towards ensuring public access as it required public records selected for permanent preservation to be transferred to the PRO when they were no more than 30 years old and to be made publicly accessible there, usually when they were 50 years old (reduced to 30 years under the Public Records Act 1967). The standard closure period is gradually being reduced to 20 years, following a review in the light of the UK Freedom of Information Act 2000.

Coppel (2014, 246), however, reminds us that 'there is an important legislative distinction between the obligations in relation to the preservation of public records and those in relation to the access to such records. Generally, the framework given by the public records legislation has been retained for the preservation of records, whilst the Freedom of Information Act 2000 controls the ability to access such records'. Most countries with national archives and records legislation include provisions for a public right of access to government records after a specified closure period, typically 20 or 30 years. However, in

some countries the right of access under archives legislation is being replaced by FOI legislation which enables requests for information of any age. Nevertheless without systematic archival preservation, public access will be impossible. If no additional resources are provided for recordkeeping activities under FOI then the routine archival work of selection for permanent preservation which will underpin access after a stated period may be abandoned in favour of responding to FOI requests for specific records or information. Records provided in response to an FOI request may or may not be selected for permanent preservation. Archival preservation and public access under FOI do not result in identical rights to information.

Other parts of the Anglophone world established different access traditions through archives services. In North America, a 'public archives tradition' developed alongside a 'historical manuscripts tradition' (O'Toole and Cox, 2006, 53, 55). The historical manuscripts tradition emerged from state historical societies, beginning with Massachusetts in 1791. State archives departments were established in the wake of the Public Archives Commission in 1899, starting in 1901 with Alabama: the state archives network was eventually completed in 1978 with New York (Shepherd, 2009, 9-10). According to O'Toole and Cox (2006, 53), the public archives tradition in the USA 'assumed that government authorities at both the local and the colony-wide levels, as representatives of the whole community, would be creators and maintainers of records', to ensure legal rights for all citizens. In 1934 legislation was passed which established the US National Archives as an independent federal agency. The first Archivist of the United States, Robert Connor, was appointed. Construction began on a building to house federal records and provide access to them. The National Archives began to accept record transfers from federal agencies in 1935. In 1949 the service was renamed National Archives and Records Service (NARS) as it took on responsibility for current records of government, which was reflected in updated

legislation in the Federal Records Act 1950. In 1984, the National Archives Act established the National Archives and Records Administration (NARA) as an independent agency. The legislation established a closure period of 30 years for federal records.

The Canadian archival tradition evolved differently from those in Europe and the USA (Shepherd, 2009, 13-14). In Canada, government archives preserved not only the official records of the state, but also private and other records, creating 'total archives' which were embraced within the official mandate of many publicly funded cultural agencies (Wilson, 1982). The acquisition of copies of archives relating to Canada but held elsewhere was an important part of the early 19th century archival endeavour, initially in the provinces of Quebec and Nova Scotia (Millar, 1998). In 1872 Douglas Brymner was appointed to preserve the archives of the Dominion of Canada. The Public Archives Act 1912 allowed the Public Archives to acquire 'public records, documents and other historical material of every kind', that is records relating to the Dominion, provinces and municipalities of Canada, both government records and historical archives, all of which were important in documenting the historical identity of Canada (Millar, 1998). By 1968, archive services were established in all Canadian provinces and archives were also started in the Northwest Territories and the Yukon in the 1970s, although only Ontario had a full scale records management programme (Swift, 1982-83). In 1987 the Public Archives was renamed the National Archives of Canada. The creation of a unified Library and Archives Canada in 2004 (under the Library and Archives of Canada Act) provided a new model of public access to information, seldom seen at national level, where the user need for information regardless of source overrode the traditional distinction between records created by government (held in national archives) and collections of published materials (held in national libraries).

In Australia, soon after federation in 1901, there were proposals to establish a Commonwealth Archives (Shepherd, 2009, 15-17). The first official archive was the

Australian War Records Section established in 1917, which was incorporated into the Australian War Memorial in 1925. National archival developments began again in the 1940s, with the establishment of the War Archives Committee in 1942 and the appointment of government archivists in half of the Australian states (McKemmish and Piggott, 1994). These were gradually enshrined in law, beginning with Tasmania's Public Records Act 1943, followed in 1960 by the Archives Act in New South Wales. In 1944, the appointment of an Archives Officer in the Commonwealth National Library was the precursor to the Commonwealth Archives Office, eventually founded in 1961. The Commonwealth Archives Office became Australian Archives in 1974. The Commonwealth Archives Act 1983 established, among other things, a public right of access to Commonwealth government records after 30 years. Following amendments to the Act in 2010, the access period for Commonwealth records is being reduced to 20 years.

