Equality and Human Rights Commission
Research report 69

Protecting information privacy

Charles Raab and Benjamin Goold

University of Edinburgh and
University of British Columbia

Equality and Human Rights Commission

First published Summer 2011

ISBN 978 1 84206 347 7

Equality and Human Rights Commission Research Report series

The Equality and Human Rights Commission Research Report Series publishes research carried out for the Commission by commissioned researchers.

The views expressed in this report are those of the authors and do not necessarily represent the views of the Commission. The Commission is publishing the report as a contribution to discussion and debate.

Please contact the Research Team for further information about other Commission research reports, or visit our website:

Research Team

Equality and Human Rights Commission

Arndale House

The Arndale Centre

Manchester

M4 3AQ

Email: research@equalityhumanrights.com

Telephone: 0161 829 8500

Website: www.equalityhumanrights.com

If you require this publication in an alternative format, please contact the Communications Team to discuss your needs at: communications@equalityhumanrights.com

Contents

Acknowledgements

We are grateful to the Equality and Human Rights Commission for their support during the writing of this report, and to the various experts and referees who offered comments and suggestions at formative stages and on subsequent drafts. We also thank Fiona McGrath for providing invaluable assistance and for her help in the preparation of the final report.

Charles Raab
Benjamin Goold

January 2011

Executive summary

Background

This report for the Equality and Human Rights Commission (the Commission) examines the threats to information privacy that have emerged in recent years, focusing on the activities of the state. It argues that current privacy laws and regulation do not adequately uphold human rights, and that fundamental reform is required. It identifies two principal areas of concern: the state's handling of personal data, and the use of surveillance by public bodies.

Privacy concepts have a long tradition in Britain and can be traced back in common law and, more recently, appear in the Universal Declaration of Human Rights. Today, the right to privacy is contained in Article 8 of the European Convention on Human Rights (ECHR), and is incorporated into UK law through the Human Rights Act (HRA) 1998. As a statutory body, the Commission has a duty to encourage compliance with the HRA and other human rights obligations under international treaties.

Developments in information technology and the purposes of state policy and the private sector mean that we are now more vulnerable than ever to unwanted surveillance. There is a growing demand for personal information from both the public and private sectors. New technology allows organisations to store, analyse and share such information in increasingly complex ways. Although recent legislation has attempted to strengthen information privacy, the law has not kept pace with changes in technology and in the uses to which it is put.

As a result, evidence suggests that the state is failing adequately to uphold the right to privacy. There has been widespread concern regarding the expansion of government databases and the processing of personal data. The Regulation of Investigatory Powers Act (RIPA) 2000, which governs the use of surveillance by the police, local authorities and other public bodies, is marred by ambiguity, leaving open the possibility of serious errors, inadvertent use of illegal surveillance techniques, and inappropriate use of surveillance powers. Surveillance is increasingly becoming a feature of everyday life in areas we previously considered private. There are concerns about the proliferation of CCTV and its lack of regulation, as well as about the potentially chilling effects of surveillance on, for example, peaceful protest. It is little wonder, in this context, that privacy has become a key public concern.

Overall finding

The central finding of this report is that the existing approach to the protection of information privacy in the UK is fundamentally flawed, and that there is a pressing

need for widespread legislative reform in order to ensure that the rights contained in Article 8 are respected. The report argues for the establishment of a number of key 'privacy principles' that can be used to guide future legal reforms and the development of sector-specific regulation.

Key findings

- The privacy landscape has been transformed in recent years by a series of landmark legislative reforms, including the HRA, the DPAs of 1984 and 1998, and RIPA.

- There has also been a dramatic increase in the amount of personal information held by the public sector, due to technological developments and a steady expansion of the role of the state.

- The current system has a weak, fractured and piecemeal approach to privacy. Acts such as the DPA and RIPA are riddled with gaps and contradictions, and are also interpreted, administered and overseen by a range of separate regulators, independent tribunals, and courts. As a consequence, it has become very difficult for individuals to understand what happens to their personal information, or what they should do when that information is misused. The current system has failed to protect privacy rights in a number of cases.

- The problem is likely to become more acute. The state's demands for personal information will continue to grow in relation to national security, law enforcement and citizens' access to public services. So far, this expansion has been accompanied by only a relatively small increase in the powers or resources available to regulatory authorities such as the Information Commissioner's Office or the various Commissioners in the field of surveillance.

- A more flexible, comprehensive approach to privacy is needed, based on a firm commitment to Article 8 of the ECHR. This involves reforming the law and the regulatory system to create a comprehensive privacy protection regime to supersede the piecemeal inventory of measures or 'tools' implemented in a disjointed fashion by various agents. The relevant regulatory agencies need to be strengthened.

- Law is essential: without legal specification of privacy rights, other instruments are likely to be incapable of providing the remedies that individuals may need. The law needs to be flexible enough to respond to the many and varied threats to privacy.

- The principles written into law or underpinning it must be reflected in the specification of other instruments. These are seen as reinforcements and complements to the law and not as substitutes for, or weaker versions of, privacy laws.

- There are many ways of protecting privacy in addition to legal provisions, including self-regulatory approaches, 'privacy-enhancing technologies', ‘privacy by design’, and public awareness and education. Such complementary, non-legal approaches to the protection of information privacy have an important part to play in upholding information privacy rights.

Recommendations

This report makes four main recommendations:

(1) A clear set of ‘privacy principles’ should be developed and used as the basis for future legislation, and to guide the decisions of regulators and government agencies concerned with information privacy and data collection in different contexts.

(2) Existing legislation that touches on privacy should be reformed to ensure that it is consistent with the privacy principles recommended earlier, and that it enhances – rather than undermines – the existing provisions of the HRA. At minimum, such reform should consolidate and improve the existing RIPA and data protection regimes in relation to information privacy and surveillance.

(3) Greater regulatory coherence should be promoted. There should be an effort to rationalise and consolidate the current approach to the regulation of surveillance and data collection in the UK, with particular attention paid to the relationship between the various statutory Commissioners responsible for protecting information privacy.

(4) Improved technological, organisational, and other means of protection should play an integral part in information privacy protection. The development and use of technological and non-legal solutions to the problem of information privacy protection should be encouraged by government, and more resources devoted to public education and awareness around privacy.

The right to privacy is at risk of being eroded by the growing demand for information by government and the private sector. Unless we start to reform the law and build a regulatory system capable of protecting information privacy, we may soon find that it is a thing of the past.

1. Introduction

1.1 Background

Privacy has a long history in Britain. Concepts related to privacy can be traced back in the common law and, more recently, in the Universal Declaration of Human Rights. The Data Protection Act (DPA) 1984 first developed statutory protections for information privacy. Under Article 8 of the European Convention on Human Rights (ECHR), everyone has the 'right to respect for his private and family life, his home and his correspondence'. Incorporated into domestic law by the Human Rights Act (HRA) 1998, Article 8 now provides an overarching framework for the protection of privacy in the UK, as well as a set of principles that can be used to guide the development of privacy and data protection laws in this country.

Yet despite the fact that there is now a clear right to privacy in the UK, over the past 10 years that right has come under increasing pressure from the state. Although the spread of public space CCTV and the introduction of full body scanners in airports such as Heathrow and Manchester are among the more visible signs of this 'assault on privacy', increasingly the threat comes from the day-to-day work of government departments, public bodies, and local authorities. As the state collects more and more information about its citizens, and as developments in technology make it easier to process and share this information, there is a danger that the protections provided by Article 8 and existing UK data protection laws will be gradually eroded.

In recent years, the proliferation of government databases, a number of high-profile data losses and examples of over-zealous police and local authority surveillance have helped to highlight the threat to privacy posed by the state. The National DNA database was found to be unlawful in the case of In *S. & Marper v United Kingdom* where the European Court of Human Rights (ECtHR) found that the system of indefinite retention of DNA samples, profiles and fingerprints of those who had not been convicted of a crime breached Article 8 privacy rights. The Government is currently proposing changes to the database. In recent years, widespread public concern has been raised regarding proposals for other databases, not least that of a national identity database.

In November 2007, the Government revealed that Her Majesty's Revenue and Customs (HMRC) had lost a computer disc containing the child benefit records of over 25 million people.[1] Less than a month later, the Government then disclosed that a computer hard drive had also gone missing in the USA, this time with the personal details of some three million UK learner drivers. Speaking to the House of Lords Select Committee on the Constitution in the wake of these revelations, the then Information Commissioner, Richard Thomas, observed that such losses had not only

damaged public confidence in the Government's ability to handle sensitive information, but had also raised serious concerns about the protection of information privacy in the UK:

> Concerns are increasing … We know now that something like nine out of ten people ... have concerns about the security of their personal information ... [and] 60 per cent are saying that they feel they have lost control over the way in which their personal information is being used.[2]

Controversy has also arisen over the growing use of covert surveillance tactics in the UK, not only by the police, but also by local authorities and other public bodies and the adequacy of the oversight regime of the Regulation of Investigatory Powers Act (RIPA). According to a report published by Big Brother Watch in May 2010, in the last two years 372 local authorities have made use of surveillance powers contained in RIPA 2000, and have between them carried out over 8,500 separate surveillance operations (Big Brother Watch, 2010; Travis, 2010). Not only have these powers been used to prevent dog fouling, fly tipping, and to ensure that government employees do not abuse parking privileges or sick leave, they have also been used to monitor individuals suspected of breaking the newly imposed smoking ban. More recently, a plan to establish a network of more than 200 CCTV cameras in and around the predominantly Muslim areas of Sparkbrook and Washwood Heath in Birmingham has led to renewed public concern about the use of police surveillance powers, not least because of the lack of public consultation and potential threat to individual privacy (Thames Valley Police, 2010).

RIPA has been commented on by the courts as 'a particularly puzzling statute' and 'perplexing'.[3] The system of internal self-authorisation, without the requirement for judicial oversight, has given rise to concern and leaves open the possibility of serious errors and inadvertent use of otherwise illegal surveillance techniques. For example, the courts recently found that internal authorisation was inappropriate where the interference was with legal professional privilege. Further problems come to light in relation to public spaces. There is no current statutory regime for the regulation of CCTV cameras, despite the recommendations of the House of Lords. As such, it is difficult for individuals who believe their privacy rights have been violated by the use of CCTV to obtain a remedy under the law. Furthermore, the use of CCTV and other public surveillance techniques can have a significant chilling effect on free speech and peaceful protest, as the Court of Appeal noted in one case, finding that the taking and retention of photographs by the police of protestors was disproportionate.[4]

Although it is clear that the public is deeply concerned about the steady expansion in state surveillance and how their personal information is being used and protected, there are also growing fears about the discriminatory effects of surveillance and data

collection. According to separate reports published by the Commission (Equality and Human Rights Commission, 2009) and GeneWatch (Staley, 2005), the National DNA Database not only poses a danger to the privacy of the public at large, but also has the potential to reinforce existing patterns of disadvantage and discrimination. As the Commission's report notes, black men, young children, and people with mental health conditions are already over-represented on the database, and there is evidence to suggest that the proportion of Asian people on the database is increasing beyond their proportion to the general population.[5] Initiatives such as the National DNA Database not only threaten to divide the UK into a country of privacy 'haves' and 'have-nots', but they also have the potential to undermine the general protections guaranteed by Article 8 and the HRA. As the ECtHR observed in the 2008 case of *S and Marper v UK*, while the state may be justified in using advanced technologies in the fight against crime, it also has a special responsibility for ensuring that privacy and personal information are properly protected.[6]

In the 2010 Queen's Speech, the new Government acknowledged many of these concerns, and announced a series of reforms aimed at curbing the spread of surveillance in the UK. In particular, it pledged to abolish identity cards and the National Identity Register, the ContactPoint database on children, and indicated that it would abandon the next generation of biometric passports. ContactPoint has now been abolished, and many of the Government's other policy commitments are already in the process of being fulfilled. Further, the Government has indicated that it will limit the retention of information on the National DNA Database, introduce a new regulatory framework for CCTV, and outlaw the fingerprinting of children at school without parental permission. These reforms represent a significant shift in government thinking about the importance of privacy and the need for clear limits on state surveillance and data collection.

However, as this report will show, there is much more to be done. As UK privacy law has struggled to keep pace with the demands of government and changes in the technology of information gathering and data sharing, the protection of information privacy has become increasingly fragmented and incoherent. In addition to the protections provided by Article 8 and the HRA, aspects of individual privacy in the UK are also governed by the Data Protection Act (DPA) 1998, RIPA, and the common law. The situation is further complicated by the fact that although Scotland and Northern Ireland are subject to the HRA, they also have their own distinct legislative regimes when it comes to matters of privacy and data protection. Equally, there is considerable confusion surrounding the regulation of surveillance by the police and security services, and the role of the various bodies responsible for monitoring them and enforcing the law. In part, some of this confusion has arisen from the ambiguity that surrounds the rules and procedures set out in RIPA.[7] It is also, however, a

function of the fact that there is considerable overlap between the powers and responsibilities of the various commissioners responsible for protecting privacy in the UK, as well as large gaps in the regulatory frameworks in which they currently operate. Finally, there is also a lack of public and political understanding about the importance of privacy, how surveillance works, and the types of legal redress available to individuals who can prove they have been harmed by the misuse of their personal information.

If the current programme of legislative reform is to be successful, it must be accompanied by a more fundamental review of law regarding information privacy and the regulation of surveillance and data collection in the UK. Taking the right to privacy contained in Article 8 of the ECHR as our starting point, there is a clear need for a more coherent approach to the problem of reconciling privacy with competing interests such as security, crime prevention, and the efficient delivery of public services. It is also important to ensure that any changes to the existing law of privacy and the regulation of surveillance are consistent with the principles set out in the HRA, and strengthen the right to respect for private and family life contained in Article 8 of the ECHR.

1.2 The aim of the report

As a statutory body, the Commission has a duty to promote equality, build good relations and protect human rights, and encourage compliance with the HRA and other human rights obligations under international treaties (Equality Act 2006, Section 9). In fulfilling these roles, and as a modern regulator, it is appropriate for the Commission to consider the protection of information privacy. Government has a responsibility to ensure that the information gathering and surveillance activities of the state are consistent with the right to respect for private and family life, and that any infringement of this right is proscribed by law, properly justified, necessary, and proportionate. Further, the state has positive obligations to ensure protection of Convention rights; this could include requirements to establish a sufficient statutory and regulatory framework to ensure that Convention rights, including Article 8 rights, are not infringed.

The aim of the report is to provide an overview of the current state of information privacy law and surveillance regulation in the UK, with a particular focus on the question of whether the rights contained in Article 8 of the ECHR are being adequately protected. The report also examines various approaches to the legal protection of privacy and the regulation of surveillance and data collection, identifies weaknesses in the current approach to privacy and surveillance, and makes a series of recommendations aimed at ensuring that the rights contained in Article 8 are respected. Although this report is not intended to provide a detailed blueprint for the

protection and regulation of information privacy, it aims to develop the Commission's expertise in this important area, and seeks to establish the Commission as a key contributor to the ongoing debate about the future of privacy in the UK.

The scope of the report is limited in four main ways. First, it focuses on one particular aspect of privacy: information privacy. As a result, although the report touches on aspects of physical privacy – such as an individual's right to privacy in their body or their home – its main concern is with the collection, use, and communication of personal information. Information privacy is affected by what happens in other dimensions insofar as personal data may be collected through processes associated with them – for instance, body searches and scanning, or electronic tagging. But it is not practical to investigate all dimensions in a report of this nature, although the human rights issues as well as certain recommendations are also germane to a multidimensional view of privacy.

Second, because one of the key responsibilities of the Commission is to ensure that government and the public sector respect the rights set out in the HRA, this report focuses on threats to information privacy arising from the activities of the state. Although the growing use of personal information by the private sector also poses a significant challenge to privacy, this report only considers the private sector insofar as it acts in conjunction with the state as is, for example, increasingly the case in the areas of health care and social services.

Third, this report does not attempt to deal with the relationship between information privacy and the media. Even though many well-known privacy cases involve media coverage of prominent politicians, business people, and celebrities, a detailed consideration of the complex issues surrounding the relationship between the right to privacy and the right to freedom of expression is beyond the scope of a report of this length.

Fourth, although this report is concerned with the protection of information privacy in the UK, its main focus is on England and Wales. References to the relevant law in Scotland – which is based, in part, on a different legislative and regulatory framework – are included largely for purposes of comparison, and the position in Northern Ireland is not considered. Applicable laws are treated as uniform throughout the UK except where otherwise indicated. Nonetheless, any reform of the law must take account of differences between the UK's three legal jurisdictions and the devolution settlements in Scotland, Wales, and Northern Ireland.

Central to this report are two key assumptions. First, that any reform of the existing law must take place within the broad framework established by the HRA. By

incorporating Article 8 of the ECHR into domestic law – which establishes that all individuals have a right to respect for their private and family life – the HRA fundamentally changed the way in which privacy is understood in the UK, and substantially increased the level of protection afforded to individual privacy in both the public and private sectors. This report takes the provisions of the HRA as its starting point, and as a consequence the reforms proposed are all intended to enhance the protections provided by Article 8.

The second assumption is that it is important for the government and parliament to be clear about the requirements of Article 8 of the Convention, and what it is that privacy laws and other means of regulation seek to protect. For the law of privacy and the regulation of surveillance and data collection to develop in a coherent and consistent way, future reforms must be guided by a commitment to a clear set of principles. In this report, a number of justifications of privacy are examined, with a view to explaining how these alternative accounts of privacy lead to different conclusions about the role of the law and legal regulation. By relating the specific proposals presented in this report to these justifications, we hope to provide a better insight into the choices available and to provide lawmakers with a principled framework for future reform.

1.3 Structure of the report

Following on from this introduction, Chapter 2 provides a brief overview of the key challenges and threats to information privacy, with a particular focus on the various social and technological trends that have emerged in recent years. Although successive UK governments have sought to provide protection for privacy through a range of statutes and a complex system of regulation, what has emerged is a weak, fractured and piecemeal approach to privacy that is ill-equipped to deal with challenges that lie ahead. This Chapter stresses the need to develop a more flexible, comprehensive approach to the protection of privacy, based on a firm commitment to Article 8 of the ECHR and a combination of both principles-based regulation and non-legal protections.

Chapter 3 then looks at why privacy matters. It highlights several prominent and overlapping theories of privacy that have influenced existing approaches to regulation, and emphasises the importance of taking a context-specific approach to issues of information privacy. In particular, this Chapter considers which approaches to privacy are most likely to enhance – rather than undermine – the rights contained in Article 8 of the ECHR and the existing framework of data protection in the UK.

In Chapter 4, the report then turns to a detailed analysis of the various laws and regulations that govern the data protection and privacy in the UK. Using various

recent examples and cases, this Chapter argues that the current framework is no longer fit for purpose, and in urgent need of rationalisation and reform. In addition to emphasising the need for greater legislative consistency and regulatory coherence, the report argues that more attention needs to be paid to the requirements of Article 8, and the need to consider complementary, non-legal approaches to the protection of information privacy.

Chapter 5 examines various complementary approaches to the protection of personal data, including the use of codes of practice and statutory guidelines. In addition, it discusses various non-legal means of protecting information privacy – such as 'privacy-enhancing technologies', 'privacy by design', and 'privacy impact assessment' – all of which aim to ensure that organisations pay more attention to privacy and to see that their data handling practices are consistent with the demands of Article 8. The Chapter also considers the importance of public awareness and education programmes, and the need for regulators, non-governmental organisations, and the media to play a greater role in helping the public to protect their own privacy.

In Chapter 6, a number of new approaches to the protection of information privacy are considered. These include new legislation aimed at consolidating the current law, and a re-organisation of the existing system of privacy regulation and Commissioners. In addition, this Chapter argues in favour of the incorporation of more 'soft law' and technical means of privacy protection. However, establishing these reforms requires a foundation of principles – related to concepts of privacy – as the touchstone for information privacy protection. The report finds that 'principles-based regulation' and legislation can reformulate existing principles, supplementing them by further ones reflecting changing technological and policy circumstances as well as contextual variations shaping individuals' experience of privacy. In addition, reform must involve other participants and policy actors besides lawmakers and regulators.

Based on this, Chapter 7 makes four specific recommendations:

(1) That there is a need for the development of a clear set of 'privacy principles' that can be used as the basis for future legislation, and which can be used to guide the decisions of regulators and government agencies concerned with information privacy and data collection in different contexts.

(2) Existing legislation that touches on privacy should be reformed to ensure that it is consistent with the privacy principles recommended earlier, and that it enhances – rather than undermines – the existing provisions of the HRA. At

minimum, such reform should consolidate and improve the existing RIPA and data protection regimes in relation to information privacy and surveillance.

(3) That an effort should be made to rationalise and consolidate the current approach to the regulation of surveillance and data collection in the UK, with particular attention being paid to the relationship between the various statutory Commissioners responsible for protecting information privacy.

(4) That the use of technological and non-legal information privacy protections should be encouraged by government, and that more resources should be devoted to public education and awareness around privacy.

Chapter 8 concludes the report by restating that information privacy is a fundamental right which is at risk of being eroded by the growing demand for information by government and the private sector. It urges the reform of law and the creation of a regulatory system capable of protecting information privacy in order to preserve the right to privacy in future.

2. The changing landscape of privacy

2.1 Introduction

In recent years the landscape of privacy has changed dramatically in the UK. New information technologies and forms of communication have continued to emerge and develop, and have presented the public and private sectors with a host of new ways of collecting, processing, and sharing the personal information of their clients and customers. At the same time, although a series of landmark legislative reforms – most notably the introduction of the HRA 1998, the Data Protection Act (DPA) 1998, and the Regulation of Investigatory Powers Act (RIPA) 2000 – have transformed how the UK approaches data collection and state surveillance, over the last 10 years the law and other regulatory mechanisms have struggled to keep up with the pace of technological change or to develop a comprehensive framework for the protection of information privacy.

We have also seen a rise in public interest in privacy, and a growing anxiety about the prospect of the UK being transformed into a 'surveillance society' (Ford, 2004; Surveillance Studies Network, 2006). According to a report analysing the Information Commissioner's Office's (ICO) tracking of public attitudes (SMSR, 2010), protecting personal information continues to be of great concern to the general public. Indeed, only prevention of crime ranks higher. Overall, a majority of the UK public continues to lack confidence in the way their personal information is protected and handled, with 60 per cent believing that they have lost control over the way personal data is collected and processed.

Thomas and Walport's (2008) review of data sharing also underlined this point, referring to a number of high profile incidents involving the loss of personal data by government that have only heightened public anxiety over how their data is looked after. In October 2007, for example, two computer discs owned by HM Revenue and Customs with the personal details (names, addresses, National Insurance numbers and bank details) of all families in the UK who were claiming benefits went missing when the disks were sent by a junior officer via TNT courier to the National Audit Office. It was later revealed that the data protection manual for HMRC staff was itself under restriction and available to only senior members, not junior civil servants. In addition, the ICO has recently highlighted further examples of serious data losses, including:

- The theft of two unencrypted laptops containing personal information relating to 17 patients, which were stolen from the Medical Day Centre of Birmingham Children's Hospital. The data included patient diagnoses, video recordings and information on the health of individual patients. (July 2010)

- The loss of a CD containing scans of 112 patient records from the Intensive Care Unit of New Cross Hospital. The CD was discovered at a bus stop near the hospital and was unencrypted with no password protection. (August 2010)

- The loss of an unencrypted USB stick containing sensitive data of patients' conditions and medication, mislaid on a train journey by a junior doctor employed by East & North Hertfordshire NHS Trust. It has not yet been recovered. (September 2010)

- The loss of an unencrypted memory stick containing personal information held by the Forth Valley NHS Board, which was later handed in to the press. Enquires established that the information had been uploaded by a member of staff onto a personally owned memory stick that was then lost. (September 2010)

As a consequence of changes in technology, communications, and public attitudes to personal information, the landscape of privacy in the UK is now drastically different from that which existed even a decade ago. Although the law, and society generally, are now faced with a range of difficult choices when it comes to the question of how best to regulate the use of personal data and protect individual privacy, there is clearly a public appetite for change and reform. Put simply, the landscape of privacy has never been as fluid as it is in 2010, nor has there been a more opportune moment for reform and the strengthening of a rights-based approach to the protection of information privacy.

This Chapter provides a brief overview of the key challenges and threats to information privacy in the UK, and identifies some of the major social and technological trends that have and continue to transform the landscape. It touches on a wide range of social, technological, and legal issues that will be developed throughout this report, with a view to providing a perspective on the challenges and opportunities ahead as regards the protection of information privacy in the UK.

2.2 Information privacy: challenges, concerns, and responses

Although privacy is by its very nature a fragile right, (Goold, 2007) personal information privacy is under particular threat in today's 'information economy' and 'information-age government'. Advanced systems of information and communication technology (ICT) now collect, process, and share information about every aspect of an individual's life, information that is used to construct profiles of our habits and behaviour, track our location and movements, evaluate risks and opportunities, and shape policies and business plans. As the House of Lords Select Committee on the Constitution noted in 2009:[8]

> Surveillance is an inescapable part of life in the UK. Every time we make a telephone call, send an email, browse the Internet, or even walk down our local high street, our actions may be monitored and recorded. To respond to crime, combat the threat of terrorism, and improve administrative efficiency, successive UK governments have gradually constructed one of the most extensive and technologically advanced surveillance systems in the world. At the same time, similar developments in the private sector have contributed to a profound change in the character of life in this country. The development of electronic surveillance and the collection and processing of personal information have become pervasive, routine, and almost taken for granted. Many of these surveillance practices are unknown to most people, and their potential consequences are not fully appreciated. (House of Lords 2009, para. 1)

The ability to collect and process personal information is essential to law enforcement, national security, and public sector service delivery. Yet although information systems and data sharing have always been a central part of the modern state's bureaucratic infrastructure, technological developments and a steady expansion in the role of government have resulted in a dramatic increase in the amount of personal information held by the public sector in recent years. In order to maintain the UK's borders, provide effective policing, and combat the threat of terrorism, successive governments have argued that it is vital for the state to be able to obtain, access, process, and share large amounts of these confidential details. Furthermore, as the line between the public and private sectors has continued to blur, this information is increasingly being shared. Add to this the growing popularity of internet shopping, online banking, and social networking sites like Facebook, and it is easy to see why data regulation and governance has become steadily more complex.

As more information is made available and shared between organisations, the danger that this information will be misused, misplaced or misunderstood increases. People may, for example, consent to provide information to an organisation for one purpose and then later discover that the same (or some other) organisation has used it for something else, possibly in breach of the DPA. Where that information has been taken out of context and combined with other pieces of personal data, it may result in the construction of a profile that is unwanted or unauthorised, or that the individual may believe to be inaccurate or misleading. In many cases, an individual will only discover that their personal information has been shared when it used by an organisation to make some decision about them, such as whether they are eligible for a state benefit or qualify for a credit card or bank loan. As the demand for information in both the public and private sectors grows, it is becoming increasingly difficult for individuals to understand what happens to their personal information, or what they should do when that information is misused.

Previous governments have tried to respond to these various developments and challenges, but unfortunately many of their efforts have met with limited success. The introduction of the DPA was, for example, hailed at the time as a major development in the protection of information privacy in the UK. Enacted in response to the European Data Protection Directive 95/46/EC, the DPA established a new legal framework for the protection of personal data. In addition to laying down a clear set of principles for the collection, processing and use of personal data by both public and private sectors, the Act also establishes a regulatory structure designed to ensure compliance with these principles and prevent practices that might threaten individual privacy. However, the Act is also severely limited in a number of key respects. First and foremost, it does not directly address many of the problems associated with the widespread sharing of personal data within government, between the public and private sectors, or between private organisations.

Similarly, RIPA was introduced to meet the UK's obligations to place state surveillance systems under an Article 8-compliant regime. However – as will be described later – there are serious flaws with RIPA itself, including its unclear system of authorisation, deficiencies in judicial oversight, and inappropriate use of powers – for example, by local authorities. Certain aspects of surveillance, most notably in relation to CCTV, stand outside the regulatory regime. In addition, many of the rules and regulations contained in the DPA and RIPA, as well as the Freedom of Information Act (FOIA) 2000, and its counterpart in Scotland, are interpreted, administered and overseen by a range of separate regulators and independent tribunals, and courts.[9] Although the introduction of the HRA has seen the establishment of a general right to privacy – by virtue of the incorporation of Article 8 of the ECHR into domestic law – the courts have been relatively cautious in their application and development of the right. As a consequence, there is no common approach to the protection of personal information in the UK, or a clear legal consensus on the limits of individual privacy.

It is against this weak, fractured and piecemeal approach to regulation that concerns about information privacy and state surveillance have begun to emerge in recent years. While the UK has one of the most extensive systems of public-area surveillance in the world – with estimates of the number of CCTV cameras running into the millions – as well as a large array of massive state databases, it would be wrong to assume that the public are unconcerned about privacy and data protection. As has already been noted, recent revelations about the loss of personal data by many departments and agencies of the state, and the use of RIPA powers by local authorities, have served to focus media and public attention on the question of privacy, and have led to a fundamental review of the way in which government and the private sector collect and use personal information (Cabinet Office, 2008).

In addition, the ambivalent reaction to the now-abandoned national identity card scheme has also served to bring into sharper relief the importance of privacy in the context of the relationship between the citizen and the state. Although in the past the question of how much the state should be allowed to know about us may not have been especially high on the political agenda, there are now calls for a reconsideration of the current approach to data collection and sharing within government, and the limits of e-government more generally. Equally, in recent years both the public and the courts have begun to question whether Article 8 goes far enough, and whether a more general right to privacy that applies beyond the public sector is needed. In short, the landscape of privacy is changing rapidly, both as new challenges to the current privacy regime emerge and public concern over the future of privacy continues to grow.

2.3 Opportunities for reform

There are a number of reasons why the area of privacy is currently in need of reform. First, developments in information technology, as well as changes in the way in which the public and private sectors now collect and use personal data, have produced a range of challenges that did not exist when the current system of privacy protections was established close to a decade ago. In addition, the sheer amount of personal information being collected, processed, and shared in the UK now presents a serious challenge to both the existing legislative regime and the regulators charged with administering it (Goold, 2009). Although recent changes to the funding and powers of the Information Commissioner's Office (ICO) have, for example, helped to ameliorate this problem, it remains the case that many of those responsible for protecting privacy and enforcing the law still lack the necessary resources or statutory authority to do so effectively. Finally, while it may have been the case that there was no need for an overarching rationale behind the protection of privacy in the past, as the distinction between state and private surveillance continues to be blurred by the increase of data collection and sharing across and between sectors, there is a danger that the system of regulation has become so disparate and convoluted that it is beyond the ability of ordinary members of the public to understand or to resort to it in protection of their rights.

Although it may be tempting to view the current system of privacy protections as a barrier to reform, this report takes a different view. While it may be true that the existing system of regulation lacks a coherent, guiding rationale and is in need of more resources, many of its constituent parts are functioning reasonably well and enjoy broad support. For example, the enactment of the DPA – and with it the establishment of the ICO – is widely regarded as a having been a fundamental step forward in UK privacy protection, and both the Act and the ICO continue to enjoy significant public and political support. Similarly, few would argue that the

incorporation of Article 8 of the ECHR into domestic law has not been a positive step, and in many respects the contribution to UK privacy law stands as one of the major achievements of the HRA.

Where there is, however, room for change, is in the overarching rationale and framework of regulation. As the technologies of data collection and surveillance continue to converge and become more ubiquitous, a system of legislation based on the idea that different sectors of government and society require different forms of privacy regulation is beginning to look increasingly outdated and impractical. This raises the question whether we need to build on existing legal, technological, and institutional frameworks for the protection of privacy, or whether more fundamental reform is needed, and is one of the key questions addressed in this report. How do we move forward in such a way as to preserve what is working well in the current system, while also ensuring that privacy protections are developed that are capable of dealing with a rapidly changing social and technological landscape?

2.4 Summary

This Chapter has provided a brief overview of the changing landscape of privacy in the UK, with a view to identifying some of the key challenges and opportunities for reform. Successive UK governments have sought to provide protection for privacy through a range of statutes and a complex system of regulation, but what has emerged is a weak, fractured and piecemeal approach to privacy that is ill-equipped to deal with the challenges that lie ahead. There is a clear need for reform and a need to develop a more flexible, comprehensive approach to the protection of privacy. This must be based on a firm commitment to Article 8 of the ECHR, and combine principles-based legislation and regulation with non-legal protections.

3. Why privacy matters

3.1 Introduction

How does one place a value on privacy? What should the law of privacy aim to protect? How do we reconcile a strong commitment to privacy as a fundamental right with the demands of national security, law enforcement, and the state's demands for personal information? Does the current approach to the protection of privacy in the UK leave certain groups vulnerable to excessive state surveillance and exacerbate existing patterns of discrimination? Is it correct to talk about the need for a balance between privacy and the public interest, or does this suggest a false opposition between these two values?

These are all questions that lie at the heart of any discussion about the development of privacy law and the regulation of state surveillance and data collection. In order to answer them, it is not only important to have a clear understanding of what is possible in terms of existing legal frameworks and regulatory mechanisms, but also an appreciation of the justifications for privacy. Unless we can agree on why privacy matters, we cannot hope to develop a coherent or consistent framework for its protection. In this section, we briefly review some of the major theories of privacy, and consider the relationship between privacy and the state's need for personal information. Different justifications of privacy are likely to point to different conclusions about the type and extent of regulation needed – questions that are explored in later chapters.

3.2 Making a case for privacy

There are several dimensions of privacy, including privacy of one's personal information, one's body, personal space, and one's communications. The focus of this project is on **information privacy**, but it also touches on certain aspects of the privacy of communications where records of communication are retained.

One of the major difficulties associated with attempts to protect privacy is the problem of definition.[10] Privacy is said to be 'a concept in disarray' (Solove, 2008, p.1), and it is difficult to find a single, accepted definition of the term. As a result, it is most useful to see 'privacy' as an umbrella term that covers a range of situations in which many different types of interests are affected (Solove, 2008, ch.2). This perspective recognises, for example, that some forms of personal information only become 'private' due to the circumstances in which they are collected or communicated (Nissenbaum, 2010). Equally, it acknowledges that the way we view privacy is intimately bound up with our understanding the public/private divide, and that this boundary is constantly shifting as a result of the ever-changing relationship between the individual and the state. Finally, this broad approach to privacy helps to ensure

that we do not simply regard privacy as a function of person or place, but rather as a product of the two, and that we do not fall into the trap of thinking that privacy is just about confidentiality or good data management practices.

Just as there is no agreed definition of privacy, there are also many different but overlapping ways in which privacy can be understood and justified. Privacy can, for example, be seen as a good in itself – as essential to our development as individuals, and bound up with ideas of dignity, liberty, and 'personhood'. In addition to promoting these values, privacy can also be justified on more instrumental grounds. Without a degree of privacy, it can become very difficult for individuals to maintain a distinction between their personal and public lives, or to exercise other important social and political rights, such as rights to freedom of religion, freedom of association, and freedom of expression.

Although it is beyond the scope of this report to consider these and other justifications for privacy in any great depth, it is important to be aware of the different ways of understanding privacy if we are to develop a programme of reform based on a set of clear and coherent principles. For the purpose of this report, we have identified six main theories for privacy, which can be summarised as follows:

Privacy as 'the right to be let alone'

Central to this notion of privacy is the ability of individuals to keep society and the state at bay, and to obtain a remedy where there has been an unwanted intrusion. The notion of privacy as 'the right to be let alone' was first advanced by Warren and Brandeis (1890), and has been referred to extensively in discussions of the Fourth Amendment in the United States and with reference to Section 8 of the Canadian Charter of Rights and Freedoms.[11] Many of the privacy protections developed in the UK as well as in the United States and Canada are based on this notion of privacy, and it has deep roots in the civil liberties traditions of these countries. This idea corresponds to many conventional understandings of privacy, such as 'a man's home is his castle', and reflects a desire on the part of individuals to avoid the prying eyes of others. This approach to privacy also plays a prominent part in many liberal accounts of the state, which stress the need for clear limits on the power of the state and the importance of privacy to the exercise of individual freedom.

Privacy as an aspect of personhood

According to this justification, all individuals need a degree of privacy in order to protect their dignity, develop as persons, and maintain a sense of self while retaining the ability to form meaningful relationships with others (Bloustein, 1964; Rachels, 1975; Schoeman, 1992; Rössler, 2005). Closely linked to ideas of autonomy and

liberty, this justification has frequently been relied on by the ECtHR in its discussions of the ambit of Article 8 of the ECHR (Feldman, 1994, 2002).

Privacy as control over information

Most commonly associated with the privacy theorist Westin (1967), and also in the German conception of 'informational self-determination', this account of privacy argues that individuals have the right to control their own personal information, and should be able to determine how and when information about them is communicated to others. Often associated with the idea of 'fair information practices', this idea has been very influential in the development of data protection laws across the world, and has been at the heart of discussions about the appropriate balance to be struck between the individual's control over personal information and the state's interests in processing data. It is important to note that while this justification of privacy presumes that some level of control over personal information is possible, it also acknowledges that the degree of control an individual is likely to be able to exercise will depend on their circumstances, as well as on the type of information in question.

Privacy as limited access to the self

Broader than the idea of privacy as the right to be let alone, this justification of privacy is based on the idea that individuals should be able to control who has access to both their person and to information about them (Gavison, 1980). Often linked to arguments about informational self-determination, this justification suggests that privacy should be understood as a form of proprietary interest which gives individuals the right to determine who they interact with and on what terms (Gross, 1967).

Privacy as secrecy

Similar to the idea of privacy as limited access, this narrower justification maintains that privacy is best understood as the individual's right to conceal facts about herself (Posner, 1978). It is a justification that has enjoyed considerable support from economic theorists of law, and that focuses on the idea that the value of information is often dependent on our ability to keep it secret and prevent unwanted disclosure. This justification is often criticised, however, on the grounds that the only people who need secrecy are those who have something to hide. This argument ignores the fact that there are many reasons why a person may want to keep something private, and that a desire for secrecy is not always evidence of bad behaviour. Individuals may, for example, keep personal information secret not out of any sense of shame, but because they fear that the information may be misunderstood when taken out of context. Equally, we keep some types of intimate information secret because we recognise that the act of sharing it can be an important step in the formation of close personal relationships.

Privacy as a social and political value

In addition to recognising privacy as an **individual** right with intrinsic value, this view of privacy is based on the claim that privacy is fundamentally important to the maintenance of a liberal, democratic **society**. According to this approach, privacy is valuable for two related reasons. First, it enables individuals to establish and maintain a variety of complex social relationships, and thereby contributes to the development of a rich and diverse society. Second, it is important because it is necessary to protect key political rights – such as freedom of association, freedom of expression, and freedom of religion – from the chilling effects of excessive state surveillance: a private 'space' is necessary for the development of dissenting views that enrich political life. It is therefore in the public interest for a democratic society to protect privacy, in addition to whatever value privacy may have for the individual (Regan, 1995; Bennett and Raab, 2006; Solove, 2008; Goold, 2009; Nissenbaum, 2010).

Given the extent to which these justifications overlap with one another, it is not necessary to choose between them. Instead, we should adopt a comprehensive approach to the question of privacy that both recognises that there are many legitimate justifications for privacy, while also acknowledging that the strength of any given justification will, to a large extent, depend on circumstances and context. Different ideas of privacy come into play, for example, when people are engaged in commercial activities as opposed to simply seeking the solitude they need to maintain a sense of dignity and self esteem. Equally, members of lawful political organisations may have very different reasons for wanting to keep their meetings private when compared with someone undergoing regular treatment for a serious illness. Privacy depends on context, and as such can be justified on many different grounds.

Having said this, however, it is still fundamentally important to be clear about what it is that any privacy law or regulatory regime is trying to achieve. Given that privacy is so notoriously difficult to define, there is always a temptation to avoid being clear about the exact purpose of protection, and to focus instead on addressing particular threats or developing responses to immediate challenges. There are significant disadvantages to this approach, as emphasised by a leading expert on privacy law and theory (Solove, 2008, p.2):

> Judges, politicians, … and scholars have often failed to adequately conceptualize the problems that privacy law is asked to redress. Privacy problems are often not well articulated, and as a result, we frequently lack a compelling account of what is at stake when privacy is threatened and what precisely the law must do to solve these problems.

In attempting to develop new forms of privacy protection – or to reform existing ones – it is important to clarify which of the above justifications is being relied upon and in what context. Although these ideas of privacy are not mutually exclusive, they are clearly focused on different values and concerns. As a result, the choice of justification will have a significant effect on how one defines the limits of and legitimate exceptions to privacy, identifies potential threats to privacy, and chooses between different legal and regulatory protections for privacy. This can be demonstrated by focusing on the question of whether the law should be based on a default expectation of privacy or a default assumption of information disclosure. If one is committed to the idea that privacy is, for example, essential to the exercise of personal autonomy and the development of the self, then one is more likely to take a 'rights-based' approach and conclude that the law should require a *prima facie* justification for all privacy infringements – especially, for example, where visual surveillance is involved. In contrast, if one believes that privacy is bound up with the ability to control information, then – in circumstances where personal data is collected – one is more likely to invoke fair information practices and laws that seek to reconcile privacy interests with the information demands of the public and private sectors. In practice, these approaches are normally combined, and the means/ends distinction between rights and information control is not clear.

3.3 Privacy and the state

As indicated earlier, the main focus of this report is the state, which is taken to refer to central and local government, law-enforcement authorities, and other organisations outside the 'public sector' undertaking public functions or that have access to personal data collected on behalf of the state. In addition to the problem of defining privacy, there is also the question of how privacy rights should be understood in the context of the state's legitimate need for information. Many recent studies and investigations – for example, by the Surveillance Studies Network (2006) – have shown how surveillance is increasingly becoming a feature of everyday life in areas that were previously considered 'private'. As surveillance cameras and tracking devices become cheaper and more ubiquitous, it is increasingly difficult for people to find places that can truly be considered private. Instead, the promise of privacy in public spaces such as streets and parks is increasingly unrealistic, with the result that the boundaries of individual privacy are increasingly being tested and eroded.

In addition, these studies have also revealed the extent to which personal information collected by the state is being shared across government agencies or with the private sector, often without the knowledge of the individuals concerned. Aside from the fact that this sharing increases the likelihood that information will be taken out of context or used for purposes other than those for which it was originally collected, it also makes it difficult for individuals to keep track of their personal information. If they are

unable to determine easily what the state or private sector knows about them, then it becomes extremely difficult to challenge decisions made on the basis of that information, to check its accuracy, or to hold anyone accountable for errors or misuse.

To some extent, the DPA helps to ensure that the state does not systematically misuse personal information or engage in activities that might seriously undermine individual privacy. For example, by laying down the requirement of 'fair processing' and giving individuals the ability to access their data, the Act helps to make the use of information by the state more transparent. In addition, the Act also sets out the conditions for the legitimate collection and sharing of personal data without consent – for example, in the exercise of statutory powers – and prohibits the use of personal data for incompatible purposes. However, these important rules and restrictions are often difficult to enforce, and remedies can be hard to come by. Although public awareness of the right to see one's own personal data reportedly increased from 75 per cent in 2004 to over 90 per cent in 2009, many individuals remain unaware of the range of protections provided by the DPA (ICO, 2010b, p.19). Furthermore, even where they are aware, they may be discouraged from exercising their rights by the apparent lack of significant sanctions.

Similarly, RIPA was created to ensure that the system for regulation of the use of intrusive surveillance powers was in accordance with Article 8, and establishes a process of authorisation for the use of intrusive surveillance powers. However, the Act is complex and difficult to use, and runs to some 30 further statutory instruments. There are concerns about the adequacy of the system of self- authorisation, and in many areas – including the regulation of CCTV – the Act's coverage is not comprehensive. Placing limits on surveillance does not guarantee that personal data is being collected or used appropriately, in part because those limitations are constantly being tested by the state and other public organisations.[12]

By placing greater emphasis on the importance of privacy, the law can help to resolve any conflicts that arise between the public or private sector demand for information and individuals' ability to control and monitor how information about them is used. In determining the limits of individual privacy, however, we must be clear about why and under what circumstances government agencies should be allowed to collect, process, and share personal information. Rules, regulations, and human rights not only place limits on the information gathering and surveillance powers of the state, but also help to define the boundary between the public and private spheres and establish the importance of information privacy in a democratic society.

Based on the theories of privacy outlined above, there are a number of ways to approach this task. Perhaps the most obvious starting point is to note that, while privacy should be protected as a fundamental right, its infringement must always be in accordance with the law, necessary, proportionate and justified. Privacy can, however, also be regarded as one of several competing legal interests or rights. If we take the former approach and privilege privacy, then attempts to restrict individual privacy in the interests of national security, the enforcement of law, or improvement in the efficiency of public service delivery are more likely to be seen as inherently problematic, and subject to rigorous tests of necessity and proportionality. This is because the promotion of such goals frequently involves restricting the general ambit of the right, and threatens to undermine privacy's legal status, as well as its symbolic or practical significance. If, however, privacy is regarded as a legal interest like any other – or, in weaker terms, as an individual preference – then it becomes more amenable to balancing exercises in an effort to reconcile the aims of the individual with those of the state. Put another way, a key question is whether potential threats to privacy should be assessed according to human rights criteria such as necessity and proportionality, or instead according to principles such as reasonableness and balancing.[13]

Another way to approach the question of how to reconcile privacy and state interests is to ask whether a contextual approach to privacy should be adopted. According to this approach, while it may be appropriate to provide strong privacy protection in some contexts (such as the home), it may not be appropriate to extend similar protection in others (such as airports or government buildings). Here, the key is to recognise that the importance of privacy varies according to circumstances, and that it may be necessary to develop distinct legal protections and regulatory frameworks tailored to different contexts and state functions. Taking this approach may resolve much of the apparent tension between privacy and the public interest, if only because it forces one to acknowledge that the importance of both – and the legitimacy of overriding the right of privacy – varies according to the particular situation in which they come into conflict.

There are also other issues that must be taken into account when considering the relationship between individual privacy and the role of the state. Looking back at the justifications canvassed above, and considering that privacy is necessary for the exercise of other key human rights – such as the rights to freedom of expression, freedom of association, and freedom of religion – any discussion of future privacy regulation must assess the protection currently afforded to these related rights. Even if it is concluded that there is no inevitable conflict between privacy and, say, national security, there may be an argument for strengthening protection of the privacy right – as we show in later chapters – on the grounds that it is essential to ensure freedom

of speech even in times of heightened insecurity or political unrest. This argument is closely related to the conception of privacy as a social and political value. Finally, it is important to stress that any attempt to reform the law of privacy in the UK must begin with the right to respect for private and family life contained in Article 8 of the ECHR. The HRA not only incorporates this right into domestic law, but it also places an obligation on the government to ensure that the information gathering and surveillance activities of the state are consistent with Article 8, and that any infringement of the right is in accordance with the law, properly justified, necessary, and proportionate. Regardless of which theory of privacy we rely upon or how we characterise the tension between the citizen and the state, it is important to remember that the onus is always on the state to explain and justify why it should be allowed to limit or infringe an individual's privacy.

3.4 The future of privacy

It is difficult to foresee what the future might bring, and therefore what kind of legal and other regulatory powers might be necessary to protect privacy and keep state surveillance and information gathering in check. Some might argue that it is inevitable that the modern state's growing demand for information – coupled with the development of increasingly sophisticated surveillance technologies such as body scanning, facial recognition software, and automated data-mining tools – will eventually result in a society in which privacy is a thing of the past. According to this fatalistic view, any new laws aimed at enhancing existing privacy protections are likely to fail, and as a consequence we should simply accept that 'privacy is dead.'

In contrast, a more optimistic view of the expansion in surveillance and the government's demand for personal information focuses instead on the positive role that technology can play in the development of public policy and business planning. The previous Government's 'transformational' agenda was in part based on this view. It emphasised that improvement in the collection, processing, and sharing of information within government did not necessarily have to come at the cost of individual privacy if the proper safeguards are firmly in place. Although the promotion of e-government is still in its relatively early stages, the state has not yet convincingly shown that it can fulfil its public service aims while also protecting the right of privacy. A succession of significant data losses in recent years has led many to question government's ability to manage large amounts of confidential information securely, and to press for the enactment and enforcement of new laws to ensure that privacy is properly protected.

Looking back over the last 40 years, however, there are also other reasons to be optimistic about the future of privacy. Although privacy has come under considerable pressure from government in recent years, at the same time there has been a

gradual strengthening and harmonisation of information privacy and data protection laws across Europe and beyond, and a growing level of public awareness about the importance of privacy. In the UK, prominent regulators and NGOs, as well as some political parties, have also repeatedly warned about the dangers of 'sleepwalking into a surveillance society' (Ford, 2004), and have helped ensure that privacy remains on the political agenda. Finally, in the last decade we have also seen the gradual emergence of a jurisprudence of privacy in national and international courts, and an increased willingness on the part of judges to favour the protection of privacy over vague appeals to national security and the needs of law enforcement. Looked at from this perspective, there is reason to believe that the 'doomsday' scenario can be avoided if an effective legislative and regulatory framework can be established.

In trying to decide how to reconcile a commitment to privacy with the state's growing demand for information, it is important to steer a path between these various optimistic and pessimistic accounts. Just as fatalists tend to have an overly deterministic view of technology and fail to acknowledge that the law and other means of regulation can do much to protect individual privacy, many optimists struggle to explain exactly how a 'balance' can be struck between privacy and the practical realities of the modern state. They also assume that progress is ratcheted and cannot be reversed, gloss over existing inadequacies of legal and other controls, and take for granted an ongoing political commitment to human rights and the protection of privacy.

For our part, the authors of this report believe that, in order to produce a regulatory framework capable of meeting the privacy challenges of the twenty-first century, it is important to be clear about what it is we are trying to protect, and why it is important, and to ensure that any new laws or regulatory mechanisms are able to be implemented in practice. In addition, it is also important to ensure that any future reforms are built on a solid and principled human rights foundation, and that existing laws and regulatory structures are properly evaluated before any attempt is made to amend or repeal them. These points will be considered throughout this report. Regardless of whether one is optimistic or pessimistic about the future of privacy, it is clear that the scale of the challenge ahead requires law-makers to move carefully, and to avoid the fractured and piecemeal approach that has marred past attempts at reform. Although this report does not address it, the question of how privacy can be protected in single countries alone, without the international or global collaboration of other forces aimed at the same goal, should also be on the agenda.

3.5 Summary

In this Chapter, we have set out the main arguments in defence of information privacy, and considered how the growing demands of the state – in particular, in relation to national security, law enforcement, and citizens' access to public services – are likely to create new challenges to existing privacy laws and data protection regimes. Several prominent and overlapping theories of privacy have influenced existing approaches to regulation. It is necessary to take a context-specific approach to issues of information privacy and to ensure that the approaches used enhance, rather than undermine, the existing framework of rights and data protection in the UK.

4. Information privacy in the UK

4.1 Introduction

As is the case in many common law countries, information privacy in the UK is governed by a wide variety of legal rules and regulations.[14] As information technologies and the demands of government have developed over time, however, the law has struggled to strike a balance between protecting the privacy of individuals and ensuring that the state and private organisations are able to acquire and process personal information for legitimate purposes. In particular, there has been a distinct tension between calls from the police and the security services – as well as organisations responsible for health, education, social welfare, and transport – for greater powers of surveillance and data collection, and an emerging public awareness of the value of information privacy.

This section of the report provides a general overview of the major laws and legal regulations that govern information privacy in the UK, as well as various informal rules and guidelines that restrict the ability of public and private organisations to collect and handle personal information.[15] In an effort to ensure that this summary is concise and accessible, specific sections of Acts and judicial decisions are cited sparingly. It is also important to stress that this Chapter is not intended to provide a comprehensive account or analysis of the relevant law. This has already been done by a number of recent parliamentary and independent reviews, many of which are cited in this report. Instead, the purpose of this Chapter is to identify areas in which the protection of information privacy is either weak or in need of substantial reform.

4.2 Overview of the current law

At present, there is no single privacy statute or comprehensive 'privacy law' in the UK. Instead, information privacy is protected through a combination of statutory provisions, legal regulations, common law rules, and systems of informal regulation (sometimes referred to as 'soft law'). This section of the report concentrates on the following main sources of information privacy protection in the UK:

- The Human Rights Act (HRA) 1998
- The Data Protection Act (DPA) 1998
- The Freedom of Information Act (FOIA) 2000
- The Regulation of Investigatory Powers Act (RIPA) 2000[16]
- Common law protections and breach of confidence, and
- Informal regulation, codes of practice, and other forms of 'soft law'.[17]

For the sake of simplicity, these different sources of law are examined in this Chapter under two broad headings: statutory protections and common law protections.

Because it is difficult to understand the operation of guidelines, codes of practice, and 'soft law' without also considering the role of regulators and alternative approaches to the promotion of information privacy, these protections are discussed in detail in Chapter 5.

4.3 Statutory protections

The Human Rights Act 1998

Prior to the enactment of the HRA, there was no established statutory or common law right to privacy in the UK.[18] Although individuals could appeal to the European Court of Human Rights (ECtHR) if they believed that their right to respect for private and family life under Article 8 of the ECHR had been infringed, the right could not be directly relied upon in UK domestic courts. With the introduction of the HRA, however, the ECHR became a part of domestic law, and a general right to respect for private and family life under Article 8 was established in the UK:

(1) Everyone has the right to respect for his private and family life, his home and his correspondence.
(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

It is important to note that the ECtHR has acknowledged that the right to respect for private and family life is 'a broad right not susceptible to exhaustive definition'.[19] Article 8 has been held to include elements such as the right to identity and personal development, gender identification, sexual orientation, the right to develop and establish relationships and be free from environmental pollution, as well as the more traditional privacy rights such as the holding and dissemination of personal information.

As a consequence of the incorporation of Article 8 into UK law, it is unlawful for a public body to interfere with an individual's privacy unless that interference is authorised by one of the specific exceptions contained in Article 8(2). In practice, this means that in addition to any other rules laid down by UK legislation or case law, any public body that interferes with an individual's privacy must be able to demonstrate that the interference with the obligation to respect private and family life is:

(1) Authorised by a law enacted by a democratic process
(2) Proportionate to the purpose in question
(3) Necessary for the functioning of a democratic society, and

(4) Conducted in accordance with one of the legitimate aims set out in Article 8(2) of the ECHR.

Since the HRA came into force on 2 October 2000, both the UK and European courts have shown an unprecedented interest in questions of privacy. While cases such as *Campbell v Mirror Group Newspapers* [2004] and *Douglas v Hello! Ltd* [2005] have helped to clarify the scope of the right as it applies to individuals and private organisations, decisions such as those handed down in *Peck v UK* (2003), *Liberty v UK* (2008), and *S. & Marper v UK* (2008) have also recognised the restrictions the ECHR and Article 8 places on the state.

In many respects, *S. & Marper v UK* (2008) provides a good example of the sorts of obligations that Article 8 imposes on the state. In that case, both the applicants had been required by the police to provide a DNA sample and have their fingerprints taken: S at the age of 11 on arrest for an offence of which he was subsequently acquitted; and Mr Marper on arrest in 2001 for an offence which was subsequently dropped by the prosecution. The police later refused to destroy their DNA samples and fingerprints. On appeal from the House of Lords, the ECtHR found a violation of Article 8 as regards the retention of both the DNA sample and its profile and fingerprints. According to the Court, the highly personal nature of a cellular sample makes it data that needs to be protected. When considering the retention regimes in other states, it noted that England and Wales and Northern Ireland are the only jurisdictions within the Council of Europe to allow indefinite retention of fingerprint and DNA material of any person of any age suspected of any recordable offence. The Court made it clear that any state that takes a leading role in developing scientific technologies to fight crime had a special responsibility for striking the right balance between the competing public and private interests.

It is also important to note that the limits of the rights contained in Article 8 are continually being questioned and tested by the courts. Depending on the circumstances, for example, Article 8 can also cover activities carried out in public. Recently, the ECtHR has held that in some circumstances photographs of an individual in a public place, taken without consent or knowledge, can amount to an interference with private life, as there is 'a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life'.[20]

Although the ECHR is primarily concerned with limiting the power of the state to interfere with individual rights – as in *S. & Marper* – it is also concerned with positive obligations. Under the Convention, states are required to take positive steps or measures to protect the Convention rights of individuals, particularly against interference by others. In this regard, the Convention recognises that the acts of

private individuals or bodies can threaten human rights just as much as the acts of state authorities. It is important to note that many of the cases on 'positive obligation' have involved Article 8 rights, and have considered the question whether the state has put in place a legal framework that effectively protects Convention rights. In light of this, it can be argued that the HRA requires the government to do more than simply respect an individual's privacy. In addition, it has a duty to protect privacy and provide effective regulatory safeguards.

In a similar vein, the requirement that any interference with Article 8 must be 'in accordance with the law' goes beyond the bare requirement that there must be a statutory or common law provision in place. Instead, it is essential that the law in question is compatible with the rule of law, sufficiently circumscribed, and subject to adequate legal safeguards. For example, it is well established that interference will not be in accordance with the law if the impugned power is an arbitrary one.[21]

Finally, an essential ingredient of the Convention – and the operation of Article 8 – is the right to an effective remedy under Article 13. Although the right is not specifically included in the HRA, it can be argued that right should be available, as many of the Tribunals responsible for regulating state surveillance activities are inaccessible to the majority of complainants and bound by highly restrictive procedural rules.

Yet although the HRA and the Convention provide a rights-based framework for the protection of information privacy in the UK, in practice the operation of Article 8 is limited in a number of key ways. While the courts have made it clear in recent years that the obligation to respect private and family life can apply to individuals and organisations as well as the state,[22] unfortunately this development is most likely to benefit those who can afford to go to court to protect their privacy. As noted by the privacy expert Dr Chris Pounder:

> I am not confident that Article 8 will provide satisfactory jurisprudence because there are very few cases going to the courts. Those cases that tend to go into the courts primarily involve... people who have celebrity status... Anybody who is trying to take an Article 8 case on has to take on the unlimited resources of the state. (House of Lords 2009, para. 131)

As important as it is to ensure that individuals have an actionable right to privacy, it is equally important to ensure that problems with access to justice do not exacerbate the divide between privacy haves and privacy have-nots. If for no other reason, this is a compelling reason for supplementing the protections provided by the HRA with other rules and regulations aimed at preserving information privacy.

Another major limitation to the right to respect for private and family life comes from the broad range of exceptions listed in Article 8 itself. Although few would suggest that privacy should be an absolute right – that is, a right which cannot be restricted in any way, such as the prohibition on torture (Article 3) – the list of exceptions to Article 8 is extensive when compared with those typically attached to privacy rights in other jurisdictions. In particular, the phrase 'in the interests of national security, public safety or the economic wellbeing of the country' is so broad as to allow a government that is hostile to the privacy interests of individuals to curtail them severely. In practice, governments are free to interpret these limitations very broadly, and are rarely required to point to empirical evidence to support a call to restrict or infringe information privacy.[23] As a consequence, there is a danger that an over-reliance on the HRA and Article 8 could leave information privacy particularly open to attack from an unsympathetic government or public agency.

Finally, there is also the question whether it is reasonable or realistic to expect government agencies and other public bodies properly to understand and adhere to principles of necessity and proportionality when dealing with the rights set out in Article 8. Although the ECHR is clear that any infringement of Article 8 must be both necessary and proportionate to the legitimate interest being pursued, courts in the UK and Europe have often struggled to provide clear guidance on the meaning and scope of these terms.[24] Clearly, bodies like the ECtHR play an important role in helping to educate those within government and the public sector as to what constitutes an unlawful infringement of the right to privacy. Yet despite the efforts of the Commission and organisations like Liberty and JUSTICE, the complexity of Article 8(2) and uncertainty as to its application remains a major problem for the protection of information privacy in the UK.

The Data Protection Act 1998

In addition to protections provided by the HRA, information privacy and the use of personal data in the UK is also regulated by the DPA, which replaced a 1984 Act of the same name. The DPA itself was enacted as the UK's transposition of the 1995 European Union Data Protection Directive 95/46/EC (European Union, 1995), a landmark effort of the EU to bring Member States' data protection laws into greater harmony in terms of the practical implementation of rules based upon common principles. Besides protecting personal data, the Directive also aimed to assist the completion of the internal market in the EU through facilitating the 'free movement of personal data' within the EU, and by establishing criteria for the transfer of personal data to non-EU countries.

As the name suggests, the DPA is primarily concerned with the 'processing' of personal data, where processing includes any use, disclosure, retention, storage,

holding or collection of such data. However, not all forms of personal information are personal data, and many manual (paper) files held in the private sector are not subject to the Act. In relation to the public sector, all personal information is personal data, but the protection afforded by the Act to personal information in manual files is usually limited to the right of access to personal data and the correction of inaccuracies.

The DPA sets out the circumstances under which such data can be processed by both public authorities and private organisations. According to Schedule 1 of the DPA, any individual or organisation engaged in the handling of personal data is required to ensure that all such data are:

(1) Fairly and lawfully processed
(2) Processed for limited purposes
(3) Adequate, relevant and not excessive
(4) Accurate and up to date
(5) Not kept for longer than is necessary
(6) Processed in line with rights of data subjects under the Act
(7) Secure, and
(8) Not transferred to other countries without adequate protection.

In practice, the first of these data protection principles – the requirement that the processing of personal data be fair and lawful – aims to ensure that individuals and organisations have legitimate reasons for collecting personal data, that they are open with data subjects about how that information will be used, and that they do not do anything unlawful with the data. In order to ensure that the storage and processing of personal data are consistent with this principle and both open and transparent, the Act establishes a system of notifications. Under this system, all organisations engaged in the handling of personal information are not only required to provide individuals with appropriate privacy notices when collecting their personal data, but also to notify the ICO of their activity (unless they are exempt under the Act), and to provide details of the type of data processing being undertaken (DPA ,1998, Part III). This information is then published in the register of data controllers and is available for public inspection. Failure to notify is a criminal offence under the Act. The general purpose of this system is to ensure that members of the public are able to find out who is processing personal information and for what purpose. In particular, the system is designed to ensure that the ICO is informed when a data controller processes personal data, and that the individuals concerned are made aware of the processing and the purposes for which it is being undertaken.

Because the DPA is fundamentally concerned with ensuring that organisations do not process personal information improperly, the regime established by the Act not only provides individuals with information rights that can be enforced by the courts, but also enables anyone who believes that his or her personal information is being improperly held or used to make a complaint to the ICO.[25] According to the Act, the Information Commissioner has the power to:

(1) Undertake assessments to ensure that public sector data controllers are complying with the Act
(2) Serve information notices requiring data controllers to provide the ICO with specified information within a certain time period
(3) Serve enforcement notices where there has been a breach of the Act, requiring data controllers to take (or refrain from taking) specified steps in order to ensure they comply with the law[26]
(4) Prosecute those who commit criminal offences under the Act[27]
(5) Conduct inspections to assess whether data controllers' processing of personal data complies with the law (with their consent, except in the case of central government departments and some public authorities, where consent is not needed), and
(6) Report to Parliament annually or on data protection issues of particular concern as they arise.

According to the Information Commissioner's Annual Report for 2009–10, most complaints brought under the DPA (52 per cent) are resolved informally. In the 17 per cent of cases in which a decision notice was served, however, those notices were only upheld by the Information Tribunal 23 per cent of the time, with the remaining notices either being partially upheld (31 per cent) or not upheld (46 per cent). This suggests that while the existing system of enforcement is working reasonably well on an informal level, the Tribunal has not been especially willing to force individuals and organisations to change their data processing practices.

Although it is clear that the DPA provides considerable protections for information privacy, it nonetheless has serious limitations. In part, the problem is one of definition. It can be argued, for example, that the definition of 'sensitive data' in the DPA needs to be re-considered, particularly in relation to the increased use of biometric data – fingerprints, retina and iris patterns, voice samples *etc*. – by the state and private sector. As a result of the decision in *S. & Marper*, an actual DNA sample, as well as any profile gained from the sample, must be regarded as personal data. Unfortunately, it is unclear whether the definition of personal information contained in the Act can be stretched to provide the protection such data deserves.

There is also the question of enforcement and compliance. Although the ICO's enforcement powers were recently expanded so that it can now order organisations to pay fines of up to £500,000 for serious breaches of the DPA, in general its powers remain relatively limited when compared with regulators in some other jurisdictions.[28] For example, although the Information Commissioner now has the power to inspect government departments and certain public authorities, private sector inspections can only be carried out with the permission of the relevant data controller. As the House of Lords noted in 2009, the need for permission limits the ability of the ICO to protect information privacy and undermines the deterrent power of the DPA (House of Lords, 2009, para. 232). In contrast, in the Republic of Ireland the DPA grants the Irish Data Protection Commissioner much stronger inspection powers,[29] and the power to conduct routine audits of data controllers, with or without their permission.

In addition to granting relatively limited enforcement powers to the ICO, the DPA also sets out a broad range of exemptions. Under Part IV of the Act, for example, when an individual's personal data is being held and processed for the purpose of safeguarding national security, the general data protection principles do not apply, nor do the data subject rights or other obligations laid down in Parts II, III, or V. In some cases much narrower, key exemptions also exist regarding matters of crime and taxation, and in relation to issues of health, education and social work. While the Act sets out the conditions under which these exemptions can be invoked, in the case of national security in particular, the decision as to whether the personal data in question is covered by the Act rests with either a Minister of the Crown or the Secretary of State. Given that one of the reasons for regulating the collection and processing of personal data is to protect individuals from unwanted or overzealous state surveillance, it can be argued that providing elected officials with such broad powers substantially undermines both the effectiveness and the symbolic value of the regime as a whole.

Finally, it is important to note that the DPA is primarily concerned with questions of data collection and processing, and not information privacy per se. Indeed, it is significant that the word 'privacy' does not appear anywhere in the text of the DPA. As a result, even if the limitations identified in this section were addressed, it is unlikely that the Act could provide the level of protection for information privacy needed in light of the threats discussed in earlier chapters of this report. Although there has been considerable debate over what constitutes personal data for the purposes of the Act, it is clear that the term is much narrower than the idea of private information, or the meaning of privacy, as discussed earlier in this report. As a result, it is difficult to see how the DPA – even if substantially amended – could by itself provide the basis for a more comprehensive framework for the protection of information privacy in the UK.

Personal data protection in the European Union – proposals for reform

As stated above, the DPA came about to give domestic effect to the landmark EU data protection directive. However, after 15 years, the European Commission has brought forth a communication outlining steps to develop a more comprehensive and coherent legislative framework, to protect individuals' data, including a revised Directive requiring national legislative changes.[30] The Commission will propose legislation in 2011 aimed at revising the legal framework for data protection with the objective of strengthening the EU's stance in protecting the personal data of the individual in the context of all EU policies, including law enforcement and crime prevention, taking into account the specificities of these areas. Non-legislative measures, such as encouraging self-regulation and exploring the feasibility of EU privacy seals, will be pursued in parallel. This revision is intended to correct deficiencies in the original and in national transpositions in the light of experience with implementation, and of new, globalising developments in the world of information processing, and reverse the drifting apart of national approaches that had occurred over this period of time. Individuals' fundamental rights would be strengthened, especially their right to the protection of personal data. It would enhance individuals' control over their data, including rights of access, rectification and deletion, and provide greater transparency. These enhancements would be in keeping with the EU Charter of Fundamental Rights,[31] which repeats the older right to a private and family life but also adds a right to the protection of personal data. The UK government to date has been cautious in its approach to the proposed reforms. However, the discussions around new EU proposals and the implementation of any subsequent EU legislation at the national level, together with non-legislative measures, will provide an important opportunity to update and enhance individual data protection measures.

The Freedom of Information Act 2000

As has been mentioned earlier in this report, in order for individuals to be able to protect their privacy and maintain control over their personal information, they must be able to know how that information is being used. While the DPA regulates access to personal information, the major piece of legislation governing the access to information generally in England and Wales (and for some Scottish bodies) is the FOIA, which came into force in January 2005; Scotland has a separate but largely comparable Freedom of Information (Scotland) Act (FOISA) 2002. Under the Act, individuals have a right to request information held by a public authority, provided that it does not directly pertain to them (the right to personal information being provided by the DPA 1998). Requests can be made either by letter or email, and according to the Act the public authority must inform the applicant whether it in fact holds that information – and supply it if also requested – within 20 working days. Crucially, the Act is retroactive and as a result applies to all government departments

and publicly funded bodies and all information held by them. Although the FOIA is the responsibility of the Ministry of Justice, it is administered and enforced by the ICO, with decisions about its application and the implications of breach being dealt with by the Information Tribunal. Regulation under the Scottish Act is the responsibility of the Scottish Information Commissioner.

In many respects, the introduction of the FOIA marked a significant development in the protection of information privacy in the UK. By extending the rights of access already established under the DPA, the Act has helped to make government and public sector data use more open and transparent. Yet while the FOIA has a broad ambit, the obligations placed on public authorities by the Act are – in common with the DPA – subject to a wide range of exemptions. These exemptions are listed in Part II of the Act and include information that is required for safeguarding national security (section 24(1)), information that might prejudice the prevention or detection of crime (section 31(1)(a)), and information that may endanger the physical or mental health of any individual (section 38(1)(a)). Significantly, the FOIA also creates two exemptions for personal data about the applicant. The first applies if the applicant is the data subject; then the appropriate mechanism for acquiring such personal data is via the subject access right of the DPA. If the applicant is not the data subject, then the public authority has to assess whether publication of the personal data (via disclosure under the FOI regime) would breach a data protection Principle. If it does breach a Principle, then the personal data cannot be accessed by the requester, and the privacy of the data subject is maintained. In contrast, in Scotland the test for release of personal data under the FOISA centres on whether the public interest in disclosure outweighs the public interest in exempting the data from disclosure. A further limitation to the effectiveness of FOI has been the limited number of organisations to which it applies. Some key bodies, such as the Association of Chief Police Officers (ACPO), have not been subject to its provisions, although the Government now plans to include them.

It is important to note that both the DPA and FOI regimes have to deal with the vexed question of what constitutes ‘personal data’; clarity on this point has been more often aided by rulings under the freedom of information regimes. When viewed in combination with the DPA, the FOIA helps to increase the transparency of public bodies and makes it more difficult for them to engage in unauthorised forms of surveillance and personal data collection as information about these activities can be the subject of requests for information (for example, policies towards surveillance). For example, under the FOIA an individual could request information about future government plans routinely to monitor personal emails, and then make a request under the DPA to determine whether their own email has actually been monitored (assuming none of the various exceptions apply in either case).

The Regulation of Investigatory Powers Act 2000

Introduced as a replacement for the Interception of Communications Act 1985 and parts of the Police Act 1977, RIPA – and RIPSA, its counterpart in Scotland – governs the exercise of surveillance powers by the police and other public bodies. In essence, RIPA was enacted to ensure that the exercise of these surveillance powers does not infringe upon the right to respect for private and family life contained in the HRA, and the Act contains a wide range of provisions covering such diverse activities as the interception of communications, wiretapping, and the surveillance of private, semi-private, and public spaces. Because the rules relating to each of these areas are extensive and often highly complex, it is beyond the scope of this report to provide anything more than a basic summary of the relevant provisions, with a particular focus on the implications for information privacy in each case.

In simple terms, RIPA helps to protect information privacy in two key ways. First, it establishes a regulatory framework for the interception of communications by the police, and second, it limits the circumstances in which the police can undertake surveillance of private residences or individuals in public. As regards the interception of communications, the key provision of RIPA is section 1(1), which makes it a crime for anyone to intercept a communication that takes place over a public network without lawful authority.[32] Given that telephone calls, posted mail, email, and voicemail are all regarded as things capable of being intercepted under the Act, on its face section 1(1) provides considerable protection for information privacy, However, according to section 5(3) of the Act, the Secretary of State can issue a warrant empowering the police to intercept a communication provided the surveillance proposed is proportionate, necessary, and:

(1) In the interests of national security
(2) For the purpose of preventing or detecting serious crime
(3) For the purpose of safeguarding the economic wellbeing of the United Kingdom, or
(4) For the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement.

Although the legislative regime as regards the interception of communications is generally clear, some questions remain unresolved. Interestingly, it has been held that the unintended monitoring of a mobile phone call by the police – as a result, for example, of that mobile phone coming within range of a covert surveillance device being used for some other purpose – does not constitute an interception provided the call is not recorded.[33] Given that this data would not be personal data under section 1

of the DPA (as it is not 'recorded'), there is no obvious remedy available to an individual whose privacy has been violated in this way. Equally curious is the fact that information obtained by foreign authorities outside of the UK is admissible as evidence provided it was intercepted lawfully in that jurisdiction.[34] Why such evidence should be admitted – when equally lawful evidence obtained domestically is not – is unclear.

In terms of information privacy, it is also important to distinguish between surveillance carried out on a private communications network and that undertaken on a public network. According to section 4 of RIPA, any organisation (including public authorities) can lawfully intercept telephone calls or emails made on their own private network provided the interception is for the purpose of monitoring the conduct of their business. Given that many people communicate through private networks, this exception to the general prohibition contained in section 1 constitutes a serious gap in the protection of information privacy. Furthermore, under section 1(6) a person or organisation in control of a private communications network may have lawful authority to intercept and monitor calls and emails, provided the users of that system have given their consent, either explicitly or implicitly (for example, by accepting such monitoring as one of the terms of their employment).[35]

In addition to the general privacy restrictions imposed by Article 8 of the ECHR, RIPA also governs much of the surveillance of private, semi-private, and public spaces. Not only does the Act set out the circumstances under which certain public authorities – most notably the police – can engage in surveillance activities, it also provides a framework for the authorisation and review of those activities by the Office of the Surveillance Commissioner (OSC). According to section 48(2) of the Act, surveillance is defined as:

(a) Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications
(b) Recording anything monitored, observed or listened to in the course of surveillance, and
(c) Surveillance by or with the assistance of a surveillance device.

Under the Act, surveillance may be defined as directed or intrusive, and this definition has implications for whether a particular type of surveillance can be authorized. Although the definitions of directed and intrusive surveillance are somewhat confusing, it is possible to define them as follows:

Surveillance is **directed** if:
(1) It comprises covert observation or monitoring by whatever means

(2) It is for the purpose of a specific investigation or specific operation (any crime or other offence), and
(3) It will or is likely to obtain private information about any person, not just the subject of the operation.

Surveillance is **intrusive** if:
(1) It is covert
(2) It is carried out on any residential property or in any private vehicle, and
(3) It involves the presence of an individual on the premises or in the vehicle, or the use of a surveillance device.[36]

It is worth noting that the structure of these definitions is in many ways typical of the Act. Although RIPA is now the primary means by which police surveillance is regulated in the UK – and is therefore legislation that most police officers are required to be familiar with – in many places it is poorly drafted and its overall structure is far from clear. Although legislative clarity is something that should be strived for in all areas of the law, it can be argued that it is particularly important where fundamental rights such as the right to privacy are at stake.

Generally speaking, where an individual's residence or vehicle is placed under covert surveillance, that surveillance will be regarded as intrusive for the purposes of the Act. As a consequence, the police can only place an individual's home under surveillance once they have obtained authorisation from the OSC.[37] Difficulties arise, however, in cases where it is unclear whether a building or some other private space constitutes a residence for the purposes of the Act. Equally problematic is the situation where an individual who is being followed under a directed surveillance authorisation enters a residence. Under the provisions of RIPA, it seems clear that intrusive surveillance authorisation would be required, although this can be granted by an authorising officer under section 36(3) prior to approval being gained from the OSC if the matter is deemed to be sufficiently urgent. Such examples highlight the ambiguities created by the distinction the Act draws between directed and intrusive surveillance. Although many police forces advise their officers and authorising officers to take a conservative approach to surveillance – and to seek approval for intrusive surveillance whenever they are in doubt – the current system of authorisation still leaves open the possibility of serious errors and the inadvertent use of otherwise illegal surveillance techniques.

Where covert surveillance is being undertaken by the police or a public authority in a public place (such as a street or a park), the question of whether RIPA authorisation is required will depend on whether the surveillance in question can be categorised as either directed or intrusive. For example, according to paragraph 1.4 of the Covert

Surveillance Code of Practice, the police must obtain a surveillance authorisation if they intend to use an existing public area CCTV system as part of a pre-planned surveillance operation.[38] As a consequence, the police cannot simply take control of a CCTV camera in order to follow a particular individual or vehicle, unless that surveillance is part of the day-to-day operation of the system.

As has already been noted in this report, the growing use of public area CCTV systems constitutes one of the major threats to information privacy in the UK. Although the vast majority of CCTV schemes operating in the UK have their own codes of practice (often based on the CCTV Code issued by the ICO), as will be discussed in the next chapter these informal codes are not legally binding and do not confer any rights on individuals who have been made the subject of unwarranted public area surveillance (other than a limited right of access to the images recorded). As a consequence, although a code may prohibit operators from following an individual unless it is for a particular purpose (such as the prevention of crime), if the surveillance is not recorded then an individual who feels they have been unjustly targeted has no obvious remedy under the law.

In part, this situation arises because the law does not generally protect privacy rights in public places. Although once an individual's activities are recorded and issues of data protection come into play, the current law does not regard the mere observation of an individual in public as an infringement of their Article 8 right to privacy.[39] It can be argued, however, that even observation without recording can seriously infringe upon an individual's privacy in public, insofar as an important aspect of that privacy is the ability to act anonymously and without fear of being watched. This is a point that has been stressed by the Council of Europe, which stated in 2007 that:

> Video surveillance of public areas by public authorities or law enforcement agencies can constitute an undeniable threat to fundamental rights such as the right to privacy... and [to the individual's] right to benefit from specific protection regarding personal data collected by such surveillance... it is recommended that specific regulations should be enacted at both international and national level in order to cover the specific issue of video surveillance by public authorities of public areas as a limitation of the right to privacy. (European Commission for Democracy Through Law (Venice Commission) 2007, paras. 79 and 81)

Furthermore, the fact that individuals may be subjected to routine surveillance without their knowledge – as is the case where public area CCTV cameras are covert – may have a significant 'chilling effect' on free speech and militate against the use of public spaces for political gatherings or protest activities. Although a statutory regime to regulate CCTV was called for by the House of Lords (House of Lords, 2009, para. 219), the Committee's recommendation was not accepted by the Government at the

time.[40] The current Government has, however, indicated that it may support a statutory system of CCTV regulation, although at the time of writing no further details or timeframe had been announced.

Returning to the operation of RIPA, it is clear that although the regulatory regime it establishes is designed to ensure that the use of police surveillance is consistent with the rights set out in Article 8 of the ECHR, this regime suffers from a number of major shortcomings. First and foremost, because the legislation is extremely complex, there has been considerable confusion within the ranks of the police as to its scope and application. According to a Review of RIPA commissioned by ACPO in 2004, the legislation is marred by ambiguity, and its chief provisions are open to a variety of interpretations. This problem is compounded by the fact that RIPA also preserves (with amendments) Part 111 of the Police Act – which deals with interference with property – and the Intelligence Services Act 1984. As a result, it has led to the development of what ACPO regard as an unnecessary level of bureaucracy and a lack of clear guidance for Senior Investigating Officers.

This is a view that has been echoed by the courts. The Court of Appeal has, for example, labelled RIPA 'a particularly puzzling statute' (*R v W* [2003] EWCA Crim 1632). Similarly, Lord Bingham in the House of Lords described the Act as 'perplexing', and noted that 'the trial judge and the Court of Appeal found it difficult to 'construe the provisions of the Act with confidence, and the House has experienced the same difficulty'.[41] As mentioned earlier, it should also be noted that the Act has given rise to an unprecedented number – over 30 – statutory instruments, which now have to be consulted in order fully to understand its remit and powers.[42]

Organisations such as Liberty and JUSTICE have also repeatedly expressed concerns over the system of authorisation established under RIPA, and the fact that it is not subject to direct judicial oversight. This is a point that was emphasised by Dr Eric Metcalfe in his evidence to the House of Lords Select Committee on the Constitution:

> RIPA powers are often self-authorising with lower level communications data powers being authorised internally and even the highest level interception powers only requiring the authority of a government minister. This can be contrasted with the USA where, historically, there has always been independent judicial authorisation at the heart of the US surveillance process. (House of Lords, 2009, para. 160)

Indeed, the fact that authorisation for surveillance activities is done 'internally' continues to be a concern for the courts. In the case of *Re McE* [2009], for example, the House of Lords held that internal authorisation was inappropriate where the

surveillance interferes with legal professional privilege – in effect saying that such circumstances are as sensitive as when surveillance is conducted in a home or private vehicle (*Re McE* [2009] UKHL 15).

A further concern has been the growing use of RIPA powers by local authorities. According to the Interception of Communications Commissioner (2010), in 2008 public bodies made 525,130 requests for communications data under RIPA, with 1,765 of these being made by local authorities (Interception of Communications Commissioner, 2010 ,pp. 8 and 15). Given that there is evidence to suggest that many local authorities lack the expertise needed to interpret the provisions of the Act, these statistics are worrying. As noted by the Chief Surveillance Commissioner (2008, pp.12-13), local authorities tend to resort to covert activity as a last resort but when they do they 'have a tendency to expose lack of understanding of the legislation' and there is a 'serious misunderstanding of the concept of proportionality'. This has led to a number of high profile instances of what Big Brother Watch – an NGO concerned with issues of privacy in UK – has referred to as abuses of the Act (Big Brother Watch, 2010). Notable examples of such abuses include the use of RIPA powers to:

- Monitor local authority employees, and to investigate concerns over car parking, work times, and sick pay
- Spy on dog owners and enforce rules against dog fouling
- Catch individuals suspected of breaking the smoking ban, and
- Prevent illegal fly tipping.

These problems are compounded by the fact that there are also several other statutes that give local authorities and other public bodies the power to access communications data: the Social Security Administration Act 1992; the Charities Act 1993; and the Environmental Protection Act 1990. As noted by Liberty (2010, pp.70-1):

> Having powers spread across the statute book also means appropriate supervision and safeguards are diluted and it increases the likelihood that personal data is being accessed inappropriately.[43]

Although RIPA does provide a level of protection for information privacy in the UK, as is the case with the DPA, the regulatory framework it establishes is clearly characterised by a number of serious gaps, deficiencies, and legislative exceptions. In addition, because it does not seek to regulate the general use of public area surveillance technologies such as CCTV, it only partially strengthens the right to respect for private and family life contained in Article 8 of the ECHR, and fails to address one of the key threats to information privacy in the UK.

Finally, there is the question whether the definitions of surveillance contained in RIPA will be able to respond to continuing developments in information technology, social networking, and online communication. Does, for example, identifying the websites an individual has accessed constitute surveillance? Does RIPA regulate the monitoring of chat room discussions by undercover police officers?[44] If the police do not use technical methods to gain access to a Facebook page, but instead do so by way of a 'fake' online identity, does this require authorisation?[45] Given that an essential part of privacy is the ability to control access to one's information, it can be argued that the use of electronic or other measures to circumvent access controls and privacy settings is a form of surveillance that should require authorisation.

Other statutory privacy protections and limitations on the sharing of personal information

At present there is no general statutory power that permits public bodies to share data, and as such according to the principles of administrative law, public bodies can disclose personal information only if they have been granted the power to do so by statute. Although this restriction may appear to be clear, difficulties arise when it is possible to infer a power to share information from some other explicit statutory power. For example, according to section 111(1) of the Local Government Act 1972, local authorities have the power to do anything that will facilitate, or is conducive or incidental to, the discharge of any of their functions.[46] Given that it is an accepted principle of administrative law that express powers should be interpreted in such a way as to authorise actions that are incidental to them, it is easy to see how a local authority may regard itself as authorised to share various forms of personal information with other government bodies. Although any such sharing must comply with the rules established under the DPA and the principles of the HRA, the fact that there is no specific regime that regulates the sharing of personal information within government is cause for concern.[47] Not only can the absence of clear, uniform rules lead to variances in practice, it is also impossible for individuals to know with any degree of certainty the conditions under which personal information held about them might be shared.[48]

The position as regards data sharing is even less clear when it comes to actions of government departments. As is the case with public bodies, a government department is only permitted to share personal data if it is authorised to do so by law. This legal authority may come from statute but also from the common law or the royal prerogative. As the Ministry of Justice (then the Department of Constitutional Affairs) acknowledged in 2003 in its guidance on public sector data sharing (DCA, 2003), the law in this area is complex, and it may be possible for a government department to share data based on the common law or royal prerogative even if a power to share data cannot be reasonably implied from some explicit statutory provision.

In addition to the rules of breach of confidence and administrative law, there are a range of other statutory provisions that prohibit the disclosure of certain types of information by public bodies and government departments. For the most part, these are based on obligations of confidence and include (DCA, 2003, Section 5, para. 6):

(1) Medical confidentiality, according to the provisions of the Abortion Act 1967 and the Access to Medical Reports Act 1988
(2) Information supplied in connection with legal proceedings, according to the established rules of court
(3) Health and safety, according to sections 27 and 28 of the Health and Safety at Work Etc Act 1974
(4) Information provided to the Inland Revenue under section 182 of the Finance Act 1989 and section 6 and Schedule 1 to the Taxes Management Act 1970
(5) Information passed to the Child Support Agency as required by section 50 of the Child Support Act 1991
(6) The Human Tissue Act 2004, and
(7) Information obtained through the exercise of powers under the Companies Act 2006.

In addition, there are two other notable situations in which public bodies may be permitted to share personal information with either another such body or a government department. The first of these arises under section 115 of the Crime and Disorder Act 1998, which gives the power to disclose information when the disclosure is necessary or expedient for the purposes of that Act. This is an extremely broad provision, and while any such disclosure will be subject to the provisions of the DPA and the principles of the HRA, it provides a wide-reaching statutory basis for data sharing between public bodies. Similar powers are also provided by section 17 of the Anti-Terrorism, Crime and Security Act 2001. According to that section, personal information can be disclosed provided such a disclosure is connected with a criminal investigation or prosecution. While section 17(5) requires that the public body in question ensures that the relevant disclosure is proportionate to the legitimate aim being pursued (as per the requirements of the HRA and Article 8 of the ECHR), when it can be demonstrated that the disclosure or sharing is in fact proportionate, there can be no action for breach of confidence.

Although there is a considerable body of legislation governing the sharing of personal information, it is nonetheless extremely difficult for individuals to determine when and under what circumstances information about them has been disclosed. While the DPA gives individuals the right to know what information is held about them, it does not explicitly require individuals or organisations to disclose whether that information has been shared. As a consequence, even if individuals are able to ascertain that a

particular organisation holds personal or confidential information about them, they cannot be certain that the information in question has not been passed on. This lack of transparency represents a significant flaw in the current regulatory framework and potentially undermines many of the advances made by both the DPA and the HRA in terms of the protection of information privacy.

4.4 Common law protections

In addition to the general right to respect for private and family life provided by the HRA and the various statutory provisions and rules surrounding the collection, storage and processing of personal information, the common law also offers individuals a degree of privacy protection through the tort of breach of confidence.[49] Although the majority of cases in which breach of confidence is likely to be raised centre on disputes over trade secrets or government information, it is well established that the action is also available where the information in question is personal or non-commercial in nature. As a consequence, where an individual's personal information has been passed to a third party without his or her consent, then an action for breach of confidence may be available, provided the court is satisfied that the information in question was of a private or confidential nature.[50] In addition, following the decision of Lord Nicholls in *Campbell v MGN* [2004] UKHL 22, there may also be recourse to action for 'misuse of private information'.

Although it has been argued that the courts should go further and develop a new tort of privacy based on principles drawn from the law of breach of confidence, there are considerable problems associated with such an approach. First and foremost, there is a danger that – because of the high cost of civil litigation and the fact that legal aid is rarely available for private actions – any new tort of privacy will only be accessible to the wealthy. In addition, it is unclear as to what sorts of compensation would be available in such cases, particularly where the individual does not have a commercially valuable reputation to protect or has not suffered physical damage or psychological harm as a result of the privacy invasion. Finally, there is also danger that judicial activism in this area will only serve to make the existing law even more fragmented, and undermine the case for improved statutory regulation. Moreover, judicial activism is necessarily jurisdiction-specific. As a consequence, while the law may develop through the courts in England, this does not necessarily lead to legal change in Scotland or Northern Ireland, with the result that protection in the UK becomes further fragmented. For all of these reasons, although it may be tempting to look to the courts for greater protection of information privacy, it is clear that the common law cannot provide the sort of overarching and coherent privacy framework that is currently needed in the UK.

4.5 Guidelines, codes of practice, and 'soft law'

In addition to the laws discussed above, and other statutory measures, there are also significant elements of 'soft law', including codes of practice and guidance issued by regulators and other bodies. These instruments vary in their degree of formality and binding force, and represent an important part of the overall regulation and protection of information privacy in the UK. Given the close relationship between the operation of 'soft law' and the role of regulators, these protections are discussed in detail in the next chapter, which focuses on alternative approaches to the protection and promotion of information privacy.

4.6 Weaknesses of the current approach

Although information privacy is protected by a wide range of laws and regulations in the UK, the current regime suffers from a number of significant weaknesses. First, because the law has tended to develop in an irregular and largely sporadic fashion, there are substantial gaps in the information privacy protections offered to individual citizens. This is due to the fact that legal reform in this area is typically reactive in character, with the law responding to rapid and often unexpected changes in both the technological and political landscape of privacy, surveillance, and data sharing. For example, concerns about the protection of information privacy in the context of advanced computer technology were behind many of the regulatory provisions introduced by the DPA and RIPA. However, in the wake of 9/11 and 7/7, the expansion of data-monitoring powers has been the focus of a great deal of legislative activity. In particular, the Anti-Terrorism, Crime and Security Act 2001 undermines both of the earlier pieces of legislation in a number of key respects, most notably as regards the obligations of internet service providers to retain records of internet use.

Equally, although concern about the widespread use of CCTV has increased in recent years, public area surveillance remains relatively unregulated when compared to other, similarly intrusive forms of state surveillance and information gathering. As a result of this reactive approach, the overall system of surveillance and data collection regulation that has emerged in the UK is at times internally inconsistent, and could best be described as piecemeal. Furthermore, because the law has struggled to keep pace with the expansion of surveillance in the UK, the resources and powers granted to regulators have begun to look increasingly inadequate in light of the challenges they face.

Secondly, the rules and regulations that govern information privacy and the use of personal information are not based on any single rationale or set of stated principles. In part, this is a result of the fact that these laws have developed through a combination of case law, legislation, and informal attempts at self-regulation. The absence of clearly defined, overarching principles means that each piece of

legislation, line of judicial precedent, or code of practice has to be understood and interpreted within its own specific context. This can make the task of determining what rules apply to any given form of surveillance or data collection complex and time-consuming, and increases the likelihood that individuals will have their privacy infringed or their personal data misused.

Finally, due to its diverse and de-centralised nature, no single body or individual is responsible for protecting information privacy in the UK, or for overseeing the system of surveillance and data collection regulation in the UK. At present, the ICO, the OSC, the Interception of Communications Commissioner, the Scottish Information Commissioner, the Independent Police Complaints Commission, the various directors of the security services, and the Secretary of State all share responsibility for monitoring and regulating surveillance practices and technologies, and/or for ensuring that information privacy is respected by the organisations within their jurisdiction. While there is some communication between these bodies, there is little evidence to suggest that there is much inter-agency coordination, either in terms of oversight of surveillance practices or the administration and enforcement of penalties for non-compliance. As a result, it is difficult to assess whether information privacy is being adequately protected, or whether there are substantial gaps in the legal regime that need to be filled by new laws or regulations.

4.7 Summary

This section has provided a brief overview of the various statues, regulations, and common law rules that govern individual privacy and the use of personal information in the UK. Although it is difficult to generalise about such a diverse and complex area of law, it is possible to identify a number of key trends in the recent development of privacy laws in the UK. While it is true that the HRA, the DPA, the FOIA, and RIPA – and the Scottish versions of the last two – have brought about significant changes in the way in which government and public authorities think about information privacy, it is clear that more attention needs to be paid to ensuring greater consistency in the way in which information privacy issues are understood and strengthening the legal regime and the powers of the regulatory agencies responsible for enforcing existing laws and regulations.

Another trend that has implications for the protection of information privacy in the UK is the continuing expansion in the surveillance apparatus of the state – most notably on the grounds of national security, prevention of crime, and public sector efficiency. Given that this expansion has been accompanied by only a relatively small increase in the powers or resources available to regulatory authorities such as the ICO or the various surveillance commissioners, the question arises as to whether the existing

system of information privacy protections is being properly enforced, or is indeed adequate.

Finally, there appears to be a continuing reluctance on the part of government to consider the possibility of widespread reform of the existing law so as to rationalise the existing piecemeal structure and create a single, comprehensive regulatory framework for surveillance and data collection.

5. Complementary approaches for enhancing privacy

5.1 Introduction

General or sector-specific privacy law is necessary, but not sufficient for privacy protection. To ensure compliance, laws depend on the efforts of a regulatory agency such as a data protection authority and other mechanisms operating within a legal framework across society, in government and in business organisations. Measures that complement statutory or common-law mechanisms have developed over many years as additions to the array of instruments for personal data protection. Some would argue that they are more effective than legal instruments and are more sensitive to the variety of information contexts and practices. Others remain suspicious that these instruments can only weaken protection, especially if they substitute for law. This Chapter examines some leading complementary approaches and assesses their contribution to the aim of protecting privacy and human rights. These approaches include codes of practice, privacy-enhancing tools and modes of evaluation that are built into the design of information systems, and the raising of public awareness. Our aim is to describe these instruments and point out their strong and weak points. We begin with a general explanation before examining the UK situation.

5.2 Self-regulatory approaches

The wide range of self-regulatory instruments cannot be discussed here.[51] However, amongst the most important are codes of practice or conduct and standards. They are derived from a general data protection law and usually operate in an information-governance context within public or private organisations. With the recognition that statutory law may be inadequate to protect information privacy by itself, codes have come to be regarded with greater favour by data protection policy-makers as adjuncts to legal regulation. Sometimes, however, codes of practice exist in the absence of specific or sectoral law governing information practices, as in the USA, which lacks an omnibus data protection law. In some countries – the Netherlands, New Zealand, Australia, Ireland, Canada and the UK provide examples – codes or standards play a more integral part of a statutory regime and may be overseen by the regulatory body.

The strength of data-protection codes, as of other self-regulatory instruments, lies largely in their tailoring of general legal provisions or ethical precepts to the circumstances of an industrial or business sector (for example, banking), a technology (for example, smart cards), a profession (for example, market researchers), or a process (for example, direct marketing). Privacy protection and – where it exists – the law are thus more likely to be understood in the concrete terms current in these sectors. It is more likely to address the specific contexts in which

individuals' personal data is processed. The process of developing a code in conjunction with the advice of interested parties and regulators may be valuable in helping data controllers appreciate the importance of protecting the privacy of their customers or clients. Going further, context-specific guidance based on a code can be a useful way of getting managers or employees to implement the fine grain of privacy protection.

However, codes have been controversial because they have often been encouraged by industries that aim to forestall legislation and who prefer self-regulation to more rigorous regulation by statute; they see codes as a less onerous substitute for law (US Department of Commerce, 1997). Privacy advocates have therefore distrusted self-regulation as a weak form of privacy protection, because it is often perfunctory and symbolic, rather than implemented with force. Where codes are adopted reluctantly or as a means of regulatory avoidance, they may be a poor substitute for rigorously enforced law. In addition, a code's mechanisms for redress, transparency, and sanctions may be wanting, and the ability of a trade association or other 'peak' organisation – or indeed, a public sector agency – to discipline its member organisations, companies, professionals or other staff may be limited.

Therefore, under these conditions self-regulation is unlikely to adhere to privacy-protection principles unless it takes place within a statutory regime. Moreover, if data controllers are not organised into sectors or industries, there is no overarching organisation capable of adopting a code that would bind or influence controllers' information-processing activities. Whether the state functions as a single entity or, in reality, as a collection of separate organisations, may have an important bearing on the usefulness of public sector codes. An important question for this country could be whether each central government agency or department should adopt its own code of practice pertaining to its functions; whether there should be one for all of them, perhaps 'owned' by the Cabinet Office; or whether there should be a central push and oversight with responsibility and further 'tailoring' resting on each organisation.

In the UK, a prominent role was envisaged for codes of practice in the 1978 Lindop Report that preceded the passage of the first UK data protection legislation.[52] Lindop explored options for creating a system of some 50 codes having the force of law and as a main activity of an independent data protection authority. In the event, subsequent UK data protection legislation did not go down this route – partly because it challenged Ministerial powers – but since then there has been a development of codes and their incorporation as parts of the regulatory regime.

Codes are integral to the UK data protection regime but have played perhaps a less conspicuous role than elsewhere. Some codes have originated within sectors or

organisations themselves, public or private, while others are promulgated by the ICO following consultation, as is explained below. Among the codes are those for the sharing of personal data (currently being revised; see below), employment, the fair processing of telecommunications directory information, privacy notices, police forces, online privacy, ICO assessment audits, and CCTV. The Audit Commission adopted a statutory Code of Data Matching Practice in 2008, applicable to its National Fraud Initiative, and Audit Scotland was consulting on one in 2010. Also bearing upon privacy are the codes of practice that fall under RIPA, for the interception of communications, acquisition and disclosure of communications data, covert surveillance and property interference, covert human intelligence, and for the investigation of protected electronic information. The Scottish Government has been developing a central set of principles for identity-management systems. This is a type of code complementing the data protection principles in the context of identity management as a specific kind of information use, although with wider applicability.

Section 51 of the DPA requires the Information Commissioner 'to promote the following of good practice by data controllers'. This includes activity with regard to codes of practice, whether the code is ordered by the Secretary of State – a Government Minister – or whether the Commissioner considers it appropriate to prepare and disseminate one. In the former case, the Commissioner lays the draft code before each House of Parliament. In the latter case, he must consult with trade associations and data subjects or their representatives before issuing the code. But he may also encourage trade associations to prepare and disseminate a code, giving an opinion on it following consultation.

The coverage that codes provide for areas of potentially privacy-invasive information practices is patchy, and the development of a more comprehensive framework for their development and implementation has been slow. Codes may have a number of shortcomings, including a lack of clear terminology, uncertainty about the intended audience, and ambiguity about the relationship between encouraging good practice and requiring legal compliance. The code may be imprecisely tailored to the circumstances of different data controllers, and may leave unclear the relationship between the code and other guidance that relates to data controllers. Moreover, public reassurance that a code is obeyed may be unwarranted. While some codes are relatively straightforward in applying data protection principles (for example, the ACPO code for police forces), others are very – if necessarily – complex in their coverage (for example, the employment practices code).

The effectiveness of codes in improving compliance or practice cannot be easily assessed, but one value of a code may lie, as mentioned, in the learning process through which they are shaped and communicated within an organisation. Another

lies in the presumption of adherence, so that ignoring a code may have adverse consequences if legal proceedings are brought against a data controller. A third lies in the relatively easier processes involved in updating and revision – as with the CCTV code, for example – when technologies or other circumstances change, rather than having to resort to the parliamentary vagaries of legislative amendment or revision.

A code of practice could play a potentially important role with regard to the sharing of data, an increasing practice across the public sector that gives rise to concerns about privacy, perhaps particularly in terms of individuals' ability to understand and control what happens to their data. The *Data Sharing Review Report* (Thomas and Walport, 2008) called for the Information Commissioner to be required to produce and keep up-to-date a data-sharing code of practice that would be approved by Parliament. This would replace the existing 2007 Framework Code of Practice, which had no statutory standing or parliamentary involvement. A statutory code would be an authoritative interpretation of data protection principles, establishing standards for information sharing. Breaches would not be illegal, but non-compliance would be taken into account by the courts and the Information Commissioner in relevant cases. The Government accepted that the Commissioner should have the recommended statutory duty to develop the code (Ministry of Justice, 2008), and the proposal was also endorsed by the House of Lords Constitution Committee in 2009 (House of Lords, 2009).

Data-sharing protocols are similar self-regulatory mechanisms that operate within legal privacy-protection frameworks in situations where personal data are exchanged or shared among agencies of different kinds. In multi-agency partnerships for social and health care or community safety, these documents set out the conditions governing data sharing among the bodies involved. They may be formal agreements made with national guidance, as for example that given by the Home Office with reference to multi-agency public protection arrangements (MAPPAs) following the passage of the Criminal Justice Act 2003 (Bellamy *et al*., 2008). Protocols, however, have often been too elaborate and complicated for frontline service practitioners to implement in their daily work. Therefore, their regulatory efficacy – taken by themselves – and ability to raise employees' awareness of privacy issues affecting public-service clients – frequently among the most vulnerable individuals, who are less capable of protecting their own privacy – may be questionable.

5.3 Designing privacy protection into information systems

Over the past 20 years, there has been an increasing worldwide interest in protecting information privacy through the use of technologies operating either at the organisational and systems end or at the individual's end of the flow of personal data.

Generally known as ‘privacy-enhancing technologies’, or PETs, they offer alternative or complementary ways of limiting privacy invasion, but the question whether privacy is thereby enhanced, merely maintained, or threatened in unforeseen ways has often been debated. PETs offer a way of building privacy into systems, rather than bolting them on as expensive and ineffective afterthoughts.

PETs may help data controllers to comply with many of the requirements of privacy laws and principles. They can preserve anonymity and confidentiality, provide physical security for data, give greater control and choice to individuals, and harness the rule-making properties of information technology (for example, software ‘code’) to the cause of privacy protection (Lessig, 1999; Reidenberg, 1998). PETs, however, should not simply be equated with data-security technologies – for example, passwords, locks, and encryption – in that those devices do not address the legitimacy of data collection, storage, or exchange, which are all integral parts of information privacy laws and principles, as well as of the right to privacy (Burkert, 1997).

It is less important to identify and describe particular PETs than to note how they can be put into practice. Some are built into the design of systems and networks (for example, default settings governing what data are collected) and may be incorporated into policies for public-service provision (for example, public-key cryptography, secure websites, and biometrics – albeit controversial in terms of privacy). Others are in the hands of individuals themselves as they seek to control their data and protect their own privacy (for example, anonymous web browsers and ‘cookie’ filters).

In terms of privacy protection, strong or weak forms of these instruments can be found. As with codes, PETs can give a false sense of reassurance, or detract from more stringent means of protecting privacy through legal requirements and enforcement that are necessary. PETs are not a ‘technological fix’ for problems of regulation, parliamentary scrutiny, or governmental self-restraint. Their effectiveness may depend on how they are implemented. This may be left to the market, giving signals to information technologists and businesses to incorporate PETs in their system architectures and commercial practices. It may be a matter for public policy, mandating PETs in IT systems used for public-sector transactions. Or the initiative may lie with the general public, demanding technical safeguards and obtaining specific consumer privacy tools. In other words, PETs’ contribution depends on normative and practical decisions. Despite the enthusiasm for PETs, their deployment has faltered: online businesses and consumers have not been sufficiently persuaded to develop or demand them (OECD, 2001). The lack of recognised standards to guide implementation, uncertainty about the benefits of

PETs, absence of managerial recognition of a responsibility to protect privacy, and the fear of adopting obsolescent PETs are cited by the ICO as among the reasons for reluctance to implement these design solutions (ICO, 2008).

Privacy technology efforts have now been re-presented and promoted at national and international levels in terms of 'privacy by design' (PbD) (Cavoukian, 2009; ICO, 2008). This reformulates the PETs philosophy with greater emphasis on system architectures rather than the individual's own implementation or on technical devices as such. PbD presses for a comprehensive set of information governance practices, standards, and modes of accountability within organisations that process personal data. PbD requires organisations to understand and accept the need for proactive ways of complying with privacy protection laws and principles. It might also ideally require them to have a more nuanced, and perhaps social-psychological, understanding of the contexts and situations in which people use technology in their relationships with others, including the state (Palen and Dourish, 2003). In the UK, emphasis is now also given to articulating the business case for privacy-protective business processes and information systems, thus helping to achieve a 'privacy dividend' (ICO, 2010a).

It is too soon to say whether these initiatives will bear fruit in the public sector where PbD and PETs could be mandated in system procurement requirements and contribute to the protection of privacy rights. However, the historic lack of success of efforts to encourage and cajole organisations, and other reasons, have prompted a stronger advocacy of PbD by various authoritative EU sources.[53] The European Data Protection Supervisor, for example, has most recently pressed for embedding the principle of PbD in EU laws and policies at general and sectoral levels of information and communication technology within the European Digital Agenda, and in other situations.

Privacy impact assessment (PIA) is a related, and increasingly popular, privacy protection technique that plays a part in self-regulation through its association with design solutions. It can have a key role within statutory regimes: it is legally mandated in some countries for new technological systems, including the USA at the federal level. PIAs are described as 'structured assessments of a project's potential impact on privacy, carried out at an early stage' (Thomas and Walport, 2008, p 31). They vary considerably in their implementation in terms of how, when, why, and by whom they are undertaken, how comprehensive they are, as well as other factors. PIAs are built upon risk assessment but are oriented towards assessing and mitigating risks to individual privacy rather than risks to the organisation. However, organisations may be prone to misconstruing PIAs as merely a way of assessing and mitigating their own legal and financial liability. In the UK, the use of PIAs has been

endorsed and promoted by the Information Commissioner (ICO, 2008; ICO, 2009). The rash of data breaches in the UK in 2007-08 resulted in a Government report that endorsed PIA for government departments (Cabinet Office, 2008). They are not required by statute, although the House of Lords has recommended that the DPA be amended to make them mandatory (House of Lords, 2009).

If their development involves organisations in a searching analysis, PIAs can help to instil a culture of privacy protection. They can also facilitate practical steps in the design and deployment of information systems, in the training of staff, and in the acceptance of managerial responsibility for privacy. If guided by principles and with an eye towards safeguarding privacy rights, they thus may contribute strongly to privacy protection independently of legal compliance requirements, and on a broader and deeper basis than the law may demand. On the other hand, PIAs are prone to perfunctory and box-ticking performance to minimal standards of analysis and reporting, rather than in terms of principles. Once again, a deceptive impression may be given of the organisation's willingness and ability to protect the data they collect, store, or share, and the PIA may fall short in assessing and mitigating risks of adverse impact on privacy. Moreover, in addressing the question how a proposed information system could affect privacy or related values, PIAs may place less emphasis on the more fundamental question whether the data processing or surveillance should happen in the first place.

5.4 Public awareness and education

Laws, codes, and technological design are insufficient for privacy protection without the ability of individuals and groups to help prevent privacy invasions and to press for remedial action. Privacy regulators rely on the public and advocacy groups to bring pressure to bear upon potential intruders on information privacy, to complain about specific violations, and to seek redress. For these purposes, regulators as well as others engage in campaigns for raising the level of public awareness about their rights and about the way information processing affects them. A public that is more aware is arguably more likely to be able to take steps to protect their personal data, to assert their right to information privacy, and to seek remedies.

Greater public awareness can be brought about through the promotional efforts of regulators, such as the ICO, who provide publicity material, usable websites, and guidance to information processors as well as the general public (European Commission, 2009). In the UK, the Information Commissioner's alarm bell about 'sleepwalking into a surveillance society' (Ford, 2004) was followed by a special report (Surveillance Studies Network, 2006) that gained prominent media exposure and prompted important inquiries by parliamentary committees. Other reports in recent years have helped to elevate the issues to prominence (Royal Academy of

Engineering, 2007; Liberty, 2007; House of Lords and House of Commons, 2008; House of Commons, 2008a, House of Commons, 2008b).

In many countries, the attempt to increase the level of public, as well as parliamentary and governmental, awareness and concern about privacy and surveillance is spearheaded by non-governmental organisations (NGOs). These have included general civil liberties and human rights groups as well as more specialised groups of privacy advocates and single-issue campaigns concerning, for example, identity cards, supermarkets' use of personal data, health privacy, or internet privacy issues. However, compared with pressure group activity in many other areas, privacy advocacy as such takes place through under-resourced, loose and fragmented networks, with sporadic success (Bennett, 2008).

In the UK, one can identify privacy-related campaigning, publication, and awareness-raising work undertaken by many NGOs.[54] The media sometimes publicise alarming examples of privacy invasion and surveillance – for example, 'snooping' on parents of school-age children – and internet blogging and privacy-advocacy websites alert people to dangers of information collection and use. Influence over public opinion and policy is hard to measure, but some groups have gained legislative success through pressure, contacts with parliamentarians, briefings, as well as contributions to drafting Bills and secondary legislation. Many groups have also maintained consultative channels to the ICO. The House of Lords has recommended that the Government should involve NGOs in the development and implementation of policies involving surveillance and data processing that have significant implications for the citizen (House of Lords, 2009).

The strength of such efforts at public education and awareness, as well as policy influence, is that they are formally independent of political party and governmental control. In addition, groups often possess specialist knowledge of technologies, business processes, academic and legal research, and sectors of public opinion that can be brought to bear upon governmental and business decisions. On the other hand, their influence often depends upon how well they capitalise on scandals and 'horror stories' for their campaigning activities and their attempts to influence public debate. Moreover, the elusiveness of the meaning of 'privacy' and the intricacy of issues and problems arising from data activities make it difficult to get messages across to the public and politicians, except perhaps with regard to a few dramatic and tangible surveillance devices such as CCTV installations. Some of these deficiencies may be mitigated to the extent that NGOs and campaigners are seen as 'within the tent' in terms of policy-making, but that in turn may bring the danger of blunting their edge.

A further benefit of raising public awareness is that it can bring issues to attention that might otherwise be obscured. For example, the question of how information privacy is distributed across society – whether it is acceptable in our society for some to have more privacy than others – is more likely to be raised and placed on the policy agenda through such activities outside government than through official routes. Marginalised or vulnerable ethnic and socio-economic groups, and not merely individuals, may be 'privacy-poor' as well. They may lack the means of recourse to legal remedies and the ability to challenge surveillance practices that impinge on them, for example as targets for data gathering and monitoring, more than on other people. Unless their cause is championed by NGOs, the media, regulators, or individual parliamentarians, it is likely to go unheeded.

5.5 Some regulatory developments abroad

Privacy or data protection laws have proliferated in Europe, North America, and the Asia-Pacific region. There are also a variety of relationships between these statutory means and the provisions of some national constitutions, charters of human rights, and other high-level declarations. National legal instruments for privacy and data protection are also shaped by international documents, of which the most prominent are those of the Council of Europe, the European Union, and the OECD (Council of Europe, 1981; OECD, 1981; European Union, 1995), but motives related to free trade and the internal market of the EU often compete with the human rights and privacy dimensions of these measures.

As in the UK, other countries have had mixed experiences with alternative or complementary approaches. Although USA federal agencies are covered by the Privacy Act of 1974, self-regulation is most prominently followed as the preferred path in the USA for the private sector where the coverage of privacy laws is patchy and regulatory 'watchdog' machinery is lacking. As suggested earlier, PETs have not, so far, fulfilled their promise anywhere although they have been selectively implemented; it remains to be seen whether PbD constitutes a lasting improvement. Concerning the raising of awareness and the public's knowledge of their rights and what happens to their data, special occasions such as 'Data Protection Day' events have risen to prominence in the past few years in many countries (Council of Europe, 2010), although beyond the immediate publicity they gain for privacy protection, their long-term effect cannot yet be gauged. If high levels of public awareness and vigilance are supposed to act as social support mechanisms underpinning legal and formal regulation, it is too soon to tell whether this is taking place. However, some surveys indicate relatively high, albeit fluctuating, levels of public concern over the protection of their data, perhaps especially online and in social networking processes.[55] But it is prudent to be cautious about surveys and focus-group research,

because of their methodological shortcomings and the inherent difficulty of carrying out enquiries into such an elusive and ill-defined value and right as privacy.

An important piece of unfinished international business is the establishment of high-level standards for privacy protection and for the rights associated with it. These can be formal and technical standards, dealing with matters of data security, as promulgated by the International Organization for Standardization or other bodies. Attempts to go further into information governance and adherence to wider criteria of good, privacy-protective practice have met with considerable business resistance.

A recent manifestation of the push towards better standards came in the 2009 Madrid Resolution of the world's privacy and data protection commissioners, supported by the 2009 Madrid Declaration of NGOs, privacy advocates, and other organisations and persons (Madrid Resolution, 2009; Madrid Declaration, 2009). These called for global standards, closely aligned with the conventional data protection principles but going further into matters that included better international regulatory co-operation, staff training, PIAs, PETs, and other proactive procedures. The Resolution emphasised:

> the universal nature of the principles and guarantees underlying this right [to privacy], and by contributing to a better protection of rights and freedoms of individuals in a globalized world, characterised by cross-border flows of information.

The Declaration went further to call for a moratorium on many forms of surveillance, and for:

> the establishment of a new international framework for privacy protection, with the full participation of civil society, that is based on the rule of law, respect for fundamental human rights, and support for democratic institutions.

5.6 Summary

There are many ways of protecting privacy in addition to legal provisions. Some of the leading instruments have been outlined, with comments on their efficacy and likelihood of doing the work that law itself cannot do. However, it is important to emphasise three significant points that will affect any reforms in the safeguarding of information privacy rights that might be proposed. The first point is that law is essential: without legal specification of privacy rights, other instruments will be busy but blind to the main issues at stake, and are likely to be incapable of providing the remedies that individuals may need.

The second point is that the principles written into law or underpinning it must be – and normally are – reflected in the specification of other instruments, which can then be seen as reinforcements and complements to the law and not as substitutes for, or weaker versions of, privacy laws. For example, the minimisation of personal data collection, the several dimensions of the quality of data (accuracy, relevance, non-excessiveness, and timeliness), and the specificity of purpose for data processing are among the principles that should be inscribed in non-statutory mechanisms if they are to provide a high degree of protection in conjunction with the law.

The third point is that the art and science of better privacy protection involves articulating the various legal and other devices with each other. The aim is to design them into a comprehensive protection regime and not leave them simply as a piecemeal inventory of measures or ‘tools’ implemented in a disjointed fashion by various agents, leaving gaps through which privacy intrusions and the erosion of rights may enter. Whose responsibility it should be – and at what levels, from the local to the global – to ensure the required integration of instruments and approaches is an important question for regulatory governance to address.

6. Moving forward

6.1 Introduction

Commentators have often criticised the gaps and inadequacy of information privacy in the US, as compared with the UK and the rest of the EU. Pointing to the EU Directive – described in Chapter 4 – and its various national incarnations, they have argued that it provides far stronger privacy protections for European citizens and residents than those enjoyed by their US counterparts. In large part, this is because it covers the private sector as well as the public, and requires a 'supervisory authority' to enforce the law and perform other important regulatory functions, rather than leaving individuals to pursue privacy violations in the courts. Unfortunately, this comparison is only partially valid, and dangerously complacent. Not only is it overly reliant on a comparison of legislative texts rather than a detailed assessment of how protections in these different jurisdictions work in practice, it also underplays the extent to which the European approach often lacks the certainty and solidity that a rights-based regime requires. Privacy is not best served by the current patchwork of laws and other instruments that are in place in the UK today, or by the lack of an overarching regulatory framework within which the idea of information privacy could play an important part in the protection of this fundamental human right.

In the UK, governments of whatever political party, and parliament, have long resisted the enactment of a general privacy law, mainly because they have a vested interest in processing personal data in pursuit of their policies. From the 1980s onwards, they have only reluctantly and reactively placed data protection law, the regulation of investigatory powers, and human rights law on the statute book, although there was a spate of legislation late in this period. As far as data protection is concerned, both in 1984 and in 1998 governments legislated for fairly minimal protection through cumbersome and ambiguous legal provisions that leave too much open to interpretation and fortuitous circumstance before privacy invasions can be challenged effectively. They have resisted giving more powers and resources to the ICO as the main regulator for information privacy, and have only recently begun to raise concerns about the rise of the 'surveillance society' and the adverse nature of many of its effects. Governments have continually given order-making powers to Ministers to override privacy restrictions on the way personal data is collected, processed, and disclosed. This trend was only recently reversed with the abandonment of clause 152 of the Coroners and Justice Bill in 2009, which would have created a broad power to share personal data for any governmental 'policy objective'. Parliament has often found itself unwilling or unable to resist policies and laws that erode privacy, and has sometimes revealed its inability to understand sufficiently the nature and extent of the threats to privacy posed by technologies, economic processes, and even well-intentioned political will. The role of NGOs and

individuals in shoring up and pursuing the enforcement of information privacy rights has been consistently undervalued.

As discussed in this Chapter and the next, there is a pressing need for reform in the area of privacy. In particular, this report argues that more emphasis needs to be placed on rationalising existing protections, ensuring greater coherence across different sectoral privacy laws, and strengthening the powers of the regulatory agencies responsible for enforcing these laws. In addition, this report takes non-legal mechanisms and instruments seriously, and aims to embed them more firmly into the culture and practices of public and private organisations.

The most important step is to bring the existing array of protective or permissive legislation into better and clearer alignment, and to focus it upon purposes more than on expediency, and to ensure that human rights are protected. Data protection law and practice should be harmonised with human rights law so that, within government policy, values beyond information security and the need for effective and efficient data processing are more clearly recognised, requiring a broader commitment to privacy from those who collect, use, and disclose personal data. The regulatory oversight and guidance provided by the investigatory powers regimes need to be clarified and made more effective so that those engaged in different forms of surveillance have a clearer grasp of the legitimate scope of their powers. The juxtaposition of several kinds of Commissioner in the world of surveillance and data protection needs reconsideration in terms of the clarity of roles, relationships, and resources to provide sufficient safeguards for the public. Gaps in the coverage of laws, so that some surveillance domains are inadequately regulated – for example, the DNA database and CCTV – need to be remedied through statutory enactment guided by existing human rights and data protection legislation.

We have seen how an overview of information privacy's rationale and conceptual basis, along with an assessment of the threats posed to privacy by the development of data collection and surveillance, can provide a context for looking at the privacy-related laws and regulatory regimes currently in place in the UK. We have identified key features of the existing system that could form a basis for future privacy protections, and pointed out areas of weakness that would need to be overcome if privacy regulation were to have a more principled foundation and a more coherent structure.

We do not believe that there is one 'best solution' for shoring up information privacy rights and ensuring that surveillance does not pose a threat to fundamental human rights. This Chapter sets out a number of principled and practical approaches that could help to achieve these goals. These approaches involve different areas of the

law as well as different social and technological means of reform, and seek to identify new paths for privacy protection. Although we identify four key approaches, these should not be seen as a menu from which one best choice must be made. There is much room for debate, one that recognises that some of the approaches – and indeed others that could be envisaged – represent different emphases rather than clear alternatives to each other.

6.2 Approach One: a principled foundation

We believe that the protection of information privacy and the regulation of surveillance and data collection must be based on a clear, principled foundation that is consistent with a commitment to equality and fundamental human rights. 'Principles-based regulation' (PBR), more than 'rules-based regulation', has found favour as an effective way of regulating privacy, and has been recently advocated in the privacy work of the Australian Law Reform Commission's (ALRC, 2008). Although PBR is characterised by a number of paradoxes that may reduce its attractiveness,[56] relying on principles provides necessary flexibility in a climate of rapid technological change and growing threats to privacy, and focuses on achievable outcomes rather than the strict enforcement of prescriptive rules. While emphasising principles, the ALRC has recommended a hybrid approach that also makes clear the importance of clear rules and sectoral regulation. In this approach, rules are provided for sectors and fields in which there is a need for clarity about how the principles are to be fulfilled. This is achieved through specifications in subordinate regulations, supplemented by guidance.

In the UK, Article 8 provides an overarching framework for the protection of privacy, and the system of data protection already operates at both the level of eight broad principles (see below) and of more specific rules and guidance, although – as in many other countries' systems – it uses a wider range of instruments as well (Bennett and Raab, 2006). Whether data protection law as such works well enough in its entirety, or needs specific redrafting and better implementation is, at the time of writing, a matter for wide consultation and deliberation in the UK and the EU. However, the question of the effectiveness of the legal and human rights instruments that are involved in UK data protection, and the translation of principles into practice, is of considerable interest.

The most prominent and long-standing set of principles in the world of privacy protection and information rights are the data protection principles. These are found, in one form or another, in the landmark documents mentioned in Chapter 4: the OECD Guidelines of 1980, the Council of Europe Convention of 1981, and the European Data Protection Directive 95/46/EC. They are also reflected in a large number of countries' national legislation and in 'fair information practice' standards

where such legislation is absent.[57] Approaches to the regulation of data collection and processing at both the global (for example, the Madrid Resolution, 2009) and lower levels (for example, for identification and verification purposes, as being developed by the Scottish Government) draw heavily upon these principles. In light of this, questions remain about how helpful these principles are when it comes to regulating online activity and uses of personal data that were not envisaged in the 1980s and 1990s. They nonetheless provide an important and practical starting point for thinking about information privacy reform in the UK.

As set out in the UK DPA, Schedule 1, Part I, the data protection principles are as follows (abridged):

- Personal data shall be processed fairly and lawfully […].

- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- Personal data shall be accurate and, where necessary, kept up to date.

- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

- Personal data shall be processed in accordance with the rights of data subjects under this Act.

- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

In addition, the DPA gives individuals the right to find out who holds what personal data about them, to obtain a copy of it, to correct or erase it if it has been unlawfully processed, and to obtain remedies if these access and correction rights have not

been complied with. Certain special categories of ‘sensitive’ personal data, such as racial origin, political opinions, religious or other beliefs, and personal data related to health or sex life, have additional legal constraints placed on their processing in Schedule 3 of the DPA.

Provided they are enshrined in legislation – as is the case with the DPA – and rigorously adhered to, these principles can help to provide a considerable level of privacy protection. This is especially true where the principles are tailored to the context and conditions of particular sectors as, for example, recommended by the Lindop Report (Home Office, 1978). However, unless additional principles – such as a principle of ‘fair processing’ – are added to the existing list, they are unlikely to be sufficient. For example, Pounder (2008) has argued that the current UK data protection regime is more concerned with the ‘how’ of data processing than with the question of whether processing should take place or not. Further, he argues that because the existing regime does not provide regulators with the powers necessary to prevent the state from engaging in overzealous surveillance and data collection, an additional nine principles are needed. Although one of these new principles deals with issues of compensation, for the most part they are aimed at ensuring that the state must demonstrate that any new surveillance measure is necessary and proportionate, or promoting better parliamentary and regulatory scrutiny of government surveillance practices (Pounder, 2008, p. 19). Such principles are central to ensuring that the rights contained in Article 8 are properly protected, and that any interference with those rights must be in accordance with the law, justified, proportionate and necessary.

In contrast to these proposals, the ALRC recommends a principle of ‘notification’ requiring ‘organisations to notify individuals or otherwise ensure they are aware of particular matters relating to the collection and handling of personal information about the individual’ (ALRC, 2008, vol. I, p. 37).[58] A related principle is transparency or ‘openness’, requiring ‘organisations to operate openly and transparently by setting out clearly expressed policies on its handling of personal information in a Privacy Policy, including how it collects, holds, uses and discloses personal information’ ALRC, 2008, vol. I, p. 39). However, experience to date with organisations’ opaque and legalistic privacy policies online and elsewhere has been far from encouraging, and better approaches to implementing transparency need to be found, perhaps including strong information rights or ‘trust’ charters adopted by public agencies (Raab, 2003). A third principle is found in the OECD Guidelines but recently developed in the international experts’ ‘Galway Project’, and it is also reflected in the 2009 Madrid Resolution of the International Conference of Data Protection and Privacy Commissioners, and in the Article 29 Working Party’s contribution to EC consultation on the future of privacy’s legal framework. This is the principle of

'accountability' which, although expressed in terms of 'companies', would also apply to the public sector; it:

> shifts the focus of privacy governance to an organisation's ability to demonstrate its capacity to achieve specific privacy objectives. It involves setting privacy protection goals for companies based on criteria established in law, self-regulation and best practices, and vesting the organisation with both the ability and the responsibility to determine appropriate, effective measures to reach those goals. [59]

It is debatable whether 'consent' should be a further principle in its own right, or whether – because it is so difficult to define and apply in practice – it should only play a supportive role to the package of other principles. The ALRC considered this question following a lengthy consultation process, and concluded that consent should not be a discrete privacy principle. It did, however, note that consent 'plays a key role in the application of other privacy principles – namely those regulating the collection of sensitive information, use and disclosure, and cross-border data flows' (ALRC, 2008, vol. I, p. 686),[60] and that it should therefore be the subject of guidance and clarification by the regulatory authority. On the other hand, Rule (2007, pp. 195-6) has argued that the default position for the public or private sector should be that there can be no collection, storage, processing, or sharing of personal data without the meaningful and informed consent of the individual concerned, or – in the case of the public sector – legislative authorisation. This idea has been adopted by some privacy regimes, and has particular rhetorical force in a democracy, where the doctrine of 'the consent of the governed' has a long-established and foundational basis in constitutional theory.

Because this commitment to consent is so frequently set aside for good cause by circumstances and necessary information requirements in different sectors (for example, in the criminal justice system), and by problems associated with gaining 'informed consent', it is open to question whether such an 'informational self-determination' principle can serve as a robust foundation for the right to privacy.[61] In addition, the circumstances under which consent is sought (or revoked) vary considerably across different sectors. As a result, this is a good example of where a general privacy principle needs to be supplemented by particular rules and guidance. But regardless of the approach adopted, there also needs to be a fundamental rethinking of the role of individual consent as regards personal information, and recognition of the fact that privacy – although a right – is in part a function of individual and social expectations in specific contexts (Nissenbaum, 2010). There is a clear need for a deeper debate about role of consent in privacy protection before a satisfactory resolution can be achieved for the UK.

In sum, both the data protection principles and the more general privacy principles outlined above can play a crucial role in helping to create and shape a framework for the effective protection of information privacy rights, and by extension, other rights that support but are not directly concerned with information privacy. They give rise to general rules, and also specific laws in sectors where there is a need to clearly define the relationship between individuals and those who might threaten their privacy through the collection and use of their personal data.

The important role that can be played by principles can also be illustrated by comparing two basic approaches to privacy law and regulation – what Nissenbaum (2010, pp. 237-8) refers to as the **omnibus** and the **sectoral** approaches. The **omnibus** approach is based on the assumption that privacy is a fundamental value, and can provide a starting point for both the development of general privacy laws and regulations as well as the drafting of detailed legislation and the application of specific rules.

The **sectoral** *a*pproach is based on the idea that each sector of society needs to take a different approach to questions of privacy, and that there is little value in attempting to define privacy or explicitly recognise an overarching right to privacy. According to this view, reform should be undertaken on a sector-by-sector basis, with different privacy laws being introduced for health, law enforcement, communications, and so on. It has become commonplace to contrast European ‘comprehensive’ data protection legislation with the American ‘sectoral’ patchwork (Gellman, 1993), but this is an oversimplification more common to policy rhetoric and does not stand up to closer analysis, at least as far as its description of Europe is concerned.

The current UK approach is a hybrid of these two approaches: omnibus and sectoral. As has already been argued throughout this report, this mixed approach has not worked particularly well in the UK, mainly because many fundamental privacy principles have been undermined or obscured as a result of the complexity and inconsistency of the current system of legal protections. At present, the protection of privacy and the regulation of surveillance and data collection is achieved through a haphazard combination of legislative provisions, regulatory guidelines, common law, judicial decisions, and other ‘soft law’ instruments. This fragmented approach to privacy has a number of serious shortcomings. On the one hand, it makes it difficult for both public and private bodies to locate and correctly interpret the relevant law, with the result that it is all too easy for these organisations to infringe the public’s legitimate and legal expectations of privacy. From the point of view of the individual, it also makes it extremely difficult to determine whether or not one has been subjected to illegal surveillance or unwarranted data collection, or to establish what, if any, remedies are available. Given this, in practice the right to an effective remedy under

Article 13 of the European Convention may not be available to the individual. Although the enactment of the DPA and the HRA, along with the establishment of the Office of the Information Commissioner (ICO), has led to a considerable improvement in this situation, the current system of regulation remains complex and opaque. Pounder (2008, p. 11) observes that, while government services may be becoming more joined up, protection is provided by a disjointed plethora of regulators in the field of personal data and surveillance, established under myriad statutory auspices. The effectiveness of the principles of openness and accountability is thus diminished, and the other main principles are very difficult to enforce even if resources were greater than they have been.

A further problem arises from the fact that although the activities of the police and other public bodies are regulated, the surveillance activities of private individuals and organisations are less well controlled. It can be inferred that the state has a positive obligation to take steps, such as putting in place a legal framework of regulatory safeguards, to protect individuals' ECHR rights against interference by others, because the activities of private organisations or persons, and not only public bodies, can endanger human rights. Although Article 8 of the ECHR provides the basis – alongside the existing tort of breach of confidence – for restricting private surveillance and protecting individual privacy, the law remains relatively underdeveloped in this area. In particular, the application of the law in relation to workplace surveillance is unclear, as is that of the law in relation to various forms of computer-based surveillance such as spyware. In order to protect privacy rights properly, the private and public sectors should have equally effective – and strong – regulations that are consistent with one another.

These reasons point to the need to reinforce an omnibus approach incorporating principles that overarch disparate rules embedded in the laws of various sectors if we are to prevent further fragmentation and confusion. We also need to consider ways of improving the architecture of existing provision for privacy protection and ensuring the consistency of further regulatory developments. Many futures for privacy protection can be envisaged, but it is useful to focus discussion upon a few approaches that represent prominent possibilities that can be seen either as alternatives or as components to be drawn upon in fashioning an improved regime. The first emphasises a single privacy statute; the second, an enhanced privacy right; the third argues for more regulatory coherence; and the fourth considers the case for an enhanced role for common law. These approaches are presented and assessed below.

6.3 Approach Two: enhanced protection via legislative reform

In light of these and other problems associated with the current system of regulation, there is an urgent need for legislative reform. This is an approach that has already been identified and recommended by others (see House of Lords (2009) for a detailed discussion). At the very least, legislative reform could simplify, consolidate and reform the DPA and RIPA.

Information privacy is protected by a wide range of laws and regulations in the UK, but the current regime suffers from a number of significant weaknesses as shown in previous chapters. The law has tended to develop in an irregular and largely sporadic fashion, and there are substantial gaps in the information privacy protections offered to individual citizens. This is due to the fact that legal reform in this area is typically reactive in character, with the law responding to rapid and often unexpected changes in both the technological and political landscape of privacy, surveillance, and data sharing.

Laws have developed through a combination of case law, legislation, and informal attempts at self-regulation. The absence of clearly defined, overarching principles means that each piece of legislation, line of judicial precedent, or code of practice has to be understood and interpreted within its own specific context. This can make the task of determining what rules apply to any given form of surveillance or data collection complex and time-consuming, and increases the likelihood that individuals will have their privacy infringed or their personal data misused.

Consolidation and reform of legislation that deals with all aspects of individual privacy, data protection, and surveillance in the public and private sectors, could more effectively protect the right to privacy enshrined in human rights legislation and ensure that each previously separate area of privacy law is organised around a clear definition of privacy and a coherent set of rationales for its protection.
It could help to ensure that all areas of society – the public, government, and the private sector – have a clear understanding of the demands of privacy and the limits of surveillance and personal data collection. In addition, reform could provide an opportunity for lawmakers to develop a definition of privacy that is not only clear and comprehensible, but which also provides the basis for a consistent set of principles that can be applied across sectors and different types of data collection, processing, and sharing.

A second reason for consolidating the existing law is that it makes the task of updating the law more straightforward. Privacy is an area that is deeply affected by changes in technology and in practical application. One of the major reasons why UK privacy law has become so fragmented is that in the past different parts of the

regulatory system have responded with varying degrees of speed to the challenges of technological change, or in some case have not responded at all. Consolidation could not only make the process of reform and updating the law more straightforward, but could also help to ensure that the definition of privacy and the principles that govern legal application remain coherent and comprehensible.[62]

Thirdly, consolidation could aid effective enforcement. Although it might be too much to expect any single regulator to take responsibility for the protection of privacy across all sectors of society, consolidated legislation that provides the legislative authority for a range of regulators – similar to the current UK situation – could not only help to minimise overlaps and gaps as regards their respective powers, but also help to ensure that those regulators worked together and in concert with one another. In addition, it could provide a clear gateway for individual complaints about possible violations of privacy, complaints that could then be referred to the appropriate Commissioner or office according to a clear division of statutory responsibilities.

Although the main focus of this report is on information privacy, it has also considered surveillance as it affects other dimensions of privacy, such as privacy of communications and behaviour in public spaces. How far the regulation of a wider range of surveillance activities should be dealt with under a reform of legislation is a matter for further consideration, and beyond the scope of this report. Having said this, it seems reasonable to assume that such reforms could address the invasion of privacy that occurs as a result of the exercise of ‘stop and search’ powers under Section 44 of the Terrorism Act, and provide a range of protections against intrusive, covert surveillance by the state. In particular, the reforms could incorporate many of the protections that are currently contained in RIPA, and provide greater clarity on how the requirements of necessity and proportionality are to be understood in the context of surveillance by the police and other state authorities.

Reform of the law might additionally give force to the role of technology in the protection of privacy, as discussed in Chapter 5. PETs and PbD are, by now, well-understood ways of protecting privacy through non-legislative means, but they are more talked about than implemented. On the other hand, PETs could be mandated by statute, or required as a consequence of the promulgation of a new general or sectoral legislation. So, too, could PIA as a related administrative and technical discipline, as in the USA.

While many of the above advantages can be obtained through consolidation of current legislation, and targeted reform, there are issues that may go beyond simple consolidation of current legislation and may require wider reform. These merit

consideration, but would require further discussion and thought before concrete proposals could be made.

As this report has shown, individual privacy is constantly under threat from a variety of quarters, as the personal data-gathering and processing capabilities of the public and private sectors continue to expand at an ever-increasing rate. Wider reform could mark a major shift in the law's focus on privacy, and represent a serious commitment on the part of the government to respecting individual privacy and the interests all of us have in our personal data. It could provide individuals with greater protection from what has been described as the emerging surveillance society, and articulate with the overarching principles. Reform could have the potential to transform the way in which we think about the place of privacy in our legal system, and the limits of public and private sector surveillance and data collection.
It could be helpful if wider reform were to set out a series of privacy principles, perhaps along the lines of those suggested by the ALRC, and augmented in keeping with current thinking. In addition it could provide an opportunity for lawmakers to consider whether wider reform should include such things as:

- a subsidiary right to 'informational self-determination' (similar to that which currently exists in Germany), related closely to existing norms about consent to data collection and further processing, which would give individuals the right to decide what information about themselves should be communicated to others and under what circumstances

- a subsidiary right to privacy in public spaces, that could provide the basis for the regulation of technologies such as public-space CCTV, and

- an explicit recognition of the data protection principles currently contained in the DPA, such that those principles as well as others indicated in Approach One would be directly enforceable by the courts, as well as via a regulator (who is independent and accessible without cost to complainants).

Given the limitations of the current right to privacy contained in the HRA – which can only be asserted against the public bodies and those undertaking public functions – it is essential that any reform also apply to the activities of private individuals and organisations. Aside from the fact that such a change would address one of the most glaring weaknesses in the current approach to privacy in the UK, it would also help to ensure that the right is one that can be easily understood by the general public, and would clarify the state's positive obligations to protect the rights contained in Article 8. Finally, given some of the issues outlined above in relation to obtaining relief for a breach of privacy – whether through the courts, tribunals or regulators – wider reform

would enhance access to an effective remedy in accordance with Article 13 of the ECHR.

It must be acknowledged that protection of privacy confronts limits set by certain other well-established rights that are also embedded in human rights legislation. The most important of these is the right to freedom of expression under Article 10 of the ECHR and Schedule 1, Article 10 of the HRA, giving rise to potential exemptions for the media. However, the remit of this report precluded the question of the media's inclusion or exemption from legal restrictions with respect to privacy. Whether, and how, any wider reform, or an improved protection of privacy rights, would have to include the media is an important matter for further consideration. This issue is extremely difficult both on political grounds, and also in view of experiences of previous unsuccessful attempts in other jurisdictions to bring the media under the control of any privacy law that was perceived to threaten the foundational right to freedom of expression, and the importance of freedom of the media in a democratic political system.[63]

Nevertheless, recent UK legal experience is that 'celebrities' claims of journalistic and photographic invasion of their privacy has given rise to prominent cases that have served to shape jurisprudence in this area. Consideration of changing the regulatory system of the media from self-regulation to bringing the media under a wider reform or within the scope of other legislated rights could too easily be seen as special protection for the wealthy and famous. On the other hand, such privacy legislation would then be available for all to use, not just the wealthy or privileged.

A further consideration with regard to privacy reform has to do with the social and political value of privacy, rather than its value solely to individuals, as discussed in Chapter 3. Legal recognition of the non-individual importance of privacy would constitute an advance over the current position. This would be especially so if it addressed the question of discrimination against social groups and categories found in certain information practices and surveillance activities and strengthened the ability to exercise other rights (for example, free speech and assembly) without subjection to the 'chilling effect' of surveillance. This protection is likely to be better provided through explicit grounding in privacy principles and law than through the existing dispersed array of legal provisions that do not refer to privacy invasion as an element in the treatment of individuals or groups.

Bringing about the sort of fundamental shift in our thinking about privacy, or necessarily ensuring that individuals and organisations will suddenly begin to take privacy seriously is more likely to be achieved by reform of the existing legislation, the introduction of a well-coordinated series of legal and extra-legal measures, a

continued focus on new and emerging threats to privacy from both the public and private sectors, and further consideration of what wider reforms are required.

6.4 Approach Three: improving the current regulatory regime

Central to this approach is the idea that sector-specific privacy laws are likely to be more effective if they are part of an overarching regulatory structure grounded in law and based on a clear and coherent set of principles and enforcement mechanisms. Approach Three is primarily concerned with the regulatory environment and specific privacy laws. However, it is compatible with other approaches insofar as it represents an overarching reform that aims to enhance other more 'localised' ways of promoting and protecting the right to privacy. Returning to Chapter 5, it is based on the idea of integrating laws and other means of safeguarding privacy with a view to creating a more coherent approach that will foster a symbiotic relationship between 'hard' and 'soft' law. Such an approach addresses the shortcomings in the current legislative and regulatory regimes, and would build upon the many past initiatives through legal reform, the imposition of strong codes of practice and guidance, and the promotion of technical and organisational change.

Some new legislation might also be desirable.[64] For example, there is a clear need for existing government databases containing personal information to be placed on a statutory footing, as this would help to define their purpose, specify their limits, and provide for effective oversight and remedies. However, care must be taken to ensure that any new legislation is based on and consistent with existing laws, such as the DPA and RIPA. At the same time, if there is little support for consolidating laws into a single statute, then various shortcomings with the existing approach to regulation will also need to be addressed. If the DPA and RIPA are to remain – and provide the basis for future reforms – they must be amended to ensure that they provide better protection for Article 8 rights. A comprehensive review of RIPA and other surveillance laws would help to ensure that there is a fair, coherent, accountable and accessible regime for the regulation of all forms of surveillance.

Regulatory and enforcement initiatives enable a variety of instruments to do the work that law by itself, and legal-compliance requirements, cannot achieve. The benefits of encouraging and rewarding good practice alongside those of sanctioning non-compliance should be more fully built into both managerial accountability practice and the training of staff at all levels where the handling of personal data is concerned. Designing privacy and other values into information systems should be encouraged by governments and by information industries, and made an integral part of infrastructure procurement processes.

In the wider society, working to involve NGOs in both raising public awareness of threats to privacy and in the development of policy-making could substantially help to further the goal of greater regulatory coherence and effectiveness. It would utilise the experience and knowledge of outside bodies that often have a better grasp of issues, problems and solutions. Greater emphasis should be placed on increasing public understanding and scepticism about what happens to their data, so that pressures can be brought to bear to improve legal compliance, everyday information practices, and transparency. More attention should be paid by regulators, NGOs, and data-using organisations themselves to assisting with subject access requests under data protection law, the value of which is often underestimated as a mechanism for redress as well as a litmus test of the privacy-protective performance of those who use personal data.

In addition, the existing system of statutory Commissioners needs to be rationalised. Although there are good reasons to take a specialised approach to regulation, unfortunately the current system of privacy protections is marred by a confusing fragmentation of responsibility and serious disparities in the amount of oversight and enforcement provided in different sectors. Whether there should be a single regulatory body – a Privacy Commission – that combines the roles of the currently separate Information, Surveillance and Interception Commissioners, or the continuation of a plural but more tightly coordinated arrangement amongst them, is a question about which opinions differ on grounds of effectiveness, political pragmatism, and public perception.[65] We believe the alternatives should be canvassed and the relative value of competing administrative criteria weighed, leading towards a proposal for reform.

Under Approach Three, efforts would also be made to enhance the ability of regulators to anticipate changes in the personal-data activities of the private and public sectors, rather than leaving them simply to react to ongoing developments. By enhancing the ability of regulatory agencies like the ICO to apply research on new technologies and investigate emerging trends in surveillance and data collection – either through increased in-house staffing or the greater use of external advisors – the law is less likely to find itself in the position of having to play catch-up or respond to dangerous gaps in the protection of privacy. Once again, NGOs could play a useful advisory role in this process, as could academic researchers.

6.5 Approach Four: an increased role for the common law

Any attempt to reform the legislative framework may also have implications for existing common law privacy protections. As has already been noted in Section 4, the tort of breach of confidence has a long history, and has recently evolved into a powerful tool for the protection of individual privacy in the UK. Originally used to

protect trade secrets and prevent employees from disclosing sensitive commercial information to a company's rivals, the tort has now expanded to include situations involving the unauthorised disclosure of personal information. Of particular note are recent developments that have enabled individuals to bring actions for breach of confidence, even in the absence of any pre-existing commercial or other relationship between the parties.

On the face of it, it appears that current developments in the law of breach of confidence are being driven by a desire on the part of the courts to provide more protection for privacy interests without going so far as to establish a new tort of privacy. Although it is tempting to welcome any expansion in the law of privacy, this approach to reform is severely limited in a number of key ways. First and foremost, because the courts are unlikely to recognise a general tort of privacy in the absence of specific legislation, common law privacy protections are likely to continue to develop in an incremental fashion and exacerbate many of the problems identified in this report. Given that the law of privacy in the UK is already highly fragmented, there is a danger that even well intentioned judicial activism in the area of privacy will only make matters worse. In addition, there is also a risk that judicial activism may lead to further disparities between the level of privacy protection enjoyed by citizens in different parts of the UK, as decisions of the English courts do not bind their counterparts in Scotland or Northern Ireland. Finally, because going to court is typically expensive and time consuming, it can be argued that common law privacy protections are only likely to be used by the wealthy, and widen the distinction between privacy haves and have-nots.

It is for these reasons that this report, while not wishing to underplay the importance of the courts and the role of the judiciary in the development of privacy law in the UK, does not view common law as an appropriate vehicle for the sort of fundamental reform that is currently needed. Even if there was an appetite for the creation of a free-standing tort of privacy, it is not clear how such a tort would operate in conjunction with existing regulatory structures, or how it would bring coherence to the law of privacy more generally. As such, the authors of this report believe that common law reform should only be pursued as a very limited strategy.

6.6 Choosing a new path for privacy

Not all threats to information privacy are of the same severity or likelihood, and there are differences between the sources of the threats as well, in terms of the forms of surveillance and information processing they represent. Not all domains of life – whether shopping, transacting with the state, engaging in financial relationships, walking in public streets, or maintaining our health – generate the same patterns of risk or affect all individuals or social groups to the same extent. Therefore, it need not

be the case that ‘one size fits all’ with regard to the approaches to be put into effect towards better privacy protection. However, it seems necessary to articulate a common set of principles underlying them – as we have shown – and to ensure that an array of privacy-protecting laws and instruments does not amount simply to an ad hoc assembly of parts that are confusing to the public and cumbersome in practice.

Any ‘new path’ based on the approaches outlined in this section must be anchored in human rights, and in particular the fundamental right to privacy and an appreciation of its importance to the kind of society in which we wish to live. It must also adhere to certain procedural requirements or principles as well. Among these, the scrutiny, transparency and accountability of the processes giving rise to the need for privacy protection are especially important. Of similar importance is the accessibility to the individual, or to those who act on behalf of individuals – perhaps aggregating their individual interests into collective ones – of the legal and other remedies or the preventative measures that together constitute the path. Some approaches meet these fundamental and procedural requirements better than others, but all must be evaluated in terms of how well they are likely to perform as a new path. But it is one thing to discern a path; it is another to assess how, at what pace, and who should traverse it.

‘Choosing a new path’ implies a selection process, involving organisations that design the means for processing personal data; public bodies that engage in personal data processing and other forms of surveillance; organisations that represent individuals’ interests; and individual actors themselves. All these actors should participate in evaluating the approaches and designing the path. In the UK, this points towards those involved in the political and legal systems: government and parliament, regulatory, law-enforcement, and other agencies, pressure groups and NGOs, the media, and the general public. It also presupposes the contribution that other interests make: businesses of all kinds, and technological industries. What the process should look like, ensuring the involvement of disparate actors, is crucial to a successful outcome – the path that is chosen. This question will be considered in Chapter 7.

7. Proposals for reform

7.1 Introduction

Throughout this report, we have considered many different ways of thinking about information privacy and how it should be promoted and protected. Chapters One and Two examined the threats posed to information privacy by advances in technology, as well as some of the dangers associated with greater levels of state surveillance, data collection, and information sharing. Chapter 3 explained why information privacy matters, and looked at a number of different justifications of privacy with a view to clarifying the value of privacy and why it deserves to be protected. In addition, that Chapter considered the relationship between privacy and state interests, both now and in future. Chapters Four and Five surveyed the landscape of domestic and international privacy law, and considered other means by which information privacy may be protected within a framework of human rights and with respect to general privacy principles. Finally, the previous Chapter outlined several approaches to privacy reform that aim to build on principles, existing privacy rights, and legal frameworks, while also promoting greater regulatory coherence and increased co-ordination amongst those responsible for protecting information privacy. These approaches are also intended to provide a structure for thinking about how different types of reform might be pursued simultaneously, and to help policymakers identify exactly what is at stake when considering the potential costs and benefits of any new information technology or state surveillance practice.

In this Chapter, we set out a number of recommendations that could provide the basis for a fundamental reform of the way in which information privacy is understood and protected in the UK. Although it is tempting to compile a long list of sector-specific reforms and legislative amendments, we believe that such a list would be both premature and of limited use. As has been noted throughout, the protection of information privacy has often been hampered by piecemeal efforts at reform and the lack of a clear rationale. In addition, given that the HRA has established a system of rights protections in the UK, it is important to ensure that any privacy reform enhances the existing Article 8 jurisprudence.

With this in mind, this Chapter makes a number of broad recommendations that are intended to provide the starting point for a more extensive and detailed programme of privacy reform. It aims to help clear a new path for privacy, one that is sensitive to the broad range of interests concerned, and yet firmly rooted in a commitment to fundamental human rights and an awareness of the relationship between the individual and the state.

7.2 Recommendations

Recommendation One: the need for privacy principles

In the view of the authors of this report, the single greatest stumbling block to the effective regulation of information privacy in the UK is the lack of a coherent legal framework for the protection and promotion of individual privacy. As a result, this report strongly recommends that any proposed programme of reform must be guided by a clear set of uniform principles, and an overarching commitment to fundamental human rights. New privacy protections must not only be compliant with the demands of the HRA, but also strengthen the right to respect for private and family life enshrined in Article 8 of the ECHR.

If information privacy protection is to benefit from new thinking, it is important to ground change in a (re)statement of overarching principles, as has been shown in Chapter 6. These principles should be at a high level but avoid unnecessary abstraction, keeping in mind that they must be implemented through specific practices and rules, and that regulation based on principles does not necessarily avoid problems of trust, enforcement, interpretation, and other kinds. We have outlined the conventional data protection principles as a starting point, and at present a considerable body of legislation and practice is based upon these principles. It is important to note, however, that these principles and practices have limitations when applied to new forms of surveillance that may affect information privacy, but do not necessarily involve the computerised storage of information or the processing of identifiable personal data. New strategies must continually be developed to cope with the increasingly novel ways in which privacy, including information privacy, is at risk. Extending the existing inventory of principles will help to cover new situations and clarify responsibilities in the relationship between individuals and the state. In particular, it is important to revisit the principle of consent and possibly reconsider its position as a foundational principle. As it stands, its status in theory is uncertain, and its realisation in practice is often treated as either impossible or optional.

We therefore recommend that the principles for information privacy protection be restated clearly, with a view to reaffirming the existing data protection principles within an Article 8 human rights framework, and also emphasising the importance of lawfulness, accountability, transparency and effective remedy. The principle of consent should be reformulated, having particular regard to the situations in which it would be valuable, and to the ways it could be implemented. The principles would benefit from discussion and debate by a short-term forum drawn largely from the world of law and academia. This forum would aim to restate and develop a body of principles that could realistically be applied to the varied contexts in which privacy is likely to be at stake in the UK in future. It would also examine ways in which the difficulties and paradoxes of ‘principles-based regulation’ can be handled.

Recommendation Two: strengthening the right to privacy through legislative reform

It is important to reinforce the existing right to privacy. The government should consider reforming existing legislation that touches on matters of privacy in order to ensure that it is consistent with the privacy principles recommended earlier, and that it enhances – rather than undermines – the existing provisions of the HRA. At minimum, such reform should consolidate and improve the existing RIPA and data protection regimes in relation to information privacy and surveillance, and will need to take into account, and incorporate any legislative changes required as a result of the proposed new EU data protection legislative regime. In addition, courts should be given additional powers – via appropriate statutory amendments – to directly enforce existing data protection regulations and other privacy principles.

It would be desirable if an appropriate legal body or commission undertook an investigation of how existing privacy rights could be reinforced, especially through the revision, simplification, and further development of statutory law. This investigation should engage a wide range of interests and draw on the expertise of specialists in the fields of law, technology, and social science.

Recommendation Three: promoting greater regulatory coherence

Any system of regulation must be based on law. As discussed earlier in this report, there are significant gaps in the current legal regime, and in particular in the system of protection established by RIPA and DPA. We recommend that a comprehensive review of the DPA, RIPA, and other surveillance laws should be undertaken to ensure that the regulatory regime governing state surveillance is fair, coherent, accountable, and accessible. In addition, all government databases that hold personal information should be placed on a statutory footing, with specific provisions regulating their remit, oversight and the provision of individual remedies.

The fragmented and un-coordinated system of regulatory Commissioners has been commented upon earlier in this report. At present, there is a clear need for reforms that will bring about greater coherence and clarity to the existing system of regulation around information privacy. This could be achieved in one of three ways: through a reallocation of powers amongst the existing agencies, by bringing them into one system, or through closer co-ordination between Commissioners. Implementation of privacy laws would also be facilitated if a more anticipatory and proactive approach to regulation, based on knowledge and understanding of trends in technology and surveillance, were encouraged in place of a largely reactive set of practices.

We therefore recommend that greater regulatory coherence should be a key priority for any future agenda of privacy reform. As a first step we recommend that a group of

experts drawn from the public sector, parliament, NGOs and academia be convened to consider the alternative ways of improving coherence. The aim of this group would be to develop the terms of the enquiry, and develop alternative regulatory models that could then be examined in detail by parliament. Ultimately, we would hope that this process would produce a series of legislative amendments and ministerial orders that could rationalise the existing system of regulators, and thereby improve the level of protection currently afforded to information privacy.

Recommendation Four: improved technological and organisational means of protection

The need for better integration between legal and non-legal means of protecting information privacy was emphasised earlier. Achieving this goal depends on developing ways of encouraging the design and use of privacy-protective technologies, assessing the impact of new information systems on privacy, encouraging stronger accountability practices in organisations, and involving NGOs in the protection and promotion of privacy. Although such measures have been widely discussed in recent years, there is a clear need for a more structured approach to the development of technological and other non-legal privacy protections if information privacy is to be safeguarded against future threats.

We therefore recommend that the government take steps to encourage the development and use of technological and other non-legal solutions to the problem of information privacy, and that where appropriate, the use of such measures should be required by law. In addition, we recommend that greater effort be made to help NGOs and the private sector develop and implement creative approaches to the protection of privacy, and that the government consider funding public education programmes aimed at making individuals more aware of the threats to privacy and the practical ways in which they can protect their own personal information.

We also recommend that information technology developers be encouraged to incorporate privacy protections into their product designs, and that the government should make the inclusion of such protections a contractual requirement when dealing with private sector contractors. In addition, the education and training of information technology professionals should be reformed to ensure that the designers and manufacturers of potentially privacy-intrusive products have an understanding of privacy and data protection principles and their relation to human rights. This reform is a matter that the relevant technology professional associations, educators, and the Information Commissioner should be encouraged to undertake in concert.

Technological solutions, however, require appropriate organisational and ‘cultural’ safeguards to be put in place. Although it is clear that central government has begun

to learn some of the lessons arising out of the data losses suffered by HMRC and other departments in recent years, these reforms need to be more widespread. As a result, we recommend that the government establish a central taskforce responsible for ensuring that improvements in information handling are properly publicised throughout government, with a view to establishing a consistent set of best practices across departments and state agencies.

8. Conclusion

Information privacy plays an essential role in our society. As this report has shown, the right to information privacy is currently under threat in the UK, and is likely to be faced with further challenges if central and local government continue to expand the surveillance apparatus of the state. While some forms of surveillance are clearly beneficial to both individuals and society at large, it is vital to ensure that information privacy is properly protected through the effective regulation of government surveillance, including data gathering, processing, and sharing.

In an effort to build on recent government, NGO, and private sector initiatives, this report has considered how the right to information privacy could be strengthened through various legal and non-legal reforms. In addition to emphasising the need for a comprehensive review of existing privacy laws and the regulation of surveillance, the report has also acknowledged the importance of ensuring that any programme of reform is consistent with the existing constitutional settlement between the different jurisdictions of the UK. Finally, the report has shown that there are important international dimensions of privacy that must be taken into account when thinking about the future of privacy protection in the UK.

At the heart of the report is a commitment to the idea that information privacy is a fundamental right, and that the legal framework that seeks to protect it must be capable of responding to new technologies and changes in the ways in which we understand and communicate personal information. If we are to develop privacy laws that will stand the test of time, we must begin to think carefully about why privacy matters and acknowledge the need for a coherent, comprehensive, and robust approach to its protection. As this report has shown, the right to privacy is at risk of being eroded by the growing demand for information by government and the private sector. Unless we start to reform the law and build a regulatory system capable of protecting information privacy, we may soon find that it is a thing of the past.

References

Article 29 Working Party (2009) *The Future of Privacy*. Brussels: Article 29 Data Protection Working Party, Working Party on Police and Justice, WP 168.

Australian Law Reform Commission (ALRC) (2008) *For Your Information – Australian Privacy Law and Practice.* Vol. 1, Report 108. Canberra: Australian Government, Australian Law Reform Commission.

Bellamy, C., 6, P., Raab, C., Warren, A. and Heeney, C. (2008) Information-sharing and confidentiality in social policy: regulating multi-agency working. In *Public Administration*. Vol. 86, No. 3.

Bennett, C. (2008) *The Privacy Advocates: Resisting the Spread of Surveillance.* Cambridge, MA: The MIT Press.

Bennett, C. and Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, MA: The MIT Press.

Bennett, C. (2010) International privacy standards: can accountability be adequate? In *Privacy Laws & Business International Newsletter*, Issue 106, August, pp. 21-3.

Big Brother Watch (2010) The Grim Ripa: Local councils authorising 11 covert surveillance operations a day. 23 May 2010. Available from: http://www.bigbrotherwatch.org.uk/home/2010/05/the-grim-ripa-local-councils-authorising-11-covert-surveillance-operations-a-day.html. [Accessed 19 December 2010].

Black, G. (2011 forthcoming) *Publicity Rights and Image: Exploitation and Legal Control*. Oxford: Hart Publishing.

Black, J. (2008) Forms and paradoxes of principles based regulation. LSE Law, Society and Economy Working Papers 13/2008. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1267722&. [Accessed 15 November 2010].

Bloustein, E. (1964) Privacy as an aspect of human dignity: an answer to Dean Prosser. In *Philosophical Dimensions of Privacy: An Anthology*. Schoeman, F. (ed.) pp. 156-202. Cambridge: Cambridge University Press.

Burkert, H. (1997) Privacy-enhancing technologies: typology, critique, vision. In *Technology and Privacy: The New Landscape*. Agre, P and Rotenberg, M., (eds.) pp. 125-42. Cambridge, MA: The MIT Press.

Cabinet Office (2008) *Data Handling Procedures in Government: Final Report*. Available from: www.cesg.gov.uk/products_services/.../data_handling_review.pdf [Accessed 25 January 2011].

Cavoukian, A. (2009) *Privacy by Design*. Toronto: Information and Privacy Commissioner of Ontario, Canada.

Chief Surveillance Commissioner (2008) *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2007-2008.* HC 659, July. London: The Stationery Office.

Council of Europe (1981) *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)*. Strasbourg: Council of Europe.

Council of Europe (2010) *Fourth Data Protection Day – 28 January 2010*. Available from: http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/Default_DP_Day_en.asp#TopOfPage [Accessed 17 October 2010].

Crossman, G. (2007) *Overlooked: Surveillance and Personal Privacy in Modern Britain*. London: Liberty.

DCA. (2003) Public Sector Data Sharing: Guidance on the Law. November 2003. Available from: http://www.justice.gov.uk/guidance/docs/data_sharing_legal_guidance.pdf[Accessed 19 December 2010].

DeCew, J. (2006) Privacy. In *Stanford Encyclopedia of Philosophy*. Available from: http://plato.stanford.edu/entries/privacy/#PriHumDig [Accessed 17 October 2010]).

EDPS (2010) Opinion of the European Data Protection Supervisor on promoting trust in the information society by fostering data protection and privacy. Available from: http://www.edps.europa.eu [Accessed 17 October 2010].

Equality and Human Rights Commission (EHRC) (2009) *The Equality and Human Rights Commission's response to the government's consultation on: Keeping the right people on the DNA database.* August 2009. London: EHRC.

Eurobarometer (2008) *Data Protection in the European Union: Citizens' Perceptions – Analytical Report.* Flash Eurobarometer 225 – The Gallup Organisation. Brussels: European Commission.

European Commission (2009) *Evaluation of the Means used by National Data Protection Supervisory Authorities in the promotion of personal Data Protection – Final Report.* Brussels: European Commission, Directorate-General Justice, Freedom and Security. Available from: http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_kantor_management_consultants.pdf [Accessed 17 October 2010].

European Commission for Democracy Through Law (Venice Commission) (2007) Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights. Study No. 404 / 2006 CDL-AD(2007)014. Strasbourg, 23 March 2007. Available from: http://www.venice.coe.int/docs/2007/CDL-AD(2007)014-e.pdf [Accessed 19 December 2010].

European Union (1995) *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. OJ no. L281. Brussels: European Union.

Feldman, D. (1994) Secrecy, dignity, or autonomy? Views of privacy as a civil liberty. In *Current Legal Problems*. Vol. 47, No. 2.

Feldman, D. (2002) *Civil Liberties and Human Rights in England and Wales*, 2nd edn. Oxford: Oxford University Press.

Ford, R. (2004) Beware rise of Big Brother state, warns data watchdog. In *The Times*, 16 August.

Gavison, R. (1980) Privacy and the limits of law. In *Philosophical Dimensions of Privacy: An Anthology*. Schoeman, F. (ed.) pp. 346-402. Cambridge: Cambridge University Press.

Gellman, R. (1993) Fragmented, incomplete and discontinuous: the failure of federal privacy regulatory proposals and institutions. In *Software Law Journal.* Vol. 6.

Gillespie, A. (2009) Regulation of Internet Surveillance. In *European Human Rights Law Review*. Issue 4, pp. 552-65.

Goold, B. (2002) Privacy Rights and Public Spaces: CCTV and the Problem of the 'Unobservable Observer'. In *Criminal Justice Ethics.* Vol. 21, No. 1 Winter/Spring.

Goold, B. (2006) Open to All? Regulating Open Street CCTV and the Case for 'Symmetrical Surveillance'. In *Criminal Justice Ethics.* Vol. 25, No. 1 Winter/Spring.

Goold, B. (2007) Privacy, identity and security. In *Security and Human Rights*, Goold, B. and Lazarus, L. (eds.) Oxford: Hart Publishing.

Goold, B. (2009) Surveillance and the political value of privacy. In *Amsterdam Law Forum*. Vol. 1, No. 4.

Goold, B., Lazarus, L and Swiney, G. (2007) Public protection, proportionality and the search for balance. London: Ministry of Justice, Research Series 10/07.

Gross, H. (1967) The concept of privacy. In *New York University Law Review*. Vol. 42.

Harfield, C. and Harfield, K. (2005) *Covert Investigation*. Oxford University Press: Oxford.

Home Office (1978) *Report of the Committee on Data Protection*, Chairman: Sir Norman Lindop, Cmnd.7341. London: Her Majesty's Stationery Office.

House of Commons (2008a) *A Surveillance Society?* Select Committee on Home Affairs, 5th Report of Session 2008-09, HC 58. London: The Stationery Office.

House of Commons (2008b) *Protection of Private Data*, Select Committee on Justice, 1st Report of Session 2007-08, HC 154. London: The Stationery Office.

House of Lords and House of Commons (2008) *Data Protection and Human Rights*. Joint Committee on Human Rights, 14th Report of Session 2007-08, HL Paper 72, HC 132. London: The Stationery Office.

House of Lords (2009) *Surveillance: Citizens and the State.* Select Committee on the Constitution, 2nd Report of Session 2008-09, HL Paper 18-I. London: The Stationery Office.

Hunton & Williams LLP (2009) *Data Protection Accountability: The Essential Elements – A Document for Discussion*. Centre for Information Policy Leadership October 2009, pp. 2-3.

ICO (2008) *Privacy by Design.* Wilmslow: Information Commissioner's Office.

ICO (2009) *Privacy Impact Assessment Handbook Version 2.0*. Wilmslow: Information Commissioner's Office. Available from: http://www.ico.gov.uk. [Accessed 17 October 2010].

ICO (2010a) *The Privacy Dividend: The Business Case for Investing in Proactive Privacy Protection*. Wilmslow: Information Commissioner's Office. [Accessed 17 October 2010].

ICO (2010b) *Information Commissioner's Annual Report Summary 2009/10.* Wilmslow: Information Commissioner's Office.

ICO (2010c) Data breaches to incur up to £500,000 penalty. Press Release, 12 January 2010. Available from: http://www.ico.gov.uk/~/media/documents/pressreleases/2010/penalties_guidance_120110.ashx [Accessed 19 December 2010].

ICO (2010d) First monetary penalties served for serious data protection breaches. Press Release, 24 November 2010. Available from: http://www.ico.gov.uk/~/media/documents/pressreleases/2010/first_monetary_penalties_press_release_24112010.ashx [Accessed 19 December 2010].

Interception of Communications Commissioner (2010) *Report of the Interception of Communications Commissioner for 2009.* HC 341, July 10. London: The Stationery Office.

Lessig, L. (1999) *Code and Other Laws of Cyberspace*. New York, NY: Basic Books.

Liberty (2007) *Overlooked: Surveillance and personal privacy in modern Britain*, London: Liberty.

Liberty (2010) *From 'War' to Law – Liberty's Response to the Coalition Government's Review of Counter-Terrorism and Security Powers 2010.* London: Liberty.

Lindsay, D. (2005) An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law. In *Melbourne University Law Review*. Vol. 29.

MacQueen, H. (2009) A Hitchhiker's Guide to Personality Rights in Scots Law, Mainly with Regard to Privacy. In *Rights of Personality in Scots Law: A Comparative Perspective*. Whitty, N. and Zimmermann, R., eds. Dundee: Dundee University Press.

Madrid Declaration (2009) *Global Privacy Standards for a Global World – The Madrid Privacy Declaration*, *3 November 2009*. Available from: http://thepublicvoice.org/madrid-declaration/ [Accessed 17 October 2010].

Madrid Resolution (2009) *International Standards on the Protection of Personal Data and Privacy – The Madrid Resolution*. Available from:

http://www.gov.im/lib/docs/odps//madridresolutionnov09.pdf [Accessed 17 October 2010].

Manson, N. and O'Neill, O. (2007) *Rethinking Informed Consent in Bioethics*. Cambridge: Cambridge University Press.

Marx, G. (2004) What's New About the 'New Surveillance'? Classifying for Change and Continuity. In *Knowledge, Technology & Policy*. Vol. 17, No. 1, pp. 18-37.

Ministry of Justice (2008) *Response to the Data Sharing Review Report.* Available from: http://www.justice.gov.uk/publications/response-data-sharing-review.htm[Accessed 25 January 2011].

Nissenbaum, H. (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

OECD (1981) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD.

OECD (2001) *Report on the OECD Forum Session on Privacy-Enhancing Technologies (PETs)***.** DSTI/ICCP/REG(2001)6/FINAL. OECD, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, Working Party on Information Security and Privacy. Paris: OECD.

OUT-LAW news (2010) EU Commission outlines plans to strengthen privacy law, 29/01/10. Available from: http://www.out-law.com/page-10712 [Accessed 17 October 2010].

Palen, L. and Dourish, P. (2003) Unpacking 'privacy' for a networked world. In *Conference on Human Factors in Computing Systems, Proceedings of the SIGCHI conference on human factors in computing systems*, pp. 129-136. Ft. Lauderdale, FL: ACM.

Posner, R. (1978) An economic theory of privacy. In *Regulation*, May/June.

Pounder, C. (2008) Nine principles for assessing whether privacy is protected in a surveillance society. In *IDIS*, Vol. 1.

Raab, C. (1999) From balancing to steering: new directions for data protection. In *Visions of Privacy: Policy Choices for the Digital Age*. Bennett, C. and Grant, R. (eds.) pp. 68-93. Toronto: University of Toronto Press.

Raab, C. (2003) Prospects for a trust charter in United Kingdom public services, International Symposium on Service Charters and Customer Satisfaction in Public Services, City University of Hong Kong, 8-9 December.

Rachels, J. (1975) Why privacy is important. In *Philosophical Dimensions of Privacy: An Anthology*. Schoeman, F. (ed.) pp. 290-99. Cambridge: Cambridge University Press.

Regan, P. (1995) *Legislating Privacy: Technology, Social Values, and Public Policy.* Chapel Hill, NC: University of North Carolina Press.

Reid, E. (2009) Protection of personality rights in the modern Scots law of delict. In *Rights of Personality in Scots Law: A Comparative Perspective*. Whitty, N. and Zimmermann, R. (eds.) Dundee: Dundee University Press.

Reidenberg, J. (1998) Lex Informatica: the formulation of information policy rules through technology. In *Texas Law Review*, Vol. 76.

Rössler, B. (2005) *The Value of Privacy*. Cambridge: Polity Press.

Rule, J. (2007) *Privacy in Peril: How we are Sacrificing a Fundamental Right in Exchange for Security and Convenience.* New York, NY: Oxford University Press.

Royal Academy of Engineering (2007) *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*. London: Royal Academy of Engineering.

Schoeman, F. (ed.) (1984) *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press.

Schoeman, F. (1992) *Privacy and Social Freedom*. Cambridge: Cambridge University Press.

SMSR (2010) *Report on the Findings of the Information Commissioner's Office Annual Track 2010 – Individuals*. Final Report, November 2010. Hull: Social and Market Strategic Research. Available from: http://www.dataprotection.gov.uk/~/media/documents/library/Corporate/Research_and_reports/annual_track_2010_individuals.ashx [Accessed 19 December 2010].

Solove, D. (2008) *Understanding Privacy.* Cambridge, MA: Harvard University Press.

Staley, K. (2005) *The Police National DNA Database: Balancing Crime Detection, Human Rights and Privacy – A Report to GeneWatch UK.* Manchester: GeneWatch UK.

Surveillance Studies Network (2006) *A Report on the Surveillance Society.* Wilmslow: Information Commissioner's Office. Available at: http://www.ico.gov.uk [Accessed 17 October 2010].

Thames Valley Police (2010) *Project Champion Review.* 30 September 2010.

Thomas, R. and Walport, M. (2008) *Data Sharing Review Report.* London.

Travis, A. (2010) Councils carry out over 8,500 covert surveillance operations. *The Guardian*, 24 May.

US Department of Commerce (1997) *Privacy and Self-Regulation in the Information Age*. Washington, DC: US Department of Commerce, National Telecommunications and Information Administration.

Warren, S. and Brandeis, L. (1890) The right to privacy. In *Philosophical Dimensions of Privacy: An Anthology*. Schoeman, F. (ed.) pp. 75-103. Cambridge: Cambridge University Press.

Westin, A. (1967) *Privacy and Freedom*. New York, NY: Atheneum.

Young. J. (ed.) (1979) *Privacy.* New York, NY: Wiley.

Endnotes

[1] HC Deb 20 Nov 2007 cols 1101–04.

[2] House of Lords (2009), para. 413.

[3] *R v W* [2003] EWCA 1632. Attorney General's reference (No. 5 of 2002) [2004] UKHL 40 at para. 9.

[4] *Wood v Commissioner for Police of the Metropolis* [2009] Court Appeal.

[5] EHRC (2009), p.5.

[6] *S. and Marper v The United Kingdom* (December 4, 2008) (Application nos. 30562/04 and 30566/04).

[7] *R v W* [2003] EWCA Crim 1632.

[8] See also Surveillance Studies Network (2006).

[9] The DPA is overseen for the UK by the ICO except for freedom of information functions, which are handled by the Scottish Information Commissioner under the Freedom of Information (Scotland) Act (FOISA) 2002. Different parts of RIPA are overseen by the Chief Surveillance Commissioner, the Interception of Communications Commissioner, and the Intelligence Services Commissioner. Until the present Government indicated its aim to abolish the Identity Cards Act 2006, there was an Identity Scheme Commissioner. Under RIPA, there is an Investigatory Powers Tribunal, and under the DPA there is an Information Tribunal.

[10] There is a large and inconclusive literature on this, canvassing many conceptions of privacy. Useful anthologies are Schoeman (1984) and Young (1979); and overviews can be found in Lindsay (2005) and DeCew (2006).

[11] Most notably in cases such as *Katz v United States* 389 U.S. 347 (1967) and *United States v Knotts* 460 U.S. 276, 276 (1983).

[12] The definition of ‘personal data’ has been keenly disputed, not least since the case of *Michael John Durant v Financial Services Authority* [2003] EWCA Civ 1746, Court of Appeal (Civil Division) decision of Lord Justices Auld, Mummery and Buxton dated 8 December 2003.

[13] For an account of the difference between proportionality and balancing, see Goold, Lazarus and Swiney (2007). Critical comments on ‘balancing’ are in Raab (1999).

[14] For the purpose of this report, common law countries are taken to include Australia, Barbados, Brunei, Canada, Hong Kong, India, Malaysia, New Zealand,

Northern Ireland, Pakistan, Republic of Ireland, Scotland, Singapore, South Africa, Sri Lanka, and the United States of America.

[15] An important definition of personal data can be found in Section 1 of the DPA, which states that personal data means data that relate to a living individual who can be identified (a) from those data, or (b) from those data and other information that is in the possession of, or is likely to come into the possession of, the data controller. For this purpose of the Act, personal data also 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.

[16] The Scottish versions of FOIA and RIPA are mentioned below. The Privacy and Electronic Communications (EC Directive) Regulations 2003 – which make it unlawful for direct marketers to transmit automated, recorded messages without the prior consent of individual telephone subscribers – are not included in this list as they are private sector regulations and beyond the scope of this report.

[17] It is important to note that the position is considerably different in Scotland. In addition to being governed by the DPA and HRA, information privacy in Scotland is also protected by FOISA and the Regulation of Investigatory Powers (Scotland) Act (RIPSA) 2002. Scotland also has its own branch of the Office of the Information Commissioner, which is headed by an Assistant Commissioner for Scotland. For a detailed review of the law of privacy in Scotland, see: Reid (2009) and MacQueen (2009).

[18] As noted by Glidewell L.J. in *Kaye v Robertson* [1991] FSR 62, 65: 'It is well known that in English law there is no right to privacy, and accordingly there is no right of action for breach of a person's privacy.' On this point, see also *W v Home Office* [2001] EWCA Civ 2081.

[19] *Peck v UK* (2003) 36 EHRR 41. It has also been held that 'Article 8… protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world.' See *PG* (2001) 46 EHRR 51 at page 56.

[20] *Von Hannover v Germany* (2005) 40 EHRR 1. See also *Peck v UK* (2003) 36 EHRR 41 and *Perry v UK* (2004) 39 EHRR 3. In *Segerstedt-Wiberg and Ors v Sweden* [2007] EHRR 2, the Court also found an interference with Article 8 where the Swedish Secret Police had collected and stored information on the applicants, consisting of newspaper articles, radio programmes, decisions of public authorities and notes of their public activities.

[21] In the s.44 'stop and search' case of *Gillan & Quinton v UK* [2009] ECHR 28, for example, the ECHR was strongly influenced by the fact that the breadth of the power in question had led to it being widely overused.

[22] As Gillian Black has observed in her forthcoming book on privacy (Black, 2011): 'There is no longer any doubt over the availability of the remedy in horizontal relationships, and this approach was underscored by Resolution 1165 of the Council

of Europe (passed against the background of the death of the Princess of Wales in a car crash following pursuit by reporters) which emphasised that Article 8 privacy rights should be enforceable against private persons, including the media.' See also para. 12 of the Resolution, and MacQueen (2009), para 12.2.1.

[23] This is a point that has been made by the privacy scholar Professor Bert-Jaap Koops. See House of Lords (2009), para. 128.

[24] See Goold *et al.* (2007).

[25] Although the ICO encourages individuals who are concerned about the ways in which their personal data is being used to make a formal complaint, the courts can also award compensation for damage arising out of a breach of the data protection principles set out in the DPA.

[26] It is important to note that these enforcement notices can be appealed, and that permission for the processing to continue may be granted until the appeal is heard.

[27] Note that ICO has no authority to prosecute criminal offences in Scotland, as this can only be done by the Crown Office and Procurator Fiscal Service.

[28] The new powers are contained in the Coroners and Justice Act 2009. The ICO may issue an assessment notice to a government department to assess compliance with the DPA and the data sharing Code of Practice. In addition, as of April 2010 the ICO can order organisations to pay a penalty of up to £500,000 for breaches of the DPA, and has recently produced statutory guidance on how it proposes to use this new power. See ICO (2010c). On 24 November, the ICO issued its first penalties, for £100,000 and £60,000, to Hertfordshire County Council (for twice faxing highly sensitive personal information to the wrong recipients; and to the company A4e for the loss of an unencrypted laptop which contained personal information relating to 24,000 people who had used community legal advice centres; see ICO(2010d).

[29] According to section 24 of the Republic of Ireland Data Protection Acts 1988 and 2003, the Irish Data Protection Commissioner can appoint an 'authorised officer' to enter and examine the premises of a data controller or data processor. In addition to being able to enter premises, the authorised officer also has the power to inspect and copy any information, and require the data controller, data processor or their staff to provide information about their procedures for complying with the Act, as well as sources of data, the purposes for which personal data is being kept, and information about the disclosure of data.

[30] Communication from the Commission to the European Parliament, the Council, The Economic and Social Committee and the Committee of the Regions, *A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, Brussels 4.11.2010. Available from: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf [Accessed 9 January 2011].

[31] *Charter of Fundamental Rights of the European Union*, 2000/C 364/01. Available from: http://www.europarl.europa.eu/charter/pdf/text_en.pdf [Accessed 9 January 2011]. The Charter was promulgated in 2000 and is now recognised by the EU's Lisbon Treaty. It applies to EU institutions and bodies, and applies to Member States when they are acting within the scope of EU law.

[32] The law does, however, provide for the interception of such communications in certain circumstances. The most straightforward of these is when both parties to the communication consent to its being intercepted, and in such cases the information obtained can be used as evidence (RIPA 2000, sections 3(1), 18(4) and 18(5)). When only one party—either the sender or the receiver—consents, however, authorization under Part II of RIPA 2000 is required. In practice, this form of authorisation is most likely used when one of the parties to the communication is an undercover police officer or the target of blackmail. According to sections 18(4) and 18(5) of the Act, information obtained from such communications is admissible as evidence.

[33] *R v E* [2004] EWCA Crim 1243, discussed in Harfield and Harfield, (2005), p. 126.

[34] *R v Aujia* [1998] 2 Cr App R 16. See also Harfield and Harfield (2005), p. 126.

[35] It is important to note that although it is clear, for example, that an employer is entitled to monitor email transmitted on their network when consent has been given or the communication relates to the employer's business, according to advice issued by the Office of the Information Commissioner in 2002, it may be illegal to intercept non-work related communications. This view is in line with the decision taken by the ECtHR in *Halford v United Kingdom* (1997) IRLR 471, where it was held that the tapping of a telephone on a private network without consent or prior warning constituted a breach of the right to privacy under Article 8 of the Convention. The situation is further complicated by the fact that although RIPA regulates access to the contents of a communication, it says nothing about the monitoring of traffic on a private network. As such, it is unclear whether an employer is legally able to monitor when private calls are made or to record the addresses of websites visited by employees. Although the ICO has suggested that operators of private networks should lay down clear guidelines for the use of their systems – and indicate when and what sort of monitoring is likely to take place – employers and other operators of private communications systems are not required by law to do so.

[36] Summarised definitions taken from Harfield and Harfield (2005), pp. 31 and 49.

[37] According to sections 28, 29, and 30 of RIPA, authority to carry out directed surveillance can only be granted by an authorising officer or some other person empowered under the statutory instruments that have since amended the Act. Examples of such authorising officers include police superintendents, certain customs officials, and local authority chief officers. As specified by section 28(2), before any authority is granted, the authorising officers must be satisfied that the surveillance in question is both proportionate to, and necessary for, one or more of the purposes set out in section 28(3), which include: the interests of national security; preventing or detecting crime or of preventing disorder; the economic wellbeing of the

United Kingdom; the interests of public safety; protecting public health; and assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department. Authorisations can last up to a period of three months. However, the authorising officer who granted or most recently renewed the authorisation is obliged to cancel it if the surveillance is either no longer necessary or no longer meets the criteria for its original authorisation. (RIPA Code of Practice paragraphs 4.28 and 4.2). In cases of intrusive surveillance, authorisation is also needed from a designated authorising officer, who must notify the Office of Surveillance Commissioners (OSC) in writing, detailing the type and purpose of the planned surveillance. Written approval must then be received by the authorising officer from the OSC before the surveillance can take place. The threshold for authorising intrusive surveillance is higher than that for directed surveillance, and it can only be carried out to prevent or detect serious crime, for national security purposes, or to protect the economic wellbeing of the United Kingdom.

[38] The Covert Surveillance Code of Practice was published by the Home Office according to section 71 of RIPA, and provides guidance on the use of covert surveillance by public authorities under Part II of the Act, and replaces the code of practice issued in 1999 pursuant to section 101(3) of the Police Act 1997. In Scotland, a broadly equivalent Code was issued according to The Regulation of Investigatory Powers (Covert Surveillance – Code of Practice) (Scotland) Order 2003.

[39] See, for example, the decision of the ECtHR in *Friedl v Austria* (1996) 21 EHRR 83. For a discussion of the privacy issues raised by the use of CCTV cameras in public spaces, see: Goold (2002, 2006).

[40] In December 2009 an interim CCTV regulator was appointed to work with the national CCTV strategy board on six key areas. ‘These are to: develop national standards for the installation and use of CCTV in public space; determine training requirements for users and practitioners; engage with the public and private sector in determining the need for and potential content of any regulatory framework; raise public awareness and understanding of how CCTV operates and how it contributes to tackling crime and increasing public protection; review the existing recommendations of the national CCTV strategy and advise the strategy board on implementation, timelines and cost and development of an effective evidence base; and promote public awareness of the complaints process and criteria for complaints to the relevant agencies (for example, Information Commissioner, local authority or private organisation) or how to deal with complaints relating to technical standards.’(Hansard 15 December 2009 col.114). The Coalition Government has pledged to bring forward proposals for CCTV regulation.

[41] Attorney General’s Reference (No.5 of 2002) [2004] UKHL 40 at paragraph 9.

[42] This view of RIPA has been rejected by the Chief Surveillance Commissioner, who stated: ‘There has been a continued improvement in the general presentation of RIPA documentation. I am disappointed that there continues to be a perception that RIPA is the cause of unnecessary bureaucracy. Where bureaucracy results it is usually the consequence of poor training, less than skillful writing or a lack of time

available to the author to construct the case for the use of covert activity coherently. It should not, in my opinion, be construed as unnecessary – when seeking the protection that this powerful legislation provides – to produce documentation which will withstand scrutiny in a court of law.' Chief Surveillance Commissioner (2008), p. 11.

[43] Note that the current Home Office review includes the use of RIPA by local authorities and access to communications data more generally within its remit. Liberty urges the Coalition Government to carry out a wider-ranging review of RIPA to include: who should authorise the use of RIPA powers, which bodies have access to such powers, and for what purpose such access is available. In addition, Liberty also argues that the Home Office should consider further safeguards to ensure that RIPA complies with human rights standards, including reviewing the procedure of the Investigatory Powers Tribunal.

[44] Marx (2004).

[45] Gillespie (2009).

[46] On this point, see Department of Constitutional Affairs (2003), Section 2.

[47] Although on the face of it the Second Data Protection Principle – that personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes (Data Protection Act 1998, Schedule 1, Part 1) – appears to prohibit data sharing unless it is in accordance with the purpose for which the information is being held, the position may in fact be more complex. For example, according to advice published by the then Department for Constitutional Affairs (2003, Section 6, para. 24) – now the Ministry of Justice – the government takes the view that '[c]ompatible does not mean 'identical to', and purposes which are quite different from the original purposes can still be compatible with those original purposes. We believe that, provided the further processing is for a purpose that is not contradictory to the originally specified purpose or purposes, it will be consistent with the second principle'.

[48] It is worth noting that one of the most recent bodies tasked with considering how best to regulate data sharing between government departments – Cabinet Committee MISC 31 – produced little in the way of substantive recommendations or solutions.

[49] The modern tort of breach of confidence is generally taken to have been established by *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* [1948] RPC 203. In order for an action for breach of confidence to succeed, three requirements must be met: (1) The information must 'have the necessary element of confidence about it' and therefore must not already be in the public domain; (2) The defendant must be under some pre-existing 'obligation of confidence'; and (3) The defendant must make some unauthorised use of the information. Although in many cases an obligation of confidence will arise from some pre-existing relationship –such as employment – following the decision in *Coco v AN Clark (Engineers) Ltd* [1969]

RPC 41 a broader approach has been taken. According to Megarry J in *Coco*, the appropriate test is one based on reasonableness, with the court being required to ask whether 'any reasonable man standing in the shoes of the recipient of the information would have realised that upon reasonable grounds the information was being given to him in confidence' (p. 47).

[50] The major defence to an action for breach of confidence is that the communication was disclosed in the public interest. Although this defence has been raised in a number of recent high-profile cases involving celebrities such as Naomi Campbell and Catherine Zeta-Jones, it is unlikely to be available in the majority of cases given that there is rarely a compelling public interest in disclosing confidential information about ordinary individuals. These cases are significant, however, insofar as they have helped to clarify the relationship between breach of confidence and the right to privacy established under the HRA. Whereas in the past the courts have taken a fairly narrow view of the idea of personal information, according to the 2004 judgement of the House of Lords in *Campbell v Mirror Newspapers*, the law of breach of confidence must now take a broader view based on the values enshrined in the HRA, most notably Article 8. Under this new approach, when a breach of confidence is claimed, the court must determine whether the information in question is sufficiently private as to fall within the ambit of Article 8.

[51] See Bennett and Raab (2006), Chs. 6 and 7.

[52] *Report of the Committee on Data Protection*, Chairman: Sir Norman Lindop, London: HMSO 1978, Cmnd. 7341, pp. 164-81. Lindop's approach has been modified in new recommendations by Dr Chris Pounder in *A Draft Blueprint for the Next Generation of Data Protection Law Based on Codes of Practice*, June 2007, available at: http://www. amberhawk.com/policydoc.asp, accessed 17/9/10.

[53] These include the Article 29 Working Party established under Directive 95/46/EC, the European Data Protection Supervisor (EDPS) and Vivian Reding, the European Commissioner for Justice, Fundamental Rights and Citizenship. See Article 29 Working Party (2009); EDPS 2010; OUT-LAW news (2010).

[54] For example, Liberty, Justice, Privacy International, No2ID, the online Foundation for Information Policy Research, the British Computer Society, and the Enterprise Privacy Group.

[55] For example, Eurobarometer (2008).

[56] See Black (2008) for caveats about principles, and for a penetrating analysis of the paradoxes of interpretation, communication, compliance, enforcement, internal management, ethics, and trust.

[57] It is important to note that because a country will often modify the data protection principles before enshrining them in domestic law, there is a danger that the universality of the principles is being gradually undermined. In this regard, the data protection principles are at risk of becoming a victim of their own success.

[58] This should not be confused with notification – formerly 'registration' – under the DPA, whereby data holders notify the regulatory authority, but not individuals, of their data processing activities. In practice, the ALRC's 'or otherwise' provision could lead to a weakening of the notification principle.

[59] Hunton & Williams LLP, Centre for Information Policy Leadership, *Data Protection Accountability: The Essential Elements – A Document for Discussion*, October 2009, pp. 2-3; 'Global Privacy Standards for a Global World – The Madrid Privacy Declaration, 3 November 2009', http://thepublicvoice.org/madrid-declaration/, accessed 10 November 2009; Article 29 Working Party, *The Future of Privacy*, WP 168, 1 December 2009. These endorsements of the principle have been criticised on grounds of vagueness and incompleteness; see Colin Bennett, 'International privacy standards: Can accountability be adequate?' *Privacy Laws & Business International Newsletter*, Issue 106, August 2010, pp. 21-3.

[60] See Chapter 19 of that report for a full discussion of consent.

[61] See Manson and O'Neill (2007) for a sceptical analysis of 'informed consent' in the field of bioethics.

[62] Ideally, this would also provide a clear rationale for the protection of privacy, