World Bank Institute

GOVERNANCE WORKING PAPER SERIES

Access to Information Program

The Right to Information and Privacy: Balancing Rights and Managing Conflicts

David Banisar

The World Bank

Canadian International Development Agency

Agence canadienne developpment international

WORKING PAPER

The Right to Information and Privacy: Balancing Rights and Managing Conflicts

David Banisar*

* David Banisar is senior legal counsel for Article 19, the Global Campaign for Free Expression, in London, UK. He is also a nonresident fellow at the Center for Internet and Society at Stanford Law School, Stanford, CA. Previously, he was the director of the Freedom of Information Project of Privacy International in London; a research fellow at the Kennedy School of Government at Harvard University, Cambridge, MA; and a cofounder and policy director of the Electronic Privacy Information Center in Washington, DC. He has served as an adviser and consultant to numerous organizations, including the Council of Europe, the Organisation for Economic Co-operation and Development, and the United Nations Development Programme.

1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org
E-mail: feedback@worldbank.org

This report has been commissioned by the Access to Information (ATI) Program at the World Bank Institute (WBI) and supported financially by the CIDA-WBI Governance Program.

The WBI Access to Information Program seeks to connect key ATI stakeholders to jointly identify, prioritize, and implement actions for effective ATI adoption and implementation. The program aims to improve in-country capacity for the formulation, implementation, use, and enforcement of ATI legislation through regional knowledge exchange and networking, and by fostering the capacity of multistakeholder coalitions to undertake effective ATI reforms.

Contents

Acknowledgments

I would like to thank Heather Brooke, Bojan Bugaric, Elizabeth Dolan, Maurice Frankel, Juan Pablo Guerrero Amparán, Katherine Gunderson, Gus Hosein, Jose Luis Marzal, Natasa Pirc Musar, Maeve McDonagh, Lina Ornelas Nuñez, Graham Smith, and Nigel Waters for providing information and advice; and peer reviewers Alvaro Herrero, Maria Marván Laborde, and Andrea Ruiz for their comments. I would also like to thank my colleagues at Article 19; and the World Bank Institute's Marcos Mendiburu, Aranzazu Guillan-Montero, and Luis Esquivel for their assistance.

Acronyms and Abbreviations

ACHPR	African Commission on Human and People's Rights
ACLU	American Civil Liberties Union
APEC	Asia-Pacific Economic Cooperation
ATIP	access to information and privacy
CCPR	United Nations Covenant on Civil and Political Rights
CSA	Canadian Standards Association International
DCMS	Department for Culture, Media, and Sport
DPA	Data Protection Act
EC	European Commission
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
ECOWAS	Economic Community of West African States
EFF	Electronic Frontier Foundation
EHRR	*European Human Rights Report*
EO	European Ombudsman
EPIC	Electronic Privacy Information Center
ETS	European Treaty Series
EU	European Union
EUECJ	Court of Justice for the European Communities
EWHC	High Court of England and Wales
FOI	freedom of information
FOIA	Freedom of Information Act

IACHR	Inter-American Commission on Human Rights
ICO	Information Commissioner's Office
IFAI	Instituto Federal de Acceso a la Información y Protección de Datos
MP	member of parliament
NJSBA	New Jersey State Bar Association
NZLC	New Zealand Law Commission
OAS	Organization of American States
ODNI	Office of the Director of National Intelligence
OECD	Organisation for Economic Co-operation and Development
OSCE	Organization for Security and Co-operation in Europe
PI	Privacy International
RCMP	Royal Canadian Mounted Police
RTI	right to information
UDHR	Universal Declaration of Human Rights
UKHL	United Kingdom House of Lords
UN	United Nations
UNHRC	United Nations Human Rights Council
USC	United States Code
USDA	United States Department of Agriculture

Executive Summary

The right to privacy and the right to information are both essential human rights in the modern information society. For the most part, these two rights complement each other in holding governments accountable to individuals. But there is a potential conflict between these rights when there is a demand for access to personal information held by government bodies. Where the two rights overlap, states need to develop mechanisms for identifying core issues to limit conflicts and for balancing the rights. This paper examines legislative and structural means to better define and balance the rights to privacy and information.

1 Introduction

In the words of Michel Gentot (n.d.) during his term as president of the French National Data Processing and Liberties Commission, freedom of information and data protection are "two forms of protection against the Leviathan state that have the aim of restoring the balance between the citizen and the state" (p. 1).

On first inspection, it would appear that the right of access to information and the right to protection of personal privacy are irreconcilable.[1] Right to information (RTI) laws provide a fundamental right for any person to access information held by government bodies. At the same time, right to privacy laws grant individuals a fundamental right to control the collection of, access to, and use of personal information about them that is held by governments and private bodies. However, the reality is more complex. Privacy and RTI are often described as "two sides of the same coin"—mainly acting as complementary rights that promote individuals' rights to protect themselves and to promote government accountability.

The relationship between privacy and RTI laws is currently the subject of considerable debate around the globe as countries are increasingly adopting these types of legislation. To date, more than 50 countries have adopted both laws.

Privacy is increasingly being challenged by new technologies and practices. The technologies facilitate the growing collection and sharing of personal information. Sensitive personal data (including biometrics and DNA makeup) are now collected and used routinely. Public records are being disclosed over the Internet. In response to this set of circumstances, more than 60 countries have adopted comprehensive laws that give individuals some control over the collection and use of these data by public and private bodies. Several major international conventions have long been in place in Europe, and new ones are emerging in Africa and Asia.

At the same time, the public's right to information is becoming widely accepted. RTI laws are now common around the world, with legislation adopted in almost 90 countries. Access to information is being facilitated through new information and communications technologies, and Web sites containing searchable government records are becoming even more widely available. International bodies are developing conventions, and relevant decisions are being issued by international courts.

Availability, legislation, and judicial decisions have led to many debates about rules governing access to personal information that is held by public bodies. As equal human rights, neither privacy nor access takes precedence over the other. Thus it is necessary to consider how to adopt and implement the two rights and the laws that govern them in a manner that respects both rights. There is no easy way to do this, and both rights must be considered in a manner that is equal and balanced.

This paper will examine the two rights and the conflicts that arise, and will describe institutional models to ensure the exercise of both rights. It will present short case studies from four countries (Ireland, Mexico, Slovenia, and the United Kingdom) that have adopted different models for addressing the conflicts, describing how those models work.

2

Rights Defined

2.1 The Right to Information

The right of access to information held by government bodies (RTI) provides that individuals have a basic human right to demand information held by government bodies. It derives from the right of freedom of expression to "seek and receive information,"[2] and is recognized worldwide as a human right.[3] Under this right, any person may make a request to a public body; the body is legally required to respond and provide the information, unless there is a legally compelling reason to refuse the request.

The RTI is "a requisite for the very exercise of democracy" (OAS 2003).[4] Democracy is based on the consent of the citizens, and that consent turns on the government informing citizens about its activities and recognizing their right to participate. The collection of information by governments is done on behalf of its citizens, and the public is only truly able to participate in the democratic process when it has information about the activities and policies of the government.[5]

The RTI is also an important tool for countering abuses, mismanagement, and corruption and for enforcing essential economic and social rights. Civic activists in Rajasthan, India, have used it to ensure that the poor get the food they are entitled to receive from corrupt food distributors (Calland and Tilley 2002), and an angry mother in Thailand used it in her efforts to learn why her daughter was not allowed into a top-quality school (Coronel 2001). It also is commonly used by environment-focused nongovernmental organizations to reveal pollution dangers in communities.

The right is typically recognized at the national level through constitutional provisions and national laws. Some of this legislation has existed for more than 200 years. Section 6 of the Swedish Freedom of the Press Act (adopted in 1766) set the principle that government records were open to the public by default and granted citizens the right to demand documents from government bodies. The 1789 French Declaration of the Rights of Man called for information about the budget to be made freely available: "All the citizens have a right to decide, either personally or by their representatives, as to the necessity of the public contribution; to grant this freely; to know to what uses it is put." Most nations have adopted laws in the past 20 years.

Today, nearly 90 countries around the world have adopted a national law or regulation that sets out specific rights and duties for

facilitating access to information (see Banisar [2006]).[6] The following elements are typically found in national RTI laws:

- A right of an individual, organization, or legal entity to demand information from public bodies, without having to show a legal interest in that information.
- A duty of the relevant body to respond and provide the information. This includes mechanisms for handling requests and time limits for responding to requests.
- Exemptions to allow the withholding of certain categories of information. These exemptions include the protection of national security and international relations, personal privacy, commercial confidentiality, law enforcement and public order, information received in confidence, and internal discussions. Exemptions typically require that some harm to the interest must be shown before the material can be withheld.
- Internal appeals mechanisms for requestors to challenge the withholding of information.
- Mechanisms for external review of the withholding of information. This includes setting up an external body or referring cases to an existing ombudsman or to the court system.
- Requirement for government bodies to affirmatively publish some types of information about their structures, rules, and activities. This is often done using information and communications technologies.

2.2 The Right to Privacy

Privacy is a broad concept relating to the protection of individual autonomy and the relationship between an individual and society (including governments, companies, and other individuals). Privacy is considered essential in protecting an individual's ability to develop ideas and personal relationships. Although it is often summarized as "the right to be left alone," it encompasses a wide range of rights—including protection from intrusions into family and home life, control of sexual and reproductive rights, and communications secrecy.[7] It is commonly recognized as a core right that underpins human dignity and such other values as freedom of association and freedom of speech.[8]

The definitions of privacy and what is sensitive personal information vary among countries and individuals on the basis of past experiences and cultural understandings. Some cultures focus on community rights over individual rights; others, such as countries in Europe, are sensitive to privacy rights because of abuses going back to World War II. In matters relating to modern information and communications technologies, there is more agreement about the importance of privacy and the control of information (this will be covered in more detail later in this report).[9]

The legal right to privacy is recognized in nearly every national constitution and in most international human rights treaties, including the Universal Declaration of Human Rights,[10] the International Covenant on Civil and Political Rights,[11] the European Convention on Human Rights,[12] the American Declaration of the Rights and Duties of Man,[13] and the American Convention on Human Rights.[14] International bodies, including the European Court of Human Rights and the United Nations (UN) Human Rights Committee, also have ruled on the right to privacy.[15]

In the information age, the right to privacy has evolved to address issues relating to the collection, use, and dissemination of personal data in information systems. New tech-

nologies have driven the collection of personal information by governments and private bodies into databases of unprecedented breadth and depth. Governments and private organizations that collect information related to government services and obligations (including tax, medical, employment, criminal, and citizenship records) and identification technologies (including identity card systems, fingerprints, and DNA mapping) have quickly evolved and expanded. New communications technologies create and collect substantial records about individuals in the process of providing communications. Services run by governments and private operators collect information about individuals, including emails, records of persons communicated with, lists of Web sites visited, and mobile locations. And, of course, people share information through social networking sites. All of these have led to concerns about abuses, including misuse of information for unlawful purposes and identity theft.

Since the 1960s, principles governing the collection and handling of this information (known as "fair information practices") have been developed and adopted by national governments and international bodies (OECD [1980]; also see U.S. Department of Health, Education and Welfare [1973]; and CSA [1996]). The principles generally are these:

- **Collection limitation principle—**There should be limits to the collection of personal data; and all such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data quality principle—**Personal data should be relevant to the purposes for which they are to be used; and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.
- **Purpose specification principle—**The purposes for which personal data are collected should be specified no later than at the time of data collection; and the subsequent use should be limited to fulfilling those purposes, or fulfilling such other purposes as are compatible with the stated purposes and specified on each occasion where a change of purpose occurs.
- **Use limitation principle—**Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified above, except under the following conditions: with the consent of the data subject, or by the authority of law.
- **Security safeguards principle—**Reasonable security safeguards should be used to protect personal data against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.
- **Openness principle—**There should be a general policy of openness about developments, practices, and policies relating to personal data. Means of establishing the existence and nature of personal data and the main purposes of their use should be readily available, as should the identity and usual residence of the data controller.
- **Individual participation principle—**An individual should have the right
  a. to obtain from a data controller (or otherwise) a confirmation that the data controller either does or does not have data relating to the individual;
  b. to obtain such data within a reasonable time
     ° at a charge (if any) that is not excessive,
     ° in a reasonable manner, and
     ° in a form that is readily intelligible to the receiving individual;
  c. to be given reasons if a request made under subparagraphs (a) and (b) is de-

nied, and to be able to challenge such denial; and

d. to challenge relevant data and, if the challenge is successful, have the data rectified, completed, amended, or erased.

- **Accountability principle—**A data controller should be accountable for complying with measures that give effect to the principles stated above.

These principles have been incorporated into important international treaties on data protection by the Council of Europe (1981) and the European Union (EC 1995); they have also been adopted by the UN General Assembly (1990) and the Commonwealth Secretariat (2002). Similar principles are under consideration by the Asia-Pacific Economic Cooperation (APEC) forum[16] and the Economic Community of West African States (ECOWAS 2008).[17]

Of those international instruments, the European Union (EU) Data Protection Directive is now the most influential, having been adopted by the 27 EU member-states (plus three European Economic Area countries) and by numerous other countries in Africa, Europe, and Latin America that trade with the EU. The directive takes a broad approach to personal information. Personal data are defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (Directive 95/46/EC, sec. 2[a]).[18] Under a decision from the European Court of Human Rights, these data include information collected under public employment.[19]

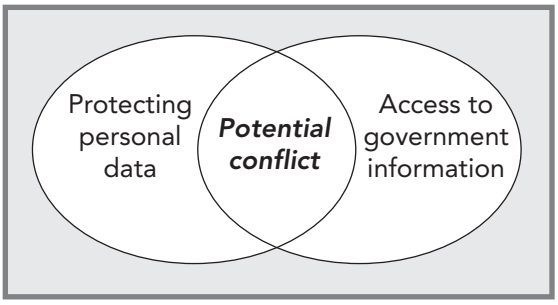
National constitutions also have been evolving to specifically recognize the control of personal data as a right. Many recent constitutions include specific rights to protect the collection and use of personal data in information systems.[20] Many countries in Latin America include a right of habeas data to control and access personal data. The May 2010 Constitution of Kenya states, "Every person has the right to privacy, which includes the right not to have . . . information relating to their family or private affairs unnecessarily required or revealed" (sec. 31).

What is more directly related to the subject of this report is the fact that the governments of more than 60 countries around the world have adopted comprehensive data protection acts based on the fair information practices that apply to personal data held by the public and private sectors (see EPIC/PI [2007]).[21] A number of other countries—including the United States,[22] Georgia,[23] and Thailand[24]—have adopted legislation that protects only personal data held by government bodies. Malaysia recently adopted a law that protects personal data held by companies, but has not adopted legislation protecting personal information held by governments.[25] In a significant number of countries where no data protection law has been adopted, there may be more general provisions in the criminal and civil codes that restrict the use of personal information (see EPIC/PI [2007]).

3 Complements and Conflicts in RTI and Privacy Laws

Right to information (RTI) and privacy laws can both complement and conflict with each other, depending on the situation. As figure 3.1 shows, the two rights play different roles in most cases, and only in a small number of cases do they overlap and lead to potential conflict.

Figure 3.1: Complement and Conflict of Privacy and the Right to Information



Source: Author's illustration.

3.1 Complementary Roles of RTI and Privacy

RTI and privacy often play complementary roles. Both are focused on ensuring the accountability of powerful institutions to individuals in the information age. The Council of Europe stated in a 1986 recommendation that the roles are "not mutually distinct but form part of the overall information policy in society" (Council of Europe 1986). The U.K. data protection registrar noted, "Data protection and freedom of information can be seen as complementary rights, with the potential to be mutually supportive in practice."[26] László Majtényi (2002), the first parliamentary commissioner for data protection and freedom of information in Hungary, says that the common purpose of the two rights is "to continue maintaining the non-transparency of citizens in a world that has undergone the information revolution while rendering transparent the state."

In many countries, the two rights are intertwined constitutionally. Under the concept of habeas data—a constitutional right that permits individuals to demand access to their own information and to control its use—countries in Latin America have adopted both types of laws.[27] Santiago Canton (the first Organization of American States special rapporteur for freedom of expression and the executive secretary of the Inter-American Commission on Human Rights) said, "The action of habeas data, or the right to obtain personal information contained in public or private databases, has been very important in

many countries in exacting accountability for human rights abuses and helping countries scarred by human rights abuses reconcile and move forward, which can only be accomplished by exposing the truth and punishing the guilty."[28]

In many cases, the two rights overlap in a complementary manner. Both rights provide an individual access to his or her own personal information from government bodies, and privacy laws allow for access to personal information held by private entities. They also mutually enhance each other: privacy laws are used to obtain policy information in the absence of an RTI law, and RTI laws are used to enhance privacy by revealing abuses.

Obtaining Personal Information Held by Government Bodies

The most obvious commonality between the two types of laws is the right of individuals to obtain information about themselves that is held by government bodies. This access is an important safeguard to ensure that individuals are being treated fairly by government bodies and that the information kept is accurate.

When a country has both laws, the general approach is to apply the data protection act to individuals' requests for personal information; requests for information that contains personal data about other parties are handled under the right to information act. In some jurisdictions, such as Bulgaria and Ireland, applications by people for their own personal information can be made under both acts.[29] In these cases, it is possible that slightly different outcomes may result because of the differences in exemptions and oversight bodies. Often, data protection laws give greater rights for access to personal information because there is a stronger right of access. In Ireland, the official policy guidance notes, "one's own personal information will very often be released under FOI [freedom of information], while under the Data Protection Act there is a presumption in favour of access to one's own personal data" (Government of Ireland 2006). In cases where there is a request for information about the individual and other persons, both acts will be considered.

In some countries, the RTI act is the primary legislation used by individuals to access their own personal information held by government departments. In Australia, all requests under the Privacy Act are filtered through the Freedom of Information Act (FOIA), resulting in more than 80 percent of all FOIA requests being from people seeking their own information (Law Reform Commission 2010). In Ireland, where both laws allow for individuals' access, even with the presumption above, the FOIA is still the act most people use: approximately 70 percent of all requests are made by individuals for their own information.[30]

In countries such as India and South Africa, where there is no general privacy law giving individuals a right of access to their own records, the RTI laws are the only means to access personal records. In India, RTI laws are regularly used by advocates for the poor to obtain records on distribution of food subsidies to show that individuals' names have been forged and records have been falsified.[31]

Some RTI acts also provide for privacy protections where there is no general privacy law. In South Africa, section 88 of the Promotion of Access to Information Act provides that, in the absence of other legislation (currently under consideration), public and private bodies must make reasonable efforts to establish internal measures to correct personal information held by the relevant bodies.[32]

Applying Privacy Laws to Obtain Information from the Private Sector

Typically, RTI laws do not apply to the private sector, except where the body is conducting government functions (such as where a contractor is operating a hospital). Only a few countries, including South Africa, have adopted RTI laws that extend the right of access to nongovernment bodies for their nongovernment functions.[33]

Data protection laws provide an important complement to RTI provisions by extending individuals' right of access to private bodies. As noted above, more than 60 countries have adopted comprehensive data protection laws that apply to private organizations as well as to government bodies. These laws give individuals the right to obtain personal information from private bodies. The use of the laws may reveal abuses by corporations or other private organizations, such as malfeasance by banks, information and communication technology companies, and previous employers.[34]

Using Privacy Laws to Obtain Policy Information

In the absence of an RTI law, privacy and data protection acts can be used to reveal important policy information. As mentioned at the beginning of this section, habeas data has been used to demand accountability and information. In a similar manner, Article 8 of the European Convention on Human Rights has been used often to obtain personal information, and the article has granted the disclosure of nonpersonal information in some cases. In 1998, using Article 8 as a basis, the European Court of Human Rights ruled that in cases where a lack of information could endanger their health, individuals may demand information from government bodies:

> *The Court reiterates that severe environmental pollution may affect individuals' well-being and prevent them from enjoying their homes in such a way as to affect their private and family life adversely. . . . In the instant case the applicants waited, right up until the production of fertilisers ceased in 1994, for essential information that would have enabled them to assess the risks they and their families might run if they continued to live at Manfredonia, a town particularly exposed to danger in the event of an accident at the factory.*[35]

Data protection laws can also be used to obtain government information that sheds light on policy. Prior to the United Kingdom's adoption of its FOIA, the Data Protection Act was used by individuals to obtain information from government bodies (see Hencke [2001]; Hencke and Evans [2002, 2003]; BBC News [2001]). Even following the implementation of the FOIA, reporters have used the Data Protection Act to discover that officials have been spying on their phone records to discover their sources of information (*Daily Mail* 2006).

Using RTI to Promote Privacy

In many countries, RTI laws are a primary tool used by privacy advocates to identify abuses and to campaign effectively against them. In the United States, groups such as the American Civil Liberties Union, the Electronic Privacy Information Center, and the Electronic Frontier Foundation routinely use the U.S. FOIA and state laws to demand government records on new and existing government programs (communications surveillance, body scanners, and spying on groups) and use the records to campaign against those programs and proposals.[36] In the United Kingdom, the

Taxpayers' Alliance[37] and Genewatch oversee the government, using the FOIA; and Statewatch uses the European Union's (EU) access regulations to oversee the EU bodies.

3.2 Conflicts between RTI and Privacy Interests

Inevitably, as figure 3.1 shows, there are overlaps in RTI and privacy interests that can lead to conflicts. Governments collect large amounts of personal information, and sometimes there is a demand to access that information for various reasons. The requestors include journalists investigating stories, civil society groups fighting for accountability, individuals demanding to know why a decision was made in a certain way, companies seeking information for marketing purposes, and historians and academics researching recent and not-so-recent events.

Every national RTI law has an exemption for personal privacy. As discussed in the following section, these laws vary greatly. As noted earlier, many countries have adopted separate privacy and data protection laws that may interact with the RTI law in determining the release of information.

Given the often complex relationship between privacy and RTI laws, the conflict frequently arises from misunderstandings about what is intended to be protected. Officials must deal with numerous issues: Should officials' names and other details be considered private? Is information in public registers available for any use? Are court and criminal records public? Clarity in law, policy, and practice to limit these problems is essential.

These issues have taken on greater importance as information increasingly is being disclosed in database format and over Internet sites. Questions about the relevance of data protection laws for the reuse of personal information (even if it is publicly available) are important. Under EU data protection law, the mere public access to information does not mean it can be used for any purpose (Working Party 1999).

In many countries, the privacy exemption is one of the exemptions used most often. In the United States, the exemptions for personal privacy (b6) and law enforcement records concerning individuals (b7c) have consistently been the two most-used exemptions. These data include the names of recipients of home loans, citizenship records, and criminal records. In Canada, the privacy exemption was used in 31 percent of all denials—far more than the next-most-used exemption (see U.S. Department of Justice [2010]; Government of Canada [2002]; and U.K. Ministry of Justice [2009]).

The following sections will review some of the common types of information that are requested and the conflicts that arise.

Information about Public Officials

Many of the records held by public bodies contain information that identifies officials who were involved in the subject at some point. This includes the names of officials who wrote memorandums, attended meetings, and approved decisions. Other records contain contact information, official expenditures, or e-mail and phone logs. It is useful to categorize this information as relating to their official capacities.

Government bodies also hold more directly personal information about officials, including their biographical data, photographs, salary records, employment records, home addresses, records of financial assets, and medical histories.

There is no global consensus about which information is nonpersonal and which is per-

sonal. As discussed above, the right of privacy is complex and defined by each culture. There are some points that can be summarized:

- **Official capacities—**Overall, the majority of countries take the position that most information relating to official capacities is not considered personal information for the purposes of withholding. It may be considered personal because it relates to a particular identifiable individual, but generally is not related to his or her personal or family life and is less likely to be sensitive. In most cases, documents cannot be withheld just because an official's name is listed as the author or recipient of a document. In 2007, the European Ombudsman found that it was maladministration for the European Parliament to refuse to disclose the expenses of members of parliament, including their travel and subsistence allowances (EO 2007). The Irish and U.K. information commissions have also ordered the release of parliament members' expense information, whereas all U.S. congressional expenditures are published biannually.
- **Employment information—**Although there is variation across cases, information more closely related to an official's performance in his or her job (including exact salary[38] and details of employee performance reviews) is withheld in many jurisdictions and is available in others.[39]
- **Personal life—**Information relating solely to a public employee's personal life rather than to his or her public actions is less likely to be released. Medical records of nonelected officials are generally considered sensitive and are not released in any system.[40] For officials, criminal records not related to their positions are often withheld (for example, see Scottish Information Commissioner [2009]). There is a general recognition that personal information about senior officials should be more available than that of junior officials. So although the salaries of junior officials may not be made available or only by scale rather than by exact numbers, the salaries of more-senior officials may be affirmatively published. Similarly, requirements for asset disclosure forms are imposed in more than 100 countries for senior and elected officials, and some may be publicly available.[41] Biographical data of decision makers and those who are being considered for very-senior positions are more commonly released than those for more-junior positions.
- **Elected officials—**There is also significant agreement that information about elected or high-rank public officials is less restricted, even when it relates to their personal lives. In 2004, the European Court of Human Rights said, "the public has a right to be informed . . . that is, certain circumstances can even extend to aspects of the private life of public figures, particularly where politicians are concerned."[42] In Hungary, the Constitutional Court ruled in 1994 that there are "narrower limits to the constitutional protection of privacy for government officials and politicians appearing in public [. . . than to that of] the ordinary citizen."[43] In India, the Supreme Court ruled that the criminal records of persons running for parliament should be released.[44] In some cases, the medical records of the highest-ranking officials (such as the president) may be publicly released.[45]

Information Held by Governments about Private Individuals

Governments also hold a significant amount of information about private individuals. This is why data protection or privacy laws were

first conceived and continue to be adopted. The materials include great amounts of bureaucratic records with information that most people consider sensitive—such as records relating to citizen's interactions with government bodies for taxation and to their health care. In the majority of jurisdictions, most of these records are considered private.[46]

Court Records

There is no consensus on access to court records. In Europe, court records naming individuals are considered very sensitive (see Leith and McDonagh [2009]); in the United States, it has been a matter of long-standing principle that the information is public.[47] In Hungary, the data protection and freedom of information commissioner negotiated an agreement between the police and media that access would be provided to criminal cases, but only the individuals' initials would be used until charges were filed (Government of Hungary 1998b).

There has been increasing sensitivity over access in many countries as more records have become available via computer networks, and there is greater concern about financial information being used for fraudulent purposes (see NJSBA [2002] and Cannon [2004]). In response to these concerns, many courts now redact certain types of information, such as financial data and identification numbers, prior to making material publicly available electronically (see Administrative Office of the U.S. Courts [2008]). In Europe, many countries require that identities be removed from cases be before they are made public.

Social Program Records

There are also differences of opinion over the release of information relating to social support programs. In most developed countries, there is sensitivity about individuals receiving social support, so personal information held by government bodies is not generally made public.[48]

In some developing countries, however, many of these records are publicly released and play a crucial role in fighting corruption. In India, all people are guaranteed the right to a certain annual minimum of food and employment. A key element of ensuring that these guarantees are protected is making the muster rolls and other information publicly available so that social audits may be accomplished.[49] This information is increasingly being made available on the Internet.[50] In Mexico, registers of scholarship recipients and other social beneficiaries are made available online.[51] This information can be crucial for identifying fraud in these programs. Box 3.1 points out two examples of fraud discovered through a review of public information.

Box 3.1: Using Publicly Available Personal Information to Fight Fraud

In India, a review of the data by a single individual using information gathered under the National Rural Employment Guarantee Scheme found that millions of rupees were being siphoned off because fake identity cards in the names of children and public employees were created and used. Previous social audits had not revealed the fraud.

In Mexico, an analysis of the agricultural subsidies register by the transparency advocacy group FUNDAR found that the families of the minister of agriculture and wanted drug barons were receiving public money.

Public Registers

An increasing controversy relates to access to information in public registers, such as birth,

marriage, and death registers; electoral registers; land records; lists of license holders; and other similar records. In many countries, there has been a long history of public access to these records. However, concern over their use for commercial purposes, for stalking, and for other reasons not related to their original purposes has grown as the registers have been digitized and made available over the Internet (see NZLC [2008]). Countries vary widely in their approaches to making public registers available and to permitting third parties to reuse the information for other reasons.[52]

Some countries' laws limit disclosure of information for certain reasons, such as commercial purposes. The New Zealand public register privacy principles state, "Personal information obtained from a public register shall not be re-sorted, or combined with personal information obtained from any other public register, for the purpose of making available for valuable consideration personal information assembled in a form in which that personal information could not be obtained directly from the register."[53] In 1999, the U.S. Supreme Court upheld a law that restricted access to a computerized list of recently arrested individuals for use in commercial marketing.[54] The U.K. government makes available a limited version of the electoral roll (from which people may opt to have their names removed) that can be used for commercial purposes, and it prohibits use of the full roll for such purposes.

Following a review of legislation related to public registers and public access, the New Zealand Law Commission recently recommended that any legislation that creates a public register keep the following principles in mind:

- free flow of information,
- transparency,
- privacy interests (including the protection of personal information),
- accountability for fair handling of personal information, and
- public safety and security (NZLC 2008).

Professional Records

Government bodies also maintain records relating to people who have more of a business relationship with government, including those who donate money and meet with officials in their capacity as employees of a company or organization. In this regard, there is an increasing demand that lobbyists be registered and that such information be made public.[55]

In general, these individuals are considered to have less of a private interest guarantee because the information is related to their professional activities rather than to their personal opinions or lives. U.K. and U.S. tribunals have found that in the absence of compelling reasons to the contrary, the identities of corporate lobbyists should be revealed.[56] However, the European Court of Justice ruled recently that businesspeople who met with officials could have their names withheld.[57]

Public Subsidies for Business Purposes

Governments also often provide subsidies to individuals as a business matter, in areas such as agriculture. There has been considerable debate over agricultural subsidies in European countries in the past few years, with the result that most of the information is now publicly available.[58] There is a growing agreement that these records are not particularly sensitive because they relate to a business activity (although they may reveal the amount of income that a small farmer may receive in a single year). However, the European Court

of Justice recently ruled that information in this area concerning individuals must be restricted.[59]

Misuse of the Privacy Exemption

Not all arguments for privacy made by officials are legitimate. A conflict sometimes arises when government officials attempt to shield their decision making from scrutiny by misrepresenting their demand for secrecy as a privacy interest. Documents and information are withheld, claiming privacy of officials or of third parties. In Argentina, the government claimed that information about official spending on advertising was personal information (see Knight Center [2010]). Former U.K. Cabinet Secretary Sir Richard Wilson, the highest-ranking U.K. civil servant, best articulated this belief, testifying, "I believe that a certain amount of privacy is essential to good government."[60]

The misuse of privacy exemptions often leads to needless conflict between the media and privacy campaigners as the media comes to believe that any privacy law is an attempt to hide government activities. As noted by Australian freedom of information expert Nigel Waters (2002), "There is a continued problem of privacy exemptions in FOI law being misused and getting privacy a bad name. This makes a major contribution to the widespread jaundiced media view of privacy law, even though it is not actually privacy law that is to blame."

3.3 Balancing the Rights of Access and Privacy

It should again be emphasized that the RTI and privacy are not always conflicting rights. They are both laws designed, in part, to ensure the accountability of the state. The important issue is how the legislation and the implementing and oversight bodies balance the two rights. As discussed above, both the RTI and privacy are internationally recognized human rights with long histories and important functions. Under human rights law, typically no right is accorded a greater weight than another.[61] The rights must be decided on a case-by-case basis with a view toward the relative importance of various interests.

⋆ ⋆ ⋆

The next chapter will discuss legislative and structural means to minimize conflicts between the two rights.

4 Legislation

In the past 10 years, there has been a marked convergence of policy and legislation in both right to information (RTI) and data protection laws. Most data protection laws follow the structure of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and the European Union (EU) Data Protection Directive. There is more divergence around RTI laws, but they generally follow the principles set out in preceding chapters of this report. The convergence in both areas results from the influence of international treaties and agreements and the efforts of a more global civil society connected through modern communication technology—a society that is constantly sharing ideas and good practices.

There has also been convergence in developing policies on the relationship between RTI and privacy laws and how best to make them interact. Although no consensus on good practice has yet emerged, a number of common areas are now clear. This chapter will review the most common policy choices made by governments and highlight their strengths and weaknesses.

4.1 Model 1—A Single RTI and Privacy Law

For those jurisdictions that have not adopted either law but plan to do so, one possibility is to adopt both laws in a single act. This allows for common definitions and internal consistency and for limiting conflict and establishing a balance from the start. Here are several examples:

- In Canada, Bill C-43, adopted in 1982, contained both the Access to Information Act and the Privacy Act. The two sections then became separate laws with separate commissions to enforce them, but with common definitions and relationships. The Canadian Supreme Court has described the two laws as a "seamless code with complementary provisions that can and should be interpreted harmoniously."[62] Many Canadian provincial laws also address both rights in a single law.
- In Hungary, the 1992 Act on the Protection of Personal Data and Public Access to Data of Public Interest is both a gener-

al RTI law and a data protection law that protects personal information held by public and private bodies.[63] It created a single oversight body with jurisdiction over both. The parliamentary commissioner for data protection and freedom of information oversees them.

- In Mexico, the Federal Law on Transparency and Access to Public Information lists both access to information and the protection of privacy for records held by federal government bodies as its primary goals. It is overseen by the Federal Institute for Access to Information (more commonly known by its Spanish acronym IFAI). More recently, legislation to extend its remit to include personal data held by the private sector has been adopted.
- In Thailand, the Official Information Act both gives citizens rights to access information held by government bodies and controls how government bodies may use personal data. Both are overseen by the Official Information Council. Legislation to protect records held by the private sector is currently being debated.

There are some disadvantages to adopting a single act to address both rights. For one, having both functions together may cause legislative confusion over the intent of the laws and may lead to opposition by some parties who would otherwise support one act or another. A more practical issue is the complexity of the legislation, which may lead to legislators being unwilling to review it because they lack the time.[64] An act that covers both areas comprehensively will need to be as detailed as two single acts because there is little overlap in the two (except for the definitions and the oversight body).

4.2 Model 2—Separate RTI and Privacy Laws: Managing Conflicts

In many jurisdictions, either an RTI or a data protection law has been adopted and is in force, or a decision has been made to introduce the laws as separate pieces of legislation. Therefore, the new law or laws must be adopted in a way that ensures the greatest harmony between the operations of the two laws. If the goal of harmony is ignored at the outset, the laws will conflict and further legislative efforts will be required later.

Here are some important considerations when adopting new legislation:

- **Definition of personal information—** Ideally, a common definition will be used for both acts. If not, then the definitions from both laws will be considered each time that access to personal information is sought.
- **Primacy of legislation—**Because both access to information and privacy are equally fundamental rights, neither law may arbitrarily trump the other. How will the legislation address this issue?
- **Privacy exemption in RTI law—**All national RTI laws provide for the withholding of personal information. There is wide variance in the scope of these exemptions, ranging from a presumption that all information is private and should be withheld to a presumption of openness with limited exceptions for sensitive information.
- **Subject access requests—**As noted earlier in this report, some jurisdictions allow for individuals to request their own per-

sonal information under either act. A better choice would be to select one act that gives greater access and to focus those requests through that law. In most European countries, this is the Data Protection Act.

- **Oversight and appeals—**What type of body will rule on the balancing of the rights? It should be a specialized body that can develop clear standards on the subject.

Personal Information Defined

Data protection laws typically take an expansive view of what is personal information. EU Directive 95/46/EC, section 2(a), defines personal information broadly as any information that identifies an individual. Such breadth can lead to a conflict with the RTI because the core principle of data protection is that information collected for one purpose should not be used for other purposes without the consent of the individual—and this is often viewed as covering everything that mentions a person.

Countries have addressed this in different ways. The Canadian access to information and privacy acts use a single definition in the Privacy Act that sets out in detail the boundaries of personal information and public information. In contrast, the Irish Freedom of Information Act (FOIA) and the Data Protection Act use different definitions, but require that the FOIA definition be used when considering the exemption.

Some countries define in more detail the types of information to be protected. Doing so enables the legislature to define some of the boundaries rather than leave them to the oversight bodies or courts to determine.

Many laws specifically exclude information relating to public functions from coverage under the privacy exemption. As noted before, Canada's Privacy Act includes detailed descriptions of both personal information and what is excluded from the definition in relation to public activities. In South Africa, the Promotion of Access to Information Act[65] requires that disclosure of information be declined if it "would involve the unreasonable disclosure of personal information about a third party, including a deceased individual." However, the information can be disclosed if it is about an individual who is or was an official of a public entity and if it relates to the position or functions of the individual, including, but not limited to

- the fact that the individual is or was an official of that public body;
- the title, work address, work phone number, and other similar particulars of the individual;
- the classification, salary scale, or remuneration and responsibilities of the position held or services performed by the individual; and
- the name of the individual on a record prepared by the individual in the course of employment (section 34).

Curiously, a few laws passed more recently—including the Indian Right to Information Act and the Indonesian Act on Public Information Disclosure[66]—do not provide for a definition of private information; they rely instead on common language definitions for interpretation.

Fairness and Data Protection

In many countries, the privacy exemption requires that all personally identifiable information must be withheld. Frequently, the RTI law specifically defers to the law on data protection for the definition of personal information to be protected and the rules governing its release. This approach is found in many European countries, including Croatia,

Kosovo, Romania, Slovakia, and the United Kingdom.

Under this approach, it is then necessary to use the data protection law to determine if information can be released. An initial inquiry will determine if consent has been obtained and can be used to justify the release of the information. A best practice is to inform individuals at the time of collection that the information may be made public under RTI legislation.[67] If consent from the person is not forthcoming, the data protection principles must be reviewed to determine if release can be justified.

Among the pertinent principles, fairness is the most important one to consider. Fairness typically depends on the circumstances under which the information was collected and the expectation at that time that the information would be used in certain ways. If the processing (in this case, the public release) of the information can be found to be fair, it can proceed and the information can be disclosed. Box 4.1 sets out guidelines used by the U.K. government to determine fairness.

Box 4.1: Elements to Determine Fairness

The U.K. Ministry of Justice recommends that the following factors be used in determining if disclosure under the U.K. FOIA would be considered fair:

- How the information was obtained.
- The data subject's likely expectations regarding the disclosure of the information. For example, would the party expect that his or her information might be disclosed to others? Or had the person been led to believe that his or her information would be kept secret?
- The effect that disclosure would have on the data subject. For example, would the disclosure cause unnecessary or unjustified distress or damage to the data subject?
- Whether the party expressly refused consent to disclosure of the information.
- The content of the information.
- The public interest in disclosure of the information.

Source: U.K. Ministry of Justice 2008.

Public Interest Test

Increasingly, many RTI laws provide for a balancing test to be used when determining whether personal information should be released. Under this test, even if the information is determined to be personal and its release would cause harm, it may be disclosed if it is found that the public interest in release is more important than the privacy interest. This allows for independent arbiters such as commissions, courts, or ombudsmen to weigh the different values and determine, case by case, when information should be released. This test is used to evaluate privacy interests in a number of countries, including Ireland, New Zealand, Slovenia, and the United States.

In the United States, the primary privacy exemption protects "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[68] The courts have found that there is an implicit public interest test "balancing the individual's right to privacy against the basic purpose of the FOIA to open up agency action to the light of public scrutiny."[69]

The Slovenian information commissioner has identified some areas where public interest would be strong:

- where the disclosure will assist public understanding of an issue of current national debate,

- where the issue has generated public or parliamentary debate,
- where proper debate cannot take place without wide availability of all relevant information,
- where an issue affects a wide range of individuals or companies,
- where the issue affects public safety or public health,
- where the release of information would promote accountability and transparency in decision making, and
- where the issue concerns the making or spending of public money (Pirc Musar 2006).

In a leading case in Ireland, the Irish information commissioner set out public interest arguments to consider when balancing requests for information:

- *The public interest in the public having access to information.*
- *The public interest in the accountability of elected representatives.*
- *The public interest in a free and informed debate on the level of remuneration/expenses paid to elected representatives.*
- *The public interest in accountability for use of public funds.*
- *The public interest in an individual's right to privacy in respect of information relating to his/her financial affairs.*
- *The possibility of damage to the image of Parliament as an institution in the event of reduced public confidence in the integrity of members of the Houses of the Oireachtas.*
- *The public interest in the entitlement of members of the Houses of the Oireachtas (Irish national parliament) to discharge their Constitutional responsibilities without being put in a position where they are or may be subjected to unjust attack for claiming financial entitlements which are theirs as a matter of law and the amounts of which are not, in the normal course, relevant to the member's performance as a public representative.*
- *The possibility of prejudice to, or distortion of, the democratic process by equation, in the eyes of members of the public, of the level of payment of expenses to members with individual performance of members, with possible adverse consequences for the careers of individual members.*
- *The possibility that disclosure of records which are, or may not be, comparable, and which are likely to be used for comparison purposes, may mislead the public and result in comment based on partially or wholly unreliable conclusions which may be damaging to the interests of individual members.*
- *The possibility that such comparisons may result in certain members being forced to release further personal information relating to their financial affairs in order to deal with inaccurate public speculation as to their income and to repair perceived damage to their interests.*[70]

Thus, it is clear from the different models described above that both the RTI and the data protection laws must clearly define how personal information is going to be considered. Under the most effective legislation, this is set out lucidly and provides for specific boundaries on types of personal information to be protected and a balancing test that examines both harms and the public interest (Pirc Musar 2010).

5 Oversight

All national right to information (RTI) laws have some form of external appeals mechanism. In approximately two thirds of countries (roughly 60), an independent oversight body such as a commission or ombudsman has been empowered to receive appeals and make determinations or recommendations on the release of information.[71] These bodies can play an important role in balancing public interest with the release of personal data.

A very strong trend exists for countries to create information commissioner offices that can decide appeals and provide oversight and guidance. There is a roughly even split in jurisdictions that have created a commission between those that have separate bodies to handle the RTI and data protection and those that have a single body to handle both. Each model has its pros and cons.

5.1 Two Bodies—Separate RTI and Privacy Commissions

Many countries have created separate bodies for enforcing the RTI and the protection of privacy. The bodies may have a single function or have other duties assigned to them.

A few countries have created an independent RTI commission as a single-function body. These countries include Belgium, Canada, France, and Portugal. More commonly, an already existing ombudsman's office also enforces the RTI law. This is the situation in New Zealand, Peru, and the Scandinavian countries. A few jurisdictions (such as Ireland) have adopted an RTI commission that also serves as the ombudsman, but with additional powers.

In nearly all countries, the data protection or privacy commission is an independent body. This is partly because of requirements under European Union law that data protection commissions be independent.[72]

There are benefits to having two bodies. A separate commission for each of the two rights can create clear champions for such rights, unencumbered by the need to balance potentially competing interests. As stated by Canadian Information Commissioner John Grace:

> *The values of openness and privacy each has a clearly identifiable and unambiguous advocate. While both commissioners are required by law to reasonably balance access rights and privacy rights, each has a clear*

> *mandate to be a lightening [sic] rod for, and champion of, one of the two values.*[73]

This could be particularly important when one is a new right that is not yet established in the public mind and the other has long been accepted and championed by a body.

A primary concern of having two bodies is that there will be conflict between the two—and that could become messy, expensive, and embarrassing. In Canada, there have been public fights between the two commissions for both policy and political reasons (see Government of Canada [2001]). There is also concern that public bodies and the public will receive conflicting advice from the two commissioners when they disagree. As noted by the Canadian Access to Information Review Task Force in 2002:

> *An institution is required to notify the Privacy Commissioner before making such a disclosure, where this can reasonably be done. A situation can arise where the Information Commissioner advises the institution to disclose personal information in the public interest, but the Privacy Commissioner advises the institution to protect the information on the grounds that the public interest in the case does not clearly outweigh the invasion of privacy that could result from disclosure. This puts the institution in the difficult position of having conflicting recommendations from the two Commissioners (Government of Canada 2002, p. 59).*[74]

If there are two commissioners, there will need to be a mechanism to resolve conflicts. Previously, the Slovenian system used an administrative dispute institute. The Slovenian information commissioner found that the system was inefficient:

> *Two bodies which operate in an area so closely interlinked would inevitably come into conflicting situations [with] the institute of an administrative dispute as a tool for settling such conflicts. Such a manner of settling mutual conflicts though, would, due to the long time periods of dispute resolutions, mean a lessened legal certainty (Pirc Musar 2006).*

Finally, not related to the scope of this report but quite relevant to many countries, there is an economic concern relating to the cost of two commissions. It may be difficult to justify two commissions in small jurisdictions when economic situations are difficult or as governments are cutting back to create a new body.

When there are two agencies, there should be formal agreements to cooperate to minimize conflicts. In New Zealand, the privacy commissioner and the ombudsman have a formal consultation process that requires the ombudsman to consider the views of the privacy commissioner before determining whether to release personal information (Slane 2002). In Ireland, the Data Protection Act requires the two bodies to cooperate.

5.2 One Body—A Single RTI and Privacy Commission

Countries increasingly have been creating single commissions to handle both access to information and privacy protection. Countries and jurisdictions that have adopted this model include Estonia, Hungary, Malta, Mexico, Serbia, Thailand, and the United Kingdom at the national level; and many Canadian provinces, German länder, Mexican states, and Swiss cantons at the subnational level.

In most cases, an existing commission is given additional authority with the adoption of new legislation. In the United Kingdom, the Data Protection Commission evolved into the Information Commission. A similar process also occurred in Germany, Malta, and Switzerland. In Slovenia, the two bodies were merged into a single new commission headed by the previous information commissioner.

The most significant benefit of having a single body is the shared expertise and reduction of conflict. As noted earlier, there is a strong interrelation between the two rights. Although they have some areas of conflict, there also are strong areas of commonality.

Having a single body can reduce the possibility of institutional conflict. In practice, many requests for information under RTI legislation will relate to personal information; having this dual expertise will allow for better balancing. Elizabeth France (1999), the U.K. data protection registrar, commented during the legislative process in June 1999:

> *The possibility of institutional conflict which would exist were there to be separate Commissioners for freedom of information and data protection matters is avoided. Working within one institution should allow more focused and effective consideration than working across institutional boundaries. Any tension will be contained within the institution. Making the actual decision about where the balance should lie between data protection and freedom of information in a particular case will not be less difficult because there is one commissioner. However, with experience and understanding of both issues in-house, the decision process itself should be eased.*

It is also easier for the public to have a single point of contact with public bodies to better exercise their rights. The Slovenian commissioner has found that having one entity resulted in greater awareness of both rights:

> *The merged body also insures for its greater visibility as well as unification of the entire legal practice of the field. It will also increase the awareness of all other government bodies while carrying out the stated legislative provisions to the benefit of all applicants (Pirc Musar 2006).*

The creation of a single body with both powers also reduces the likelihood that public bodies can misuse data protection, knowing that their decisions are subject to review by an oversight body that is an expert in both areas of legislation. As László Majtényi, the first Hungarian information commissioner, stated in his first report, "[i]t goes without saying that nobody can lawfully obstruct the freedom of information and the press in the name of data protection" (Government of Hungary 1998a, p. 73).

There is also an important economic argument to having only a single body. None of the administrative costs—such as human resources, technical infrastructure, and administrative support—are duplicated. When the Canadian information and privacy commissioners, who shared common corporate services, split apart in 2002, the costs for both bodies increased by an estimated Can$1 million each.

The strongest drawback to adopting a single-commission model is the danger that one interest may be stronger or perceived as more powerful and that the bodies do not equally protect or balance both interests (Tang 2002). Any conflicts are likely to be decided internally rather than publicly, where they would receive a public viewing and de-

bate. The Canadian privacy commissioner worried that it would "diminish" or "dilute" the profile of privacy at a time when there were profound privacy challenges.[75]

An imbalance could be especially problematic where one law has a greater constitutional protection or has been in force for a significantly longer period of time. In the United Kingdom, this concern led to the creation of two distinctly separate workforces for the different rights inside the information commission (which had previously been enforcing only data protection rights). Only after five years are the two workforces being merged.

There is also a concern that a single body may not be provided with adequate resources to take on additional duties—duties that are significantly different in some ways. In Australia, the Tasmania ombudsman (who is also the information commissioner and the integrity commissioner, and who holds several other posts) recently expressed concern that new functions added to his mandate have resulted in additional work without enough resources being provided (ABC News 2009).

There is no clear answer for every jurisdiction on the issue of whether it is better to have one commission or two. Countries may wish to create a new institution to ensure that the profile of one of the rights is clearly promoted and not diluted by other functions. In other cases, an existing body (such as an ombudsman) may be appropriate. And, of course, economic or political concerns may dictate one model over the other.

★ ★ ★

In the next chapter, both oversight models will appear in the case studies presented there—including one jurisdiction that has switched from one model to the other. The discussion will examine some of the benefits and limitations of the different models.

6 Case Studies

6.1 Ireland

Ireland's Data Protection Act was adopted in 1988 and amended in 2005 to implement the European Union (EU) data protection directive. The act created the Office of the Data Protection Commission as an oversight and enforcement body. Ireland's Freedom of Information Act (FOIA), adopted in 1997, created an Office of Information Commission to enforce the act. The government appointed the ombudsman to act jointly as the information commissioner. The second commissioner was also jointly appointed as ombudsman. Under the Data Protection Act, "the Commissioner and the Information Commissioner shall, in the performance of their functions, co-operate with and provide assistance to each other" (sec. 1[5][b]).

The definition of privacy in the two acts is not identical. Section 2 of the FOIA defines personal information as data about an "identifiable person" that is normally "known only to the individual or members of the family, or friends, of the individual," or is confidential. It provides 12 paragraphs of examples of what is personal information, including "educational, medical, psychiatric or psychological history," financial affairs, religion, and tax and identification numbers. These definitions are followed by three paragraphs of information expressly excluded from the definition of personal information, including the activities of an officeholder of a public body and those providing public services under contract, and opinions of the individual regarding the public body (including its staff).

Separately, the Data Protection Act defines personal information as "data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller" (sec. 1[1]). However, to ensure that there is no conflict between that act and the FOIA, section 1(5)(a) of the Data Protection Act provides a specific exemption for release of personal information under the FOIA. This is considered by a leading commentator (McDonagh 2006) to be a "trumping" of the privacy right, but subject to constitutional protections and international obligations.

Individuals may request personal information about themselves from government bodies under either the Data Protection Act or the FOIA. Most requests to public bodies are made under the latter, except requests to bodies that are not covered by the FOIA—such as the Guardi (police) and the private sector.

Under section 28 of the FOIA, personal information must be withheld unless (1) it is about the requestor, (2) the person gives consent, (3) the information is of a class that is publicly available or the person has been notified that it is part of that type of class, or (3) its release is necessary to avoid a serious and imminent danger to the life or health of an individual (see Government of Ireland [2006]).

The exemption is subject to a public interest test that allows for the release of the information if "the public interest that the request should be granted outweighs the public interest that the right to privacy of the individual to whom the information relates should be upheld" or if it benefits the individual. The information commissioner ruled in 1999 that the expenses of members of parliament (MPs) should be released as a matter of public interest. In that case, the commissioner examined the questions about financial privacy and public spending:

> *As a general proposition I would accept that, when an individual discloses details of his/her financial affairs including details of financial transactions with third parties to a public body, there is an understanding that the information is given in confidence. However, does such an understanding normally exist in relation to the payment of public money to individuals, be they members of the Oireachtas [Parliament] or employees of a public body? It is pertinent to recall at this point that the information at issue in this case concerns amounts paid to individuals to defray expenses incurred by them in discharging their functions as public representatives. The payments do not arise out of some private activities or private aspect of their lives. On this point they can be distinguished from, say, a payment made to a claimant under the Social Welfare Acts, where there is an expenditure of public money but the payment derives from some private aspect of the claimant's life such as family circumstances or inadequacy of means (Government of Ireland 1999).*

Since that time, the commissioner has examined numerous other cases related to privacy and access. The breakdown of cases indicates that this question is the one most examined by the office. Other information that has been ordered released under the public interest test includes payments of agricultural subsidies and the names of and payments to experts, outside lawyers, and senior academics.[76] In a recent settled case, the commissioner negotiated a settlement for the release of detailed expenditure records in database form from the Department of Arts, Sport and Tourism to allow for easy comparisons (Sheridan 2010). However, a complaint about the decision has been filed with the Data Protection Commission.[77]

6.2 Mexico

Mexico adopted the Federal Law on Transparency and Access to Public Information in 2002.[78] The law states that its objective is to both promote transparency and protect personal information held by public bodies. It does not apply to personal data held by private bodies. In 2010, the Federal Law on Protection of Personal Data Held by Individuals was adopted.[79] The more recent law applies to personal data held by private companies and individuals. Personal information is defined as "any information concerning an identified or identifiable natural person." A new initiative is being considered by Congress to revise and extend the data protection

provisions of the right to information (RTI) law to improve the protection of information held by federal bodies.

As part of a federal system, each of the 32 states has adopted its own access to information law, and many are considering data protection laws. In the Federal District (Mexico City), both RTI and data protection laws have been adopted, and a single commission handles both issues.[80]

The 2002 RTI law created a Federal Institute for Access to Information (IFAI) to monitor federal government bodies' compliance with both access to information and protection of personal data legislation. The IFAI was changed into the Federal Institute for Access to Public Information and Data Protection with the adoption of the 2010 act, and will now have the authority to enforce the protection of personal information held by the private sector.

Personal information is defined in article II(2) of the law as "[a]ll information concerning an individual, identified or identifiable, including their ethnic or racial origin, or related to their physical, moral or emotional characteristics, their personal and family life, residence, telephone number, patrimony, ideology, political opinions, religious or philosophical beliefs or convictions, physical or mental health, sexual preferences, or any other similar preferences that could have an impact on their intimacy." Article 18 protects personal data as confidential and thus exempt from release. Personal data related to public spending or present in public registries is not considered confidential.

According to chapter IV of the 2010 law, federal public bodies are required to provide individuals access to their own information and details on the procedures for correcting that information to ensure that all handling is "adequate, appropriate and moderated in connection with the purposes for which they were obtained"; to ensure it is accurate, updated, and corrected it if it is incorrect; and to ensure that it is kept secure.

The IFAI rules on all appealed cases concerning access to government-held information. Many of these cases relate to the personal information of third parties, both officials and members of the public; and they have required the IFAI to balance the two rights. In balancing these rights, the institute balances public accountability against protecting personal data (Irazábal and Núñez 2009). In the cases, some of the factors have included the public interest in knowing about criminal prosecutions, the importance of the public being aware of the elements of a scientific investigation, and the value of public accountability when public funds are spent. In cases where privacy has been upheld, the IFAI has analyzed whether the release of information would give the public insight into the performance of the data subjects or their suitability for their jobs. Following such analysis, it decided that release would not provide such insight, and so denied release of the information. In a different case (one that sought the telephone numbers of wildlife units), another decision was reached and the numbers were released. The IFAI has also denied release of information from the Mexican Population Register—even though the information was not considered confidential—because it was available elsewhere.

6.3 Slovenia

The Personal Data Protection Act was adopted in 1999 and replaced in 2005 with a new act based on EU Directive 95/46/EC. The law created an Inspectorate for Protection of

Personal Data within the Ministry of Justice as its oversight and enforcement body. The Access to Public Information Act was adopted in 2003. The law created a commissioner for access to public information to enforce its provisions.

The two commissions were merged into a single information commissioner by the Information Commissioner Act in 2005. There were concerns that the inspectorate for data protection was not as strong and independent as required under EU rules. Prior to the merger of the offices, disputes were handled through the initiation of an administrative dispute; however, no cases were filed. Following the merger, the National Supervisor for Data Protection was established under the authority of the information commissioner, and staff was substantially increased.

Slovenia's Access to Information Act allows for the withholding of information when "the disclosure . . . would constitute an infringement of the protection of personal data in accordance with the Act governing the protection of personal data." Personal data are defined in the Data Protection Act as "any data relating to an individual, irrespective of the form in which it is expressed." An individual is defined as "an identified or identifiable natural person to whom personal data relates; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity, where the method of identification does not incur large costs or disproportionate effort or require a large amount of time." However, the commissioner has said that, based on a Constitutional Court ruling, a name is not sufficient to constitute personal data in the absence of other identifying data.[81]

Under the Access to Information Act, access cannot be withheld if it is "related to the use of public funds or information related to the execution of public functions or employment relationship of the civil servant." It also contains a public interest test that provides that "the access to the requested information is sustained, if public interest for disclosure prevails over public interest or interest of other persons not to disclose the requested information."

Under the decisions of the commissioner, the public interest in the release of information is the issue that has been examined numerous times.[82] The commissioner has ordered the release of information relating to the misconduct of officials because it is in the public interest[83] and the release of the name of a job applicant who was already a public servant,[84] and has denied release of video surveillance records from the state prosecutor's office.[85]

6.4 United Kingdom

The United Kingdom first adopted the Data Protection Act in 1984, in response to the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[86] The act created a data protection registrar to enforce it. In 1998, the act was replaced to implement EU Data Protection Directive 95/46/EC, which changed the data protection registrar into the data protection commission and granted it stronger powers. In 2000, the FOIA was adopted. The act transformed the data protection commission into the information commission, with authority to enforce both acts.

When the FOIA proposal was first considered, the government position was that

there would be a separate information commission. In the end, the government revised its position, stating,

> *Dual enforcement regimes raise serious coordination problems, are confusing to applicants, wasteful of resources and require complicated procedures to ensure that issues of privacy and access to information have both been properly assessed in the many cases in which they overlap. This is why it has been decided that for the UK FOI Act the role of Information Commissioner should be merged with that of Data Protection Commissioner (U.K. Home Office 1999).*

In addition, the Freedom of Information (Scotland) Act 2002 created a separate Scottish information commission that has authority only over access to information. The Scottish information commissioner considers the U.K. data protection exemptions when deciding on the release of information.[87]

The FOIA adopts the definition of personal data found in the U.K. Data Protection Act: "data which relate to a living individual who can be identified—(a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual." Eight data protection principles set the rules for the processing of personal information. They require that the processing is fair and lawful, that the data are collected and used only for specific and lawful purposes, that the data are adequate and relevant for the purpose for which they are collected, that they are accurate and up to date, that they are kept no longer than necessary, that they are processed in accordance with the rights of the individual, that they are kept secure, and that they are not transferred to third countries.

Under the FOIA, when an individual requests personal information about himself or herself, he or she is directed to the subject access provisions of the Data Protection Act. Although this typically is a good solution, given the stronger requirements under EU law and the European Convention for the Protection of Human Rights and Fundamental Freedoms on access to personal records, there is a substantial weakness in the United Kingdom. Under the U.K. Data Protection Act, individuals who are denied access cannot appeal to the information commissioner. Rather, they must apply in court. They have fewer rights to demand access than are available under the FOIA.

When it comes to accessing records that contain personal information about other people, there is a complex relationship. A simplified explanation is that requests for information about third parties are generally exempt if they violate the data protection principles of the Data Protection Act. Under the FOIA, there is an absolute exemption for personal information. Thus, any decisions on the release of personal data must analyze the information using the data protection principles rather than the FOIA. However, this is not to say that information containing personal data is never released. The key issue is whether the release of the information would be unfair under the principles. This includes a consideration of how the information was collected in the first place, the effect on the person from whom the information was collected, whether consent to release the information was obtained, and the public interest in releasing the information.[88]

According to the U.K. Ministry of Justice (2010), the privacy exemption is the most

common one cited by public bodies. Many cases before the information commission, the information tribunal, and the courts have focused on this subject; and they have required balancing by those bodies. A significant case occurred in 2008, one related to MPs. Journalists had asked for detailed records of the expenditures of MPs—expenditures that not only related to their official office and travel expenses but also to subsidies they received for housing. Following a protracted series of decisions by the information commissioner, information tribunal, High Court, and Court of Appeals,[89] much of the information was released, based on its public interest. Some of this information was withheld on privacy grounds, but later leaked. It revealed some corrupt and unethical practices by MPs. In another case in 2008, the House of Lords ruled on the release of anonymous health statistics.[90] Separately, the information tribunal has ruled several times recently[91] on the identity of senior officials, establishing that they do not have a reasonable expectation of anonymity in any document (even sensitive ones); at the same time, junior officials may have this expectation, depending on the public nature of their jobs and when they meet with lobbyists. The tribunal also ordered the release of anonymous statistics on abortion.[92]

7 Conclusion

Access to information and protection of privacy are both rights intended to help the individual in making government accountable. Most of the time, the two rights complement each other. However, there are conflicts—for example, privacy laws often are improperly invoked by governments. And there are cases where the conflicts are legitimate.

There is no simple solution to balancing the two rights, but most issues can be mitigated through the enactment of clear definitions in legislation, guidelines, techniques, and oversight systems.

Of key importance is that governments take care when writing the laws to ensure that the access to information and data protection laws have compatible definitions of personal information. They should adopt appropriate public interest tests that allow for careful balancing of the two rights. Finally, they should create appropriate institutional structures that can balance these rights and ensure that data protection and right to information officials work together, even if they represent different bodies.

Endnotes

[1] For the purposes of this working paper, the terms "right to information laws," "access to information laws," and "freedom of information laws" refer to the same type of laws that provide for a legal right of access to information held by public bodies.

[2] See the Universal Declaration of Human Rights (UDHR), art. 19.

[3] For a detailed overview of international standards on RTI, see Mendel (2008) and Banisar (2006).

[4] In 2006, the Inter-American Court of Human Rights ruled that "the State's actions should be governed by the principles of disclosure and transparency in public administration that enable all persons subject to its jurisdiction to exercise the democratic control of those actions, and so that they can question, investigate and consider whether public functions are being performed adequately. Access to State-held information of public interest can permit participation in public administration through the social control that can be exercised through such access" (Marcel Claude Reyes et al. v. Chile, judgment of September 19, 2006).

[5] See, for example, ACHPR (2002); and the Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, and the OAS Special Rapporteur on Freedom of Expression, November 26, 1999.

[6] A global map of countries with access to information legislation is available at http://www.privacyinternational.org/foi/foi-laws.jpg.

[7] Writing on December 17, 1992, in Niemietz v. Germany (16 EHRR 97), the European Court of Human Rights noted, "The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life.'" For a detailed overview of the different rights, see EPIC/PI (2007).

[8] For example, see the following documents: UN Human Rights Committee (1988); UN Human Rights Council (2009); and Bensaid v. United Kingdom 44599/98 [2001] ECHR 82.

[9] For example, see the November 3, 2009, Madrid Privacy Declaration: Global Privacy Standards for a Global World, at http://thepublicvoice.org/madrid-declaration/.

[10] UDHR, art. 12.

[11] Ibid., art. 17.

[12] Ibid., art. 8.

[13] Ibid., art. 5, 9, and 10.

[14] Ibid., art. 11.

[15] For example, see Netherlands—CCPR/C/82/D/903/1999 [2004] UNHRC 60 (November 15, 2004), http://www1.umn.edu/humanrts/undocs/html/903-1999.html.

[16] APEC Privacy Framework, 2005, http://www.apec.org/About-Us/About-APEC/Fact-Sheets/Collection/APEC-Privacy-Framework.aspx.

[17] Also see Organisation of Eastern Caribbean States (2004).

[18] See also Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, June 20, 2007, at http://www.gov.gg/ccm/cms-service/download/asset/?asset_id=12058063.

[19] Copland v. United Kingdom (App. No. 62617/00) 2007.

[20] For example, see the constitutions of Albania (1998, sec. 35). Cape Verde (1999, sec. 42), the Former Yugoslav Republic of Macedonia (1992, sec.18), Mozambique (1990, sec. 71), and Thailand (2007, sec. 35).

[21] For a map of data protection laws around the world, see http://www.privacyinternational.org/survey/dpmap.jpg.

[22] See the Privacy Act of 1974, 5 USC 552(a). There is also a patchwork of sectoral legislation applying to heath, financial, and credit records; some telecommunications records; educational records; and other areas at both the national and state levels. For a comprehensive overview, see Solove and Schwartz (2008).

[23] General Administrative Code, sec. 27.

[24] Official Information Act, B.E. 2540 (1997).

[25] Malaysian Personal Data Protection Act, 2010.

[26] Freedom of Information: Consultation on Draft Legislation Cm 4355, May 1999, Response of the Data Protection Registrar.

[27] See Guadamuz (2001); and the Rule on the Writ of Habeas Data, issued by the Philippines Supreme Court (A. M. No. 08-1-16-SC, January 22, 2008, http://www.lawphil.net/judjuris/juri2008/jan2008/am_08-1-16_sc_2008.html).

[28] Canton's remarks of October 30, 2002, are available at http://www.wpfc.org/index.php?q=node/221.

[29] See Decision of the Supreme Administrative Court of Bulgaria No. 7146, July 30, 2004. An informative discussion of this decision can be found at http://www.aip-bg.org/library/dela/yonchev.htm.

[30] According to the Ninth FOI Report of the Irish Minister of Finance, 67 percent of all requests in 2008, 72 percent in 2007, and 70 percent in 2006 were for the applicants' personal information.

[31] For example, see *Times of India* (2010).

[32] The text of the act is available at http://www.sun.ac.za/university/Legal/dokumentasie/access%20to%20information.pdf.

[33] Only Antigua and Barbuda and South Africa have adopted laws that apply to private bodies "in the protection of any right."

[34] See, for example, *Sunday Times* (2008).

[35] Guerra and Others v. Italy, 116/1996/735/932, February 19, 1998.

[36] See EPIC v. DHS (Suspension of Body Scanner Program), http://epic.org/privacy/body_scanners/epic_v_dhs_suspension_of_body.html; EFF (2010); and public FOIA documents on spying in Washington, released by the American Civil Liberties Union, http://www.aclu-wa.org/public-documents.

[37] Taxpayers' Alliance is available at http://www.taxpayersalliance.com/.

[38] For salary disclosure in the United States, see Sunshine Review (2010). For salary disclosure in the United Kingdom, see ICO (2009) and BBC News (2010).

[39] However, also see Chang v. Navy, Civil Action No. 00-0783 (D. D.C.).

[40] Under European law, medical records are considered the most sensitive records to be protected from release. For example, see Z v. Finland (1997) 25 EHRR 371, http://www.unhcr.org/refworld/publisher,ECHR,,FIN,3ae6b71d0,0.html.

[41] For examples, see Djankov et al. (2009); World Bank (2006); People's Union for Civil Liberties (PUCL) v. Union of. India (2003) 4 SCC 399; CPIO Supreme Court of Delhi v. Subhash Chandra Agarwal, Delhi High Court, W.P. (C) 288/2009; Reid (2010); and CNN/IBN (2010).

[42] Von Hannover v. Germany (Application No. 59320/00), June 24, 2004.

[43] Decision 60/1994 (XII, 24) AB.

[44] Union of India v. Association for Democratic Reforms (2002) 2 LRI 305.

[45] The European Court of Human Rights ruled in 2004 that there was a public interest in a doctor revealing information that French President François Mitterand was seriously ill while in office and had hid that from the public. The court ruled that a temporary injunction was appropriate, but that a permanent one violated Article 10 of the European Convention on Human Rights (Éditions Plon v. France [Application No. 58148/00], May 18, 2004). A recent case from India ruled that medical information could be released if there was a sufficient public interest: "personal information including tax returns, medical records etc. cannot be disclosed in view of Section 8(1)(j) of the Act. If, however, the applicant can show sufficient public interest in disclosure, the bar (preventing disclosure) is lifted and after duly notifying the third party (i.e. the individual concerned with the information or whose records are sought) and after considering his views, the authority can disclose it" (Secretary General, Supreme Court of India v. Subhash Chandra Agarwal, High Court of Delhi, January 12, 2010).

[46] In some jurisdictions, tax records are publicly available. For example, see Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy (2008), EUECJ C-73/07, December 16; and Government of India (2009). Also see *Bangalore Mirror* (2010); Luna Pla and Ríos Granados (2010); and Law et al. News (2010).

[47] Nixon v. Warner Communications, Inc., 435 U.S. 589 (1978); Richmond Newspapers Inc. v. Virginia, 448 U.S. 555 (1980). For a review of Australian law, see Australian Law Reform Commission (2008).

[48] For example, the U.S. Court of Appeals for the District of Columbia noted, "The [U.S. FOIA] exemption . . . is phrased broadly to protect individuals from a wide range of embarrassing disclosures. As the materials here contain information regarding marital status, legitimacy of children, identity of fathers of children, medical condition, welfare payments, alcoholic consumption, family fights, reputation, and so on" (Rural Housing Alliance v. USDA, 498 F.2d 73 [D.C. Cir. 1974]).

[49] See "Social Audits—Tracking Expenditures with Communities: The Mazdoor Kisan Shakti Sangathan (MKSS) in India," available at http://unpan1.un.org/intradoc/groups/public/documents/un/unpan024549.pdf.

[50] For example, see the Web site for the Department of Rural Development of India's Ministry of Rural Development, http://www.nrega.nic.in/netnrega/home.aspx.

[51] For example, see Consejo Nacional de Ciencia y Tecnología, Convocatorias becas en el país 2009, http://www.conacyt.gob.mx/Convocatorias/Paginas/Convocatoria_Becas_Pais2009.aspx.

[52] In Mexico, information that is already in the public domain is not considered confidential and cannot be withheld from request. In 2008, the European Court of Justice ruled

that a news service using tax information from a public register was exempt from the EU Data Protection Directive. See Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy (2008), EUECJ C-73/07, December 16.

[53] The principles are available at http://legislation.knowledge-basket.co.nz/gpacts/reprint/text/2006/se/026se59.html. Also see Stewart (2002).

[54] Los Angeles Police Department v. United Reporting Publishing Corp., 528 U.S. 32 (1999).

[55] See the European Transparency Initiative Web site, http://ec.europa.eu/transparency/index_en.htm.

[56] "The few cases considering a private party attempting to influence government policy typically find in favor of disclosure, lacking countervailing concerns not present" (EFF v. ODNI, 09-17235, February 9, 2010). "Individuals are acting in a public or representative capacity, and would have an expectation that their details might be released to third parties" (Creekside Forum v. Information Commissioner and Department for Culture, Media, and Sport [2009] UKIT EA-2008-0065 [May 28]).

[57] Commission v. Bavarian Lager, Case C-28/08, June 29, 2010.

[58] For example, see http://ec.europa.eu/agriculture/funding/index_en.htm and http://farmsubsidy.org/.

[59] EUECJ cases C-92/09 and C-93/09, November 9, 2010.

[60] Testimony of Sir Richard Wilson before the Select Committee on Public Administration, U.K. House of Commons, July 11, 2002.

[61] See Volker und Markus Schecke (EUECJ C-92/09, November 9, 2010, at 85): "No automatic priority can be conferred on the objective of transparency over the right to protection of personal data . . . even if important economic interests are at stake."

[62] Canada (Information Commissioner) v. Canada (Commissioner of RCMP), 2003 SCC 8, October 29, 2003.

[63] Act No. LXIII of 1992, available at http://abiweb.obh.hu/dpc/index.php?menu=gyoker/relevant/national/1992_LXIII.

[64] In Tanzania, a draft bill introduced by the government in 2006 to address access to information, privacy, and media rights was more than 85 pages in length—a fact that led to its not being considered.

[65] Text of the act is available at http://www.sun.ac.za/university/Legal/dokumentasie/access%20to%20information.pdf.

[66] Indonesian Act on Public Information Disclosure No. 14 of 2008.

[67] For public officials, this would be a general notice setting out that information collected in the course of their official activities is not considered personal information that will be withheld. For private individuals, this area is more complex because data protection rights—especially relating to sensitive personal information—cannot simply be waived in many cases.

[68] 5 USC 552 (b)(6).

[69] Department of Air Force v. Rose, 425 U.S. 352 (1976).

[70] Case 99168—Mr. Richard Oakley, The Sunday Tribune newspaper and the Office of the Houses of the Oireachtas, July 27, 1999, http://www.oic.gov.ie/ga/CinntianChoimisineara/CinntiibhfoirmFhada/Name,1629,ga.htm.

[71] For more information on the roles and activities of oversight and appeals bodies, see Neuman (2009).

[72] Under Article 28(1) of European Union Directive 95/46/EC, data protection commissions "shall act with complete independence in exercising the functions entrusted to them." The European Court of Justice recently ruled, "[t]he guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the supervision of compliance with the provisions on protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established not to grant a special status to those authorities themselves as well as their agents, but in order to strengthen the protection of individuals and bodies affected by their decisions. It follows that, when carrying out their duties, the supervisory authorities must act objectively and impartially. For that purpose, they must remain free from any external influence, including the direct or indirect influence of the State or the Länder, and not of the influence only of the supervised bodies" (Case C-518/07, OJ May 1, 2010).

[73] Access to Information Commissioner, Annual Report of 1991–92, p. 16, http://www.oic-ci.gc.ca/eng/rp-pr-ar-ra-archive.aspx.

[74] However, the task force did state that the current situation was acceptable and did not recommend a merger of the two bodies.

[75] Remarks of the information commissioner of Canada to the Canadian Access and Privacy Association, October 28, 2003.

[76] Communication with Maeve McDonagh, April 2010.

[77] Communication with Elizabeth Dolan, Irish Information Commission, October 2010.

[78] Diario Oficial de la Federación, June 11, 2002, http://www.ifai.org.mx/transparencia/LFTAIPG.pdf.

[79] Diario Oficial de la Federación, January 12, 2011, http://dof.gob.mx/nota_detalle_popup.php?codigo=5175251.

[80] For more information about the commission, visit http://www.infodf.org.mx/web/.

[81] Decision No. 090-59/2009/, July 9, 2009.

[82] See the list of pertinent cases at http://www.ip-rs.si/index.php?id=384.

[83] Decision No. 021-124/2008/12, December 19, 2008.

[84] Decision No. 021-80/2005/6, November 2, 2005.

[85] Decision No. 090-94/2009, October 7, 2009. According to the ruling, records had "no direct connection with the performance of the public function of the body."

[86] Treaty No. 108, 1981, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

[87] For example, see Scottish Information Commissioner (2010) concerning the decision that release of childhood

leukemia statistics for a local area would violate the data protection law.

[88] For a detailed analysis, see U.K. Ministry of Justice (2008).

[89] Corporate Officer of the House of Commons v. Information Commissioner and others [2008] EWHC 1084 (Admin).

[90] Common Services Agency v. Scottish Information Commissioner [2008] UKHL 47.

[91] Alasdair Roberts v. Information Commissioner and Department for Business, Innovation and Skills (EA/2009/0035); Robin Makin v. Information Commissioner and Ministry of Justice (EA/2008/0048); Creekside Forum v. Information Commissioner and Department for Culture, Media, and Sport (EA/2008/0065).

[92] Department of Health v. IC (Additional Party: the Pro Life Alliance) (EA/2008/0074).

References

ABC News. 2009. "Ombudsman Calls for More Resources." November 2. http://www.abc.net.au/news/stories/2009/11/02/2730603.htm.

ACHPR (African Commission on Human and Peoples' Rights). 2002. "Declaration of Principles on Freedom of Expression in Africa." Banjul, The Gambia. http://www.achpr.org/english/declarations/declaration_freedom_exp_en.html.

Administrative Office of the U.S. Courts. 2008. "Judicial Conference Policy on Privacy and Public Access to Electronic Case Files." March. http://www.uscourts.gov/RulesAndPolicies/JudiciaryPrivacyPolicy/March2008RevisedPolicy.aspx.

Australian Law Reform Commission. 2008. *For Your Information: Australian Privacy Law and Practice.* Report 108, 3 vols. Sydney, NSW. http://www.austlii.edu.au/au/other/alrc/publications/reports/108/.

Bangalore Mirror. 2010. "Taxmen Deluged with "Ex" Files." September 23.

Banisar, David. 2006. *Freedom of Information Around the World 2006: A Global Survey of Access to Government Information Laws.* London, UK: Privacy International. http://www.privacyinternational.org/foi/foisurvey2006.pdf.

BBC News. 2001. "DTI Denies Smear Campaign Claims." January 8. http://news.bbc.co.uk/2/hi/uk_news/politics/1106142.stm.

———. 2010. "Thousands of Whitehall Salaries Published." October 15. http://www.bbc.co.uk/news/uk-politics-11551683.

Calland, Richard, and Alison Tilley, eds. 2002. *The Right to Know, the Right to Live: Access to Information & Socio-economic Justice.* Cape Town, South Africa: Open Democracy Advice Centre.

Cannon, Andrew. 2004. "Policies to Control Electronic Access to Court Databases." *University of Technology, Sydney, Law Review* 6: 37–46. http://www.austlii.edu.au/au/journals/UTSLRev/2004/3.html.

CNN/IBN. 2010. "PM to Disclose Assets of Cabinet Ministers." November 14. http://ibnlive.in.com/news/pm-to-disclose-assets-of-cabinet-ministers/134964-37-64.html?from=tn.

Commonwealth Secretariat. 2002. "Model Data Protection Act." London, UK. http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/{82BDA409-2C88-4AB5-9E32-797FE623DFB8}_protection%20of%20privacy.pdf.

Coronel, Sheila, ed. 2001. *The Right to Know: Access to Information in Southeast Asia.* Quezon City: Philippine Center for Investigative Journalism.

Council of Europe. 1981. "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data." European Treaty Series 108. Strasbourg, France. http://conventions.coe.int/treaty/en/treaties/html/108.htm.

———. 1986. "Recommendation 1037: On Data Protection and Freedom of Information." In *Texts Adopted at the 2nd Part of the 38th Ordinary Session of the Parliamentary Assembly, September 1986.* Strasbourg, France.

CSA (Canadian Standards Association International). 1996. "Model Code for the Protection of Personal Information." Toronto, Ontario.

Daily Mail. 2006. "Anger as Police Obtain Journalist's Mobile Records to Discover Source." December 1. http://www.dailymail.co.uk/news/article-419986/Anger-police-obtain-journalists-mobile-records-discover-source.html.

Djankov, Simeon, Rafael La Porta, Florencio Lopez-de-Silanes, and Andrei Shleifer. 2009. "Disclosure by Politicians." Working Paper 2009-60. Tuck School of Business at Dartmouth, Hanover, NH. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1334126.

EC (European Commission). 1995. "Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data." *Official Journal of the European Union* L281: 31–50. http://ec.europa.eu/justice/policies/privacy/law/index_en.htm.

ECOWAS (Economic Community of West African States). 2008. "Telecommunications Ministers Adopt Texts in Cyber Crime, Personal Data Protection." Press release 100/2008.

EFF (Electronic Frontier Foundation), 2010. "EFF Posts Documents Detailing Law Enforcement Collection of Data from Social Media Sites." Blog post, March 16. http://www.eff.org/deeplinks/2010/03/eff-posts-documents-detailing-law-enforcement.

EO (European Ombudsman). 2007. "Draft Recommendation to the European Parliament in Complaint 3643/2005/(GK) WP." September 24. Strasbourg, France. http://www.ombudsman.europa.eu/recommen/en/053643.htm.

EPIC/PI (Electronic Privacy Information Center/Privacy International). 2007. *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments.* Washington, DC. http://www.privacyinternational.org/survey/dpmap.jpg.

France, Elizabeth. 1999. Third Report of 1998–99, Freedom of Information Draft Bill, vol. II: HC 570-II of 1998–99, memorandum 2. London, UK.

Gentot, Michel. n.d. "Access for Information and Protection of Personal Data." Commission Nationale de l'Informatique et des Libertés. http://www.pcpd.org.hk/english/infocentre/files/gentot-paper.doc.

Government of Canada. 2002. *Access to Information: Making It Work for Canadians. Report of the Access to Information Review Task Force.* Ottawa, Ontario. http://www.atirtf-geai.gc.ca/accessReport-e.pdf.

———. 2009. "Info Source Bulletin Number 32B; Statistical Reporting. Statistical Tables 2008–2009, Access to Information." Ottawa, Ontario. http://www.infosource.gc.ca/bulletin/2009/b/bulletin32b/bulletin32b02-eng.asp#k.

Government of Canada, Office of the Privacy Commissioner. 2001. "Privacy Commissioner George Radwanski Writes to

Information Commissioner John Reid Regarding Prime Minister's Agendas Case." News release, May 10. http://www.privcom.gc.ca/media/nr-c/02_05_b_010510_e.asp.

Government of Hungary, Parliamentary Commissioner for Data Protection and Freedom of Information. 1998a. "Annual Report 1998." Budapest. http://abiweb.obh.hu/dpc/index.php?menu=reports/1998.

———. 1998b. "The First Three Years of the Parliamentary Commissioner for Data Protection and Freedom of Information." Annual reports 1991-96-97. Budapest. http://abiweb.obh.hu/dpc/index.php?menu=reports/1995.

Government of India, Central Information Commission. 2009. "Decision No. CIC/LS/A/2009/000647/SG/5887." December 14. http://rti.india.gov.in/cic_decisions/SG-14122009-32.pdf.

Government of Ireland, Department of Finance. 2006. "Data Protection and Freedom of Information in the Public Sector." Central Policy Unit, Notice No. 23. Dublin. http://www.dataprotection.ie/docs/%22Important_new_data_protection_guidance_for_all_public_/411.htm.

Government of Ireland, Information Commissioner. 1999. "Case 99168—Mr. Richard Oakley, The Sunday Tribune newspaper and the Office of the Houses of the Oireachtas." July 27. Dublin. http://www.oic.gov.ie/en/DecisionsoftheCommissioner/LongFormDecisions/Name,1629,en.htm.

Guadamuz, Andreas. 2001. "Habeas Data: An Update on the Latin America Data Protection Constitutional Right." Paper prepared for the 16th British and Irish Law, Education and Technology Association Annual Conference, University of Edinburgh, Scotland, April 9–16. http://www.bileta.ac.uk/Document%20Library/1/Habeas%20Data%20-%20An%20Update%20on%20the%20Latin%20America%20Data%20Protection%20Constitutional%20Right.pdf.

Hencke, David. 2001. "MP Challenges Secrecy Culture." *The Guardian,* June 27. http://www.guardian.co.uk/politics/2001/jun/27/freedomofinformation.uk.

Hencke, David, and Rob Evans. 2002. "Ashcroft Memos May Spur Data Law Repeal." *The Guardian,* February 5. http://www.guardian.co.uk/politics/2002/feb/05/uk.freedomofinformation.

———. 2003. "Ashcroft Wins Apology over Political Vendetta." *The Guardian,* June 6. http://www.guardian.co.uk/politics/2003/jun/06/uk.conservatives.

ICO (U.K. Information Commissioner's Office). 2009. "When Should Salaries Be Disclosed?" Version 1, February 23. http://www.ico.gov.uk/for_organisations/freedom_of_information/information_request/~/media/documents/library/Freedom_of_Information/Practical_application/SALARY_DISCLOSURE.ashx.

Irazábal, Alonso Lujambio, and Lina Ornelas Núñez. 2009. "Personal Data Protection by the Government: The Action of the Federal Institute for Access to Public Information." Mexico City, Mexico: Instituto Federal de Acceso a la Información y Protección de Datos.

Knight Center for Journalism in the Americas. 2010. "How Much Does Argentina's President Spend on Ads? An NGO Fights to Find Out." *Journalism in the Americas* news blog, March 26. http://knightcenter.utexas.edu/archive/blog/?q=en/node/6772.

Law et al. News. 2010. "Information on Religion Cannot Be Obtained under RTI." November 29. http://www.lawetalnews.com/NewsDetail.asp?newsid=2903.

Law Reform Commission, New South Wales. 2010. "Access to Personal Information." Report 126. Sydney, Australia. http://www.lawlink.nsw.gov.au/lawlink/lrc/ll_lrc.nsf/pages/LRC_r126toc.

Leith, Philip, and Maeve McDonagh. 2009. "New Technology and Researchers' Access to Court and Tribunal Information: The Need for European Analysis" *Scripted* 6 (1/April).

Luna Pla, Issa, and Gabriela Ríos Granados. 2010. *Transparencia, Acceso a la Información Tributaria y el Secreto Fiscal. Desafíos en México.* Mexico City: Universidad Nacional Autónoma de México. http://www.bibliojuridica.org/libros/libro.htm?l=2861.

Majtényi , László. 2002. "Freedom of Information, The Hungarian Model." http://www.lda.brandenburg.de/sixcms/media.php/2232/maitenyi.pdf.

McDonagh, Maeve. 2006. *Freedom of Information Law in Ireland*. 2nd ed. Dublin: Round Hall Sweet & Maxwell.

Mendel, Toby. 2008. *Freedom of Information: A Comparative Legal Survey.* 2nd ed. Paris, France: United Nations Educational, Scientific, and Cultural Organization.

Neuman, Laura. 2009. "Enforcement Models: Content and Context." Access to Information Working Paper Series. Washington, DC: World Bank. http://siteresources.worldbank.org/EXTGOVACC/Resources/LNEumanATI.pdf.

NJSBA (New Jersey State Bar Association). 2002. "Privacy and Electronic Access to Court Records in New Jersey." December 11. http://www.graysonbarber.com/pdf/Public%20Access%20to%20Court%20Records%2012-11-02.pdf.

NZLC (New Zealand Law Commission). 2008. *Public Registers: Review of the Law of Privacy, Stage 2*. Report 101, January. Wellington, New Zealand. http://www.lawcom.govt.nz/sites/default/files/publications/2008/02/Publication_129_391_Public_registers_web_72.pdf.

OAS (Organization of American States). 2003. "Access to Public Information: Strengthening Democracy." AG/RES. 1932 (XXXIII-O/03) June 10. Washington, DC. http://www.oas.org/juridico/english/ga03/agres_1932.htm.

OECD (Organisation for Economic Cooperation and Development). 1980. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." Paris, France. http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

Organization of Eastern Caribbean States. 2004. "Privacy Bill." Proposed draft. http://unpan1.un.org/intradoc/groups/public/documents/TASF/UNPAN024634.pdf.

Pirc Musar, Natasa. 2006. "New Principles of the Amended Act on Access to Public Information in Slovenia: Commissioner or Ombudsman." Ljubljana, Slovenia. http://www.ip-rs.si/fileadmin/user_upload/Pdf/konference/Novosti_ZDIJZ_Manchester_ang.pdf.

———. 2010. "How to Strike the Right Balance between Freedom of Information and Personal Data Protection: Using a Public Interest Test." PhD diss., Leiden University, The Netherlands.

Reid, Tyrone. 2010. "Crusade Against Secrecy—Public Barred from Viewing Financial Disclosures of Elected Officials." *Ja-*

maica Gleaner. November 14. http://jamaica-gleaner.com/gleaner/20101114/lead/lead1.html.

Scottish Information Commissioner. 2009. "Decision Notice: Decision 115/2007, Mr. Joseph Millbank and Dundee City Council." St. Andrews. http://www.itspublicknowledge.info/UploadedFiles/Decision115-2007.pdf.

———. 2010. "Decision Notice: Decision 21/2005, Mr. Michael Collie and the Common Services Agency for the Scottish Health Service." St. Andrews. http://www.itspublicknowledge.info/UploadedFiles/Decision021-2005.pdf.

Sheridan. Gavin. 2010. "Department of Arts, Sport and Tourism Expenses Database." The Story, March 12. http://thestory.ie/2010/03/12/departments-expenses-database/.

Slane, Bruce. 2002. "Freedom of Information and Privacy: Competing Interests with Complementary Aims." Paper prepared for the International Symposium on Freedom of Information and Privacy, Auckland, New Zealand, March 28.

Solove, Daniel J., and Paul Schwartz. 2008. *Information Privacy Law.* 3rd ed. New York: Aspen Publishers.

Stewart, Blair. 2002. "Public Register Provisions—Addressing Privacy Issues." Paper prepared for the International Symposium on Freedom of Information and Privacy, Auckland, New Zealand, March 28.

Sunday Times. 2008. "Couple Stung by £100,000 'Secret' Loan." December 7. http://www.timesonline.co.uk/tol/news/uk/article5299156.ece.

Sunshine Review. 2010. "Public Employee Salary." http://sunshinereview.org/index.php/Public_employee_salary.

Tang, Raymond. 2002. "Data Protection, Freedom of Expression and Freedom of Information: Conflicting Principles or Complementary Rights?" Paper presented at the 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, Wales, September 9–11. http://www.pcpd.org.hk/english/infocentre/speech_200210911.html.

The Times of India. 2010. "RTI Helps Poor Diamond Polishers Get Back Cancelled BPL Cards." August 24. http://timesofindia.indiatimes.com/city/rajkot/RTI-helps-poor-diamond-polishers-get-back-cancelled-BPL-cards/articleshow/6428102.cms.

U.K. Home Office. 1999. "Freedom of Information: Preparation of Draft Legislation: Background Material." May. London. http://www.publications.parliament.uk/pa/cm199899/cmselect/cmpubadm/570/57007.htm.

U.K. Ministry of Justice. 2008. "Freedom of Information Guidance: Exemptions Guidance, Section 40-Personal Information." May 14. London. http://www.justice.gov.uk/about/docs/foi-exemption-s40.pdf.

———. 2009. "Freedom of Information Act 2000. Fourth Annual Report on the Operation of the FOI Act in Central Government 2008." June. London. http://www.justice.gov.uk/freedom-of-information-annual-report-2008.pdf.

———. 2010. "Freedom of Information Act 2000. 2009 Annual Statistics on Implementation in Central Government." April 29. London. http://www.justice.gov.uk/foi-statistics-report-2009.pdf.

UN (United Nations). 1948. "Universal Declaration of Human Rights." New York. http://www.un.org/en/documents/udhr/index.shtml.

UN General Assembly. 1990. "Guidelines for the Regulation of Computerized Personal Data Files" A/RES/45/95, December

14. New York. http://www.un.org/documents/ga/res/45/a45r095.htm.

UN Human Rights Committee. 1988. Covenant on Civil and Political Rights General Comment 16 (Article 17: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation), April 8. http://www.bayefsky.com/general/ccpr_gencomm_16.php.

UN Human Rights Council. 2009. Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism. A/HRC/13/37. December 28. http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf.

U.S. Department of Health, Education, and Welfare. 1973. "Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems July, 1973." Washington, DC. http://aspe.hhs.gov/DATACNCL/1973privacy/tocpreface members.htm.

U.S. Department of Justice, Office of Information Policy. 2010. "Summary of Annual FOIA Reports for Fiscal Year 2009." Washington, DC. http://www.justice.gov/oip/foiapost/2010foiapost18.htm.

Waters, Nigel. 2002. "Privacy Exemptions in FOI Laws—An Unnecessary Barrier to Accountability" Paper prepared for the International Symposium on Freedom of Information and Privacy, Auckland, New Zealand, March 28.

Working Party on the Protection of Individuals with Regard to the Processing of Personal Data. 1999. "Opinion No. 3/99 on Public Sector Information and the Protection of Personal Data." May 3. Brussels, Belgium. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp20en.pdf.

World Bank. 2006. "Income & Asset Disclosure Requirements for Heads of State and Governments, World Bank Client Countries." Washington, DC. http://siteresources.worldbank.org/INTLAWJUSTINST/Resources/IncomeAssetDisclosureinWBClientsasofJune62006.pdf.

About the World Bank Institute's Governance Practice

Governance is one of seven priority themes in the World Bank Institute's recently launched renewal strategy—a strategy that responds to client demand for peer-to-peer learning by grounding WBI's work in the distillation and dissemination of practitioner experiences. The Institute is committed to building knowledge and capacity on the "how to" of governance reforms, with emphasis on supporting and sustaining multistakeholder engagement in bringing about such reforms.

WBI's Governance Practice works with partners, including networks of country and regional institutions, to develop and replicate customized learning programs. Its programmatic approach aims at building multistakeholder coalitions and in creating collaborative platforms and peer networks for knowledge exchange.

For further information:
WBI
The World Bank
1818 H Street, NW
Washington, DC 20433
Fax: 202-522-1492

Visit us on the web at: http://wbi.worldbank.org/wbi/topics/governance

Photo Credit: (Front Cover) iphotostock.com.