Many countries enacted national records and archives legislation in the second half of the 20th century, ensuring the preservation of and public access to archives. UNESCO drafted a *Model Law on Archives* in 1972 and published guidance (Ketelaar, 1985), which stated that 'freedom and liberty of access to archives constitutes a right of every citizen'. This right was often enacted through national archives legislation. The International Records Management Trust published a Model Records and Archives Law in 1999 which made a clear link between proper management of current government records and reliable and trustworthy archives (IRMT, 1999). A further wave of archival legislation in the early 2000s focused on updating of legislative provisions, in the light of changes in government services such as privatisation but also responding to the new demands of digital records. Many Acts, such as the National Archives of South Africa Act 1996 and the National Archives Act of Malaysia 2003, sought to provide for the preservation and use of the national archival heritage through public access and also for the proper management of current records. Increasingly national archive services

were mandated to take a role in the current records and information management of government, as well as the preservation of access to its archival heritage. Some, such as the Public Records Act of New Zealand 2005, went as far as to state the larger principles which lie behind national archives: enabling government to be held accountable, enhancing public confidence and trust in the public record, enhancing cultural heritage and national identity, as well as providing for a public right of access to records.

SECRECY AND PRIVACY: KEEPING INFORMATION CLOSED

On the contrary, other legislation emerged during the 20th century which sought to keep information closed. From the end of the 19th century, legislation was enacted which prohibited public access to some types of government information, designated official secrets. In the later 20th century, laws preventing access to personal information about individuals, so called data protection or privacy legislation, were passed. Secrecy and privacy legislation is designed to prevent public access to records and information on the grounds of harm to the state or to the individual. Recordkeepers are an important operational part of the secrecy and privacy processes, that is, of preventing access to information.

Secrecy

Birkinshaw (2010, 76-77) reminds us that while the UK Parliament exercised its right to information in a variety of ways from the late 18th century, including by means of government publication of reports and evidence from Royal Commissions and annual reports to Parliament by different state agencies, government controlled what information came into the public domain. As government grew, keeping information confidential became more

difficult. The UK for the first time 'provided for the prosecution and punishment of unauthorised disclosure of official information' in the Official Secrets Act, 1889 (Birkinshaw, 2010, 82). The Act was considered somewhat ineffective and a new statute, in 1911, dealt more firmly with leaks and disclosure in a period of foreign threat, espionage and suspicious activities. The broad scope of the Official Secrets Act 1911 endured until the global availability of information and its easy access in the 1980s, together with some high profile publication of secret government information, led to the breakdown of traditional approaches to government controls of information and the repeal of the Act. Pope (2003) suggests that a 'preoccupation with secrecy' is common in many countries with a history of colonial rule and an inheritance of 'administrative systems and officials obsessed with secrecy', as well as in developing and emerging democracies, such as in Eastern Europe.

Many British Commonwealth countries adopted the UK Official Secrets Acts or their provisions from 1889 onwards, including Canada, for example. India adopted an Official Secrets Act in 1923. Malaysia also adopted UK provisions in its Official Secrets Act 1972. Birkinshaw (2015, 381) considers the UK Official Secrets Act 1989 'the first significant concession by central government towards relaxation of official secrets laws', since only a few specified classes of information were protected from unauthorized disclosure (relating to security and intelligence, defence, international relations, prevention of crime, and information entrusted in confidence). Some countries have replaced official secrets with legislation aimed at increasing national security and information control in the face of terrorism and security threats, such as Canada's Security of Information Act 1985. The introduction of such legislation has been criticised for reducing government transparency and seems to run counter to more general moves towards openness. By the 21st century, official secrets were generally limited to a fairly small number of specific instances and the emphasis

moved from keeping official information closed to a widespread presumption of openness and encouragement of information reuse.

Privacy

There is, however, one type of information which is still considered closed, that is personal data about individuals. Privacy legislation gives data subjects (usually limited) rights over the processing of their own personal data and regulates the creation, processing and retention of personal data and records. There are significant national and cultural differences over privacy and protection of personal data. The greater availability of data about individuals held in a form which could be computer processed in data banks and data centres led to concerns over the proper protection of personal data in the 1960s and 1970s. The USA enacted a Privacy Act in 1974 to control the collection, use, and sharing of information in order to protect the privacy of individuals identified in federal information systems. In Canada, the Privacy Act 1985 provided Canadian citizens with a right to request access to and correct their personal information held by a federal government institution, subject to some exceptions. Australia likewise introduced a Privacy Act in 1988 which set out Information Privacy Principles to regulate the handling of personal information by federal agencies and some private organisations and to allow individuals to correct information about themselves.

The first UK Data Protection Act 1984, which came into force in 1986, brought the UK into line with the requirements of a European Directive on data protection which had to be enacted in each European member state. In the EU, privacy laws are generally entitled data protection and apply only to living people. The UK Data Protection Act 1998 extended the data protection regime which had applied only to records in electronic form to all record

formats. The Data Protection Act sets out eight data protection principles, including fair and lawful processing of personal data for a specified and lawful purpose, data controllers having to be registered and some protections for the rights of data subjects. The UK Act imposed a duty on those holding personal data about living people to comply with the eight data protection principles, to register with the Data Protection Registrar (now the Information Commissioner) and to allow data subjects access to the data and, if necessary, to correct it. Different countries have different cultural attitudes to personal information: Nordic countries regard personal tax and salary data as open but most other countries regard personal financial data as intensely private.

The privacy principles raise some ethical dilemmas for recordkeepers for example, access to data about third parties for research, or the accessibility and use of personal records in cases of historic child abuse, regime change and human rights abuses, which are not easy to resolve. Archives have been challenged to protect sensitive personal data about individuals involved in cases of historic abuse in institutional settings, including children's homes, residential schools, church institutions and adoption agencies. Many countries have now set up historical reviews of institutional settings where children and young people were subject to abuse, to investigate the accusations of survivors and their families. For example, in Australia between 1910 and 1970, many Indigenous children were forcibly removed from their families, 'taught to reject their Indigenous heritage, and made to adopt white culture. Their names were changed, and they were forbidden to speak their traditional language. Some were adopted by white families, and many were placed in institutions, where abuse and neglect were common' (Australians Together, 2015). A government report on what had happened, *Bringing Them Home*, gives a voice to many of the survivors in a very personal way, albeit anonymised. The inquiry took public evidence 'from Indigenous organisations and individuals, State and Territory Government representatives, church representatives,

other nongovernment agencies, former mission and government employees and individual members of the community. Confidential evidence was taken in private from Indigenous people affected by forcible removal and from adoptive and foster parents. Many people and organisations made written submissions to the Inquiry, including many who also gave oral evidence' (Commonwealth of Australia, 1997, 16). There are now questions for recordkeepers about the continuing preservation and access to all these records, in particular where family members want access to records about themselves and their siblings or parents, whom they may be trying to trace. Often their requests are turned down on the grounds of the privacy of the other individuals involved, thus preventing some survivors accessing their own records (and thus their stolen lives) in full.

In Scotland, The Shaw Report (Scottish Government, 2007, 3) considered 'the systems of laws, rules and regulations (the regulatory framework) that governed residential schools and children's homes', 'against the background of abuse suffered by children in residential schools and children's homes in Scotland between 1950 and 1995'. The review reported that a significant obstacle in finding out what had happened was poor recordkeeping in the past and present difficulties in identifying and accessing records which did exist. For instance, 'some potentially significant records in archives were closed' and 'there was no legal requirement for local authorities and organisations to help by giving access to information. Some were helpful; some were less so' (Scottish Government, 2007, 5). The Review identified 'an urgent need to take action to preserve historical records, to ensure that residents can get access to records and information', including a review of public authority recordkeeping under the Section 61 Code of Practice on Records Management under the Freedom of Information Scotland Act 2002 and the 'permanent preservation of significant records held by private, non-statutory agencies that provide publicly funded services to children' (Scottish Government, 2007, 7). It recommended that 'voluntary organisations,

religious organisations and local authorities, working in partnership, should commission guidance to ensure that their children's residential services records are adequately catalogued to make records readily accessible'(Scottish Government, 2007, 7). Recordkeeping issues are critical to such historic enquiries and recordkeepers find themselves in difficult situations in trying to preserve confidentiality and the privacy of different data subjects and yet ensure access to the records needed for the public good.

Increasingly, researchers and policy makers want to use individual-level data produced by government bodies for a variety of public policy, education and health improvement research projects. Access to personal data by accredited researchers under controlled conditions such a safe havens and secure sites may be negotiated, for instance under national schemes such as the UK Administrative Data Research Network (ADRN, 2015). Linking data together can provide richer sources for analysis than a single dataset created by one government agency. Data must first be de-identified using good practice guidelines which seek to guarantee and secure individual rights to privacy and confidentiality of the data, such as the UK Information Commissioner Office's Code of Practice on Anonymisation (UK ICO, 2012). Anonymised data can then be aggregated and linked in different ways, such as different cohorts in a single set of data or different datasets about the same individuals (for example, on educational outcomes and health). However, the possibility of de-anonymisation and re-identification through linked data raises privacy concerns.

The recent 'right to be forgotten' introduces another twist in the story. As a result of a court case in 2014, Google Spain's search engines and access to third party data was made subject to the EU Data Protection Directive on personal data processing. A consequence is that data subjects are now allowed to require the removal of their names and of personal data from Google searches and links, a so-called 'right to be forgotten' (Birkinshaw, 2015). This 'censorship' of personal data has been controversial.

RESPONSIVE RELEASE OF GOVERNMENT INFORMATION: ACCESS TO AND FREEDOM OF INFORMATION

Freedom of information concepts date back as far as Sweden's Freedom of the Press Act 1766, but FOI legislation has only been widely adopted in the early 21st century. In some countries rights of access to information (RTI) are enshrined in the constitution or a Bill of Rights, although in many countries RTI is brought about through primary legislation to give citizens freedom of information (FOI). Several phases or 'waves' of adoption of FOI have been identified, beginning with the USA (1966). The second wave in the 1980s included Canada (1983), Australia (1982), New Zealand (1982). The UK (2000) was part of a third wave, including Ireland (1997), South Africa (2000), and much of Eastern Europe (Shepherd, 2015, 716). More than half the number of existing FOI laws have been adopted since 2000, while other countries have drafted or discussed FOI but not yet fully enacted the legislation (eg. in Kenya, Botswana, Ghana). By 2006, seventy countries had access to information legislation and a further fifty had made some moves towards it. By 2014, over 100 countries had FOI legislation (50 in Europe, a dozen in Africa, 20 in the Americas and Caribbean, more than 15 in Asia and the Pacific, two in the Middle East) and the number is still growing (Banisar, 2016).

Often FOI is a part of complex web of laws regulating information access, adopted for a variety of reasons. FOI is rarely established by a single piece of comprehensive legislation: often it interacts with, contradicts or is complemented by other legislation concerning privacy, data protection, human rights, health and safety, and the environment. It is not a single universal concept and has some very different characteristics in different cultural contexts and legal jurisdictions. Sometimes, as in the UK, it was part of a cultural and

societal shift from a more secretive closed society where access to government records and official secrets was restricted and controlled, to a more open one in which access to information is seen as a civic right. FOI is often the focus of campaigns by the media and civil society groups, such as the Campaign for Freedom of Information in the UK. FOI is sometimes linked to modernising government, new public management and good governance. FOI is sometimes envisaged as a constitutional right in new democracies or as a part of public sector reform in developing countries required by funding bodies (such as the World Bank or the International Monetary Fund). FOI is also seen as a strategy for deepening democracy and increasing government accountability to its citizens and as a tool of anticorruption. Once enacted, FOI has rarely, if ever, been repealed, although a few governments have attempted to limit its use by, for instance, the introduction of charges.

Although FOI establishes a statutory right to access government information, it does not in itself guarantee free and unlimited information access. The legislative rights and the mechanisms by which these rights are implemented differ. In some countries legislation may be enacted but never used, or written so as to prevent access, for instance through excessive exemptions. FOI may be contradicted or limited by other pieces of legislation, such as data protection or privacy laws which prevent the release of personal data, as discussed above. In case of threats to national security, information access may be restricted and FOI may be suspended, weakened or overruled. Even when FOI legislation has been fully enacted, a number of operational requirements are needed to make it useable. These differ in detail from jurisdiction to jurisdiction, but include appeals tribunals, regulatory authorities, reporting mechanisms, publication schemes, access protocols and request systems, time limits for responses and appeals, improved recordkeeping systems and training for government staff in request handling. Government and organisational culture may obstruct access: culture change in government is often needed to ensure sufficient awareness of the legislation and

regulations by public officials. Bureaucratic system failures, more than secrecy, can often inhibit public information access. Advocacy is needed to ensure that citizens understand how to exercise their new rights. In some jurisdictions, access is effectively restricted by excessive delays, for example if there is no statutory time limit for responses, or by excessive fees for making applications or receiving information. Some governments favour providing free access to government data for commercial exploitation, rather than seeking to recover access costs from business.

Birkinshaw (2010) points out that information is not neutral, its 'control, use and regulation' are exercises in power. Examples of information asymmetry between governments and their citizens abound, such as police 'stop and search' powers or investigations into historic abuse in institutional settings. Governments control the FOI system even in the most open regime by creating and holding the information which might be made accessible. Politicians and officials can resist disclosure or introduce delays in releasing information, although media coverage, appeals systems and sanctions discourage this. Governments are frequently viewed as secretive and untrustworthy. Poor recordkeeping systems can contribute to a lack of trust, by making information deliberately inaccessible or inadvertently hard to find, resulting in failures of searches to retrieve information and in records which are incomplete, unreliable or missing.

There has been debate over the chilling effect of FOI on record creation. FOI is said to encourage public officers to make decisions without making an official record, by oral agreements and the use of non-official channels of communication, such as private email accounts. Archivists and historians have debated whether FOI leaves behind 'empty archives' (Flinn and Jones, 2009). Governments may be creating fewer and less reliable official written records as a result of the degradation of centralised registry systems and cultural moves to more informal structures of policy-making, rather than as a result of FOI. Fewer government

records may be captured and preserved because of the failure to manage digital records systems efficiently, resulting in uncontrolled recordkeeping. Arguably the ease of digital records creation and storage is leading to more records being created and preserved in multiple versions. Public and private organisations with poorly managed digital records systems often fail to destroy records which are no longer needed and potentially expose themselves to legal requirements for recovery or the risk of unauthorised disclosure. UK research has suggested little evidence of the chilling effect on 'the thoroughness and frankness of official advice' or on the quality of UK government records, in spite of the 'powerful myth … which is hard to eradicate despite the lack of evidence' (Hazell, Worthy and Glover, 2010, 13, 256). Officials were 'confident that the quality and thoroughness of submissions had not changed' and that recordkeeping had not been adversely affected by FOI (Hazell, Worthy and Glover, 2010, 263).

The UK Freedom of Information Act 2000 exemplifies the important link between records management and the ability of citizens to retrieve reliable and trustworthy information under FOI. UK public authorities need to know what information they hold and to manage and retrieve information effectively in order to respond to FOI requests within the statutory time limit of 20 days. Records management practices were therefore explicitly promoted as essential to a public authority's ability to comply with the Act, formally recognised by Parliament in a Code of Practice on Records Management. The Code stated that 'Freedom of information legislation is only as good as the quality of the records and other information to which it provides access. Access rights are of limited value if information cannot be found when requested or, when found, cannot be relied upon as authoritative' (UK National Archives, 2009, 4). The Code has enabled the regulator, the Information Commissioner, to intervene where public authorities were found to be failing to meet expected standards of good practice in records management.

FOI in most jurisdictions has limited effects on the private sector, since it generally only applies to government or public institutions (unlike data protection or privacy laws which tend to apply to personal data regardless of where or by whom it is held). As governments privatise services, enter into public-private partnerships or co-opt third sector bodies to provide services to citizens, non-governmental institutions are increasingly responsible for public services. And yet, these institutions often fall outside of FOI boundaries. FOI requires resources to operate efficiently and is vulnerable to resource reductions and cuts in an austerity era. Some politicians have even argued that the legislative force of FOI would no longer be needed if more government information was published proactively and made open.

OPEN GOVERNMENT AND OPEN GOVERNMENT DATA: PROACTIVE RELEASE OF DATA

Good governance, open government and open government data are closely related concepts. Although there is no single agreed definition of open government data, it has been described as ‘data that meets the following criteria; accessible (ideally via the Internet, … without limitations based on user identity or intent), in a digital machine readable format for interoperation with other data and free of restriction on use or redistribution in its licensing conditions’ (UK Cabinet Office, 2012, 8). Among its significant characteristics, government ‘open data and content can be freely used, modified, and shared by anyone for any purpose’ (Open Knowledge Foundation, 2012) and is not restricted by privacy concerns. It can be reused for research, civic or personal interest and commercial purposes. However, open government data is not the same as FOI, since proactive data release relies on the government to decide which data can be released. Under FOI, requestors make the choice of which

information to ask for. Given that it is difficult to fully anticipate what requestors want, since many are pursuing specific interests, or are single issue activists or journalists following a particular story, FOI reduces the information asymmetry (by placing control with the requestor) in a way that open data may not.

Halonen (2012) notes that 'the open-data movement did not originate in a vacuum' but has grown from a long tradition of access to and reuse of public information, some of which is set out in the preceding sections of this chapter. The Public Sector Information (PSI) European Directive (2003) introduced a new era of reuse of government information by researchers (Cerrillo-I-Martínez, 2012), based 'on principles of accountability and transparency on the one hand and innovation and economic growth on the other hand' by 'creating jobs and stimulating innovation and at the same time increase transparency and accountability of the government' (Janssen, 2011, 451).

The UK government has been prominent in the open data movement. In 2010, data.gov.uk was launched, 'a web portal that provides a single access point to thousands of data sets held by different public bodies, freely available for any type of use' (Janssen, 2011, 451). Public Data Transparency Principles were published in 2012 (UK Open Government Data, 2015), the Open Data Institute was set up and an Open Data White Paper published (UK Cabinet Office, 2012). UK government has published open data, including data on the environment, towns and cities, health, the economy, transport and government spending, such as requiring local public authorities to publish monthly all spending over £500. In 2015, data.gov.uk held around 25,000 datasets from a large number of mainly public sector organisations.

The UK government was one of the eight founding countries of the Open Government Partnership (OGP) in 2011, along with Brazil, Indonesia, Mexico, Norway, the Philippines, South Africa and the United States of America. All of them endorsed the Open Government

Declaration which commits countries to 'foster a global culture of open government that empowers and delivers for citizens, and advances the ideals of open and participatory 21st century government' (Open Government Partnership, 2015). OGP has since grown to sixty-nine governments. ATI is one of four eligibility criteria for participation in OGP, alongside citizen engagement, fiscal transparency and income and asset disclosure. Signatories pledge to 'increase the availability of information about governmental activities'. This objective states that 'governments collect and hold information on behalf of people, and citizens have a right to seek information about governmental activities' (Open Government Partnership, 2015). In support of this right to information, countries will increase access to information about governmental activities and 'systematically collect and publish data on government spending and performance'. There is a focus on 'high-value information, including raw data, in a timely manner, in formats that the public can easily locate, understand and use, and in formats that facilitate reuse' (Open Government Partnership, 2015). Herrero (2015, 4) suggests that 'the emergence of access to information as one of the central tenets of the Open Government Partnership (OGP) has become a major driving force in the promotion of ATI reforms worldwide'. Each country appoints an Independent Reporting Mechanism (IRM) and conducts annual self-assessments of progress.

Countries signed up to OGP must develop action plans in conjunction with civil society organisations which contain 'commitments that advance transparency, accountability, participation and/or technological innovation' (Open Government Partnership, 2015). The UK's Second National Action Plan commitments include developing an inventory of all government datasets, published and unpublished, and identifying those with the most significant economic and social impact which will form a 'National Information Infrastructure' (Open Government Partnership, 2015). In the USA, President Barack Obama made open government a high priority, symbolised by his first executive action to sign the

Memorandum on Transparency and Open Government. The USA is one of few countries to have issued a third OGP Action Plan, in 2015, which includes commitments to redesign the government portal, USA.gov, and improve the range and accessibility of government information online. Other commitments relate to better management of federal records and emails and to improvements in the implementation of FOI, such as a pilot to test the feasibility of posting all FOI-released records online. The US National Archives is developing tools to teach students about how best to use FOI. Commitments by other countries in their action plans vary depending on the state of open government development, but include specific improvements to access legislation, in-country infrastructure developments to support ATI, implementation of e-commerce systems, internet portals and request systems, research into public attitudes and capacity building and training (Open Government Partnership, 2015).

Many governments assert the relationship between more open government processes and the proactive publication of government data. However, opening up government data is not a 'matter of simply publishing public data' (Janssen, 2011). Data release requires additional data processing in order to produce reusable and releasable data (for example, to remove personal data about individuals). Publishing raw data without context, in heterogeneous formats and with risks of the identification of individuals will not enhance the cause of open government data. Data redundancy and inconsistency, poor data integrity and quality and a lack of interoperability can be mitigated partly through the development of standards and implementation of policies. For example, the UK has promoted the use of a Five Star Scheme (http://5stardata.info/) which classifies data from that published in proprietary formats (1 star) to data which can be fully accessed online and is linked to other data (5 star) (UK Cabinet Office, 2012). An alternative emerging approach is the creation of Open Data Certificates (Open Data Institute, 2015) which seek to improve the quality of data

publication for reuse by providing information, including descriptive metadata, about the attributes of each dataset. As Halonen asserts (2012, 83) 'the value of transparency increases when data is given a proper context and thus people can truly understand and use it.'

Opening up government data will, however, tend to increase information asymmetries unless citizens are actually able to use open data. Even within a single country, not everyone has equal access to open data. As Gurstein (2011, sec.2) points out, users need 'digital infrastructure (…), hardware or software, financial or educational resources/skills which would allow for the effective use of data'. Gurstein (2011, sec.4) identified seven elements necessary in this process, including access to the Internet, up-to-date computers and software, mastering the ICT skills needed, having the data available, having the skills to interpret the data, and having sufficient resources to enable the reuse of the data. The digital infrastructure in many countries and regions does not easily allow citizens to access and reuse government open data.

Implementing an open data policy incurs costs to public authorities and requires systems, protocols and specialist skills. Recordkeepers in public organisations need to work in partnership with ICT system designers and data creators to ensure that data are managed and released appropriately. Data which are made open ought to be managed as part of the records and information systems in the creating organisation. Open government data should originate from authentic recordkeeping systems, so that the data can be trusted. The data which are released should then have characteristics which will make them trustworthy: authenticity, integrity, reliability and usability. As with other records, open data should be genuine and trustworthy, reliable and accurate, and they should have been maintained over time in a way which guarantees their integrity.

Open data use and reuse can raise complex issues from the data producer's perspective. Open data should never include identifiable personal data, yet managing data

anonymisation is challenging, both technically and procedurally. The risks of de-anonymisation and re-identification of data subjects need to be considered. Data creators and publishers often worry about data misuse or its misinterpretation. Researchers and policy makers are reluctant to publish data while they are still using them in development, as they worry that their ideas may be copied or misunderstood. Even after the publication of research results, many researchers regard data as private rather than public intellectual assets even if they were producing using public money, for example in a university.

Many governments assert that open data will drive economic development. Some businesses rely on open data to produce commercial products, such as transport apps which give you bus or train timetables or apps which tell you about the hygiene of restaurant kitchens (so called 'scores on the doors'). In this way government views the commercial data user as a partner in developing public information services without direct cost to the public authority. Civil society organisations sometimes accuse government of wasting valuable public assets by giving the data away freely to businesses which are then able to add value and profit from using open data.

Recordkeepers play a major part in ensuring that open data are accessible and usable over time and are contextualised through good metadata. Too often, open data are regarded as ephemeral and the recordkeeper's role is bypassed when data are released directly by the creator, the website manager or by the public relations department. Once published, open data are then no longer seen as the creating body's responsibility. Standardised metadata, contextual descriptions, data documentation and codebooks, and searchable tagging are needed if data is to be more easily accessible and interpretable over time. If open data are to have long term public value or are to form the basis of accountable public policy and decision making, they need to be managed over time in a systematic and properly documented way. As with organisational records, administrative data which is made open should be subject to

appraisal so that data can be selected for permanent preservation in an archive or subject to systematic deletion periodically. Maintaining all open data on a public website in a usable form (the approach taken at present by many public organisations) is likely to prove costly and over time will prove impossible. Open data portals and websites are already difficult to search and relevant data is often difficult to find and use.

If open data is not well managed over time the result will be less transparency and openness and a loss of trust. In a quest for more openness to provide citizens with a practical 'right to information', poor data management may result in citizens failing to find what they need and want.

CONCLUSION

This chapter has considered the concept of 'right to information' (RTI), 'access to information' (ATI) or 'freedom of information' (FOI) which has been adopted by many countries around the world, often linked to the rights of citizens to information for public accountability, transparency and good governance and for their own freedom of opinion and expression and the exercise of their human rights. The chapter has addressed the question, 'does a right to information exist?', by consideration of four different aspects of access to information: national archives and records legislation; secrecy and privacy including official secrets and personal data; the responsive release of information by governments under freedom of information laws; and the proactive release of information under open government data policies. In each section there has been consideration of the legislative and historical context, drawing on examples from different countries, and an examination of themes from relevant literature, drawn from recordkeeping, law and politics literatures.

The chapter has considered at each stage what the recordkeeping role could or should be in the various legislative and government policy contexts. The professional archival role which began to develop in the late 19th and early 20th centuries, underpinning national archives and records legislation and services, focused on the selection and preservation of records deemed to have permanent value as archives, so that these archives could be systematically transferred to national archive services, where they could be made available to the public after a specified closure period. In this role, recordkeepers needed to be able to undertake appraisal and selection of administrative and policy records of government and ensure their proper description and accessibility once the physical records were transferred to the archive service. Recordkeepers seldom played a role in the operation of secrecy laws, which developed separately from archival legislation, and were applied to records considered to need security classifications in the national interest. Often these records were not transferred to the national archives and records of secret and intelligence services were not historically subject to routine appraisal and selection under national archives legislation. Recordkeepers have, however, been active in operating information laws and policies, including privacy, freedom of information and open government data. Although recordkeepers often need to advocate for the important role they can play in these spheres, increasingly, their expertise in managing administrative data and records is crucial to the proper protection of personal and official data while ensuring the release of information into the public domain. Recordkeepers need knowledge and skills in the complex legal framework and administrative processes which deliver the right to information if they are to provide expert advice to ensure that secrecy and privacy is respected and yet information is released for the benefit of society. This analysis demonstrates the essential role played by archives and records as ‘arsenals of democratic accountability’ and by archivists and recordkeepers as essential actors in ensuring a citizen’s right to information.

References

Avery, C. and M. Holmlund eds. 2010. *Better Off Forgetting: Essays On Archives, Public Policy, And Collective Memory.* Toronto, Ontario, Canada: University of Toronto Press.

Australians Together. 2015. http://www.australianstogether.org.au/stories/detail/the-stolen-generations .

Banisar, D. 2016. *National Comprehensive Data Protection/Privacy Laws and Bills 2016 Map*. http://dx.doi.org/10.2139/ssrn.1951416

Birkinshaw, P. 2010. *Freedom of Information: The Law, the Practice and the Ideal.* 4th ed. Cambridge: Cambridge University Press.

Birkinshaw, P. 2015. 'Regulating Information'. In *The Changing Constitution,* edited by J. Jowell and D. Oliver. 8th ed., 378-409. Oxford: Oxford University Press.

Chapman, R.A. and M. Hunt. 2006. *Open Government in a Theoretical and Practical Context.* Aldershot: Ashgate.

Cerrillo-I-Martínez, A. 2012. 'The reuse of public sector information in Europe and its impact on transparency'. *European Law Journal*, 18(6): 770-792.

Commonwealth of Australia, 1997. *Bringing Them Home: Report of the National Inquiry into the Separation of Aboriginal and Torres Strait Islander Children from Their Families*. Sydney: Commonwealth of Australia.

Coppel, P. 2014. *Information Rights: Law and Practice.* 4th ed. Oxford: Hart Publishers.

Duchein, M. 1992. 'The history of European archives and the development of the archival profession in Europe' *American Archivist*. 55: 14-25.

Eastwood, T. 1993. 'Reflections on the development of archives in Canada and Australia'. In *Archival Documents: Providing accountability through recordkeeping* edited by S. McKemmish and F Upward, 27-39. Melbourne: Ancora Press.

Flinn, A. & Jones, H. (eds). 2009. *Freedom of Information. Open Access, Empty Archives?* London: Routledge.

Florini, A. 2002. 'Increasing Transparency in Government' *International Journal on World Peace*, 1 September 2002, 19(3): 3-37.

Florini, A. 2007. *The Right to Know: Transparency for an Open World.* NY, Columbia University Press.

Gurstein, M.B. 2011. Open data: Empowering the empowered or effective data use for everyone? *First Monday*, 16(2).

Halonen, A. 2012. *Being Open about Data. Analysis of the UK open data policies and applicability of open data.* London: Finnish Institute.

Hazell, R., B. Worthy and M. Glover. 2010. *The Impact of the Freedom of Information Act on Central Government in the UK: Does FOI Work?* Basingstoke: Palgrave Macmillan.

Herrero, A. 2015. *Access to Information Commitments in OGP Action Plans: A Report on the Progress of Reforms Worldwide.* World Bank Governance Global Practice and Red de Transparencia y Acceso a la Información Pública (RTA). http://redrta.org/ .

Hood, C. and D. Heald. 2006. *Transparency: The Key to Better Governance?* Oxford: Oxford University Press.

Hurley, C. 2002. 'Records and the Public Interest'. In *Archives and the Public Good : Accountability and Records in Modern Society*, edited by R. J. Cox and D. A. Wallace, 293-318. London: Quorum Books.

Hurley, C. 2005. 'Recordkeeping and Accountability'. In *Archives: Recordkeeping in Society* edited by S. McKemmish, M. Piggott, B. Reed and F. Upward, 223-253. Wagga Wagga, N.S.W.: Charles Sturt University.

Iacovino, L. 2010. 'Archives as Arsenals of Accountability'. In *Currents of Archival Thinking* edited by T. Eastwood & H. MacNeil, 181-212. Oxford: Libraries Unlimited.

International Records Management Trust. 1999. *A Model Records and Archives Law*. http://www.irmt.org/documents/educ_training/public_sector_rec/IRMT_archive_law.pdf

International Records Management Trust. 2009. *Training in Electronic Records Management. Glossary of Terms.* http://www.irmt.org/

Janssen, K. 2011. 'The influence of the PSI directive on open government data: An overview of recent developments'. *Government Information Quarterly,* 28(4): 446-456.

Ketelaar, E. 1985. *Archival And Records Management Legislation And Regulations: A Ramp Study With Guidelines.* Paris: UNESCO.

McKemmish, S. and M. Piggott (eds) 1994. *The Records Continuum: Ian Maclean and Australian Archives first fifty years*. Clayton, Aus: Ancora Press & Australian Archives.

Millar, L. 1998. 'Discharging our debt: the evolution of the total archives concept in English Canada', *Archivaria,* 46: 103-146.

Meijer, A. 2001. 'Accountability in an Information Age: opportunities and risks', *Archival Science,* 1:4: 361-372.

O'Neill, O. 2002. *BBC Radio 4: Reith Lectures, A Question of Trust*. http://www.bbc.co.uk/programmes/p00ghvd8 .

Open Data Institute. 2015. https://theodi.org/ .

Open Government Partnership. 2015. http://www.opengovpartnership.org/ .

Open Knowledge Foundation. 2012. *Open Definition*. http://opendefinition.org .

O'Toole, J. and R. Cox. 2006. *Understanding Archives and Manuscripts.* Chicago: Society of American Archivists.

Pope, J. 2003. 'Access to information: whose right and whose information?'. In *Transparency International. Global Corruption Report 2003* edited by R. Hodess, 8-23. London: Profile Books.

Roberts, A. 2006. *Blacked Out: Government Secrecy in the Information Age*. Cambridge: Cambridge University Press.

Robertson, K.G. 1999. *Secrecy and Open Government: Why Governments Want You to Know*. Basingstoke: Macmillan.

Scottish Government, 2007. *Historical Abuse Systemic Review: Residential Schools and Children's Homes in Scotland 1950 to 1995 (The Shaw Report).* Edinburgh: The Scottish Government.

Shepherd, E. 2009. *Archives and Archivists in 20th century England*. Aldershot: Ashgate.

Shepherd, E. 2015. 'Freedom of Information, Right to Access Information, Open Data: Who is at the table?'. *The Round Table*, 104(6): 715-726.

Swift, M.D. 1982-83. 'The Canadian Archival Scene in the 1970s: Current Developments and Trends'. *Archivaria*, 15, Winter: 47-57.

UK Administrative Data Research Network. 2015. http://adrn.ac.uk/ .

UK Cabinet Office. 2012. *Open Data White Paper: Unleashing the Potential*. (Cm 8353). London: Stationery Office.

UK Committee on Departmental Records, *Report*. 1954. (The Grigg Report, Cmd 9163). London: HMSO.

UK Information Commissioner's Office (ICO). 2015. https://ico.org.uk/ .

UK National Archives. 2009. *Lord Chancellor's Code of practice on the management of records, issued under section 46 of the Freedom of Information Act 2000*. http://www.nationalarchives.gov.uk/information-management/manage-information/planning/records-management-code/ .

UK Open Government Data. 2015. https://data.gov.uk/ .

United Nations. 1948. *Universal Declaration of Human Rights.* http://www.un.org/en/universal-declaration-human-rights .

United Nations. 1966. *International Covenant on Civil and Political Rights.* http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx .

Wilson, I.E. 1982. 'A noble dream: the origins of the Public Archives of Canada', *Archivaria*, 15: 16-35.

World Bank. 2007. *Strengthening World Bank Group engagement on governance and anticorruption. Main Report*. Washington DC: World Bank Group. http://documents.worldbank.org/curated/en/2007/03/7478369/strengthening-world-bank-group-engagement-governance-anticorruption-vol-1-2-main-report

Worthy, B., J. Amos, R. Hazell, G. Bourke. 2011. *Town hall transparency? The impact of freedom of information on local government in England*. London: UCL Constitution Unit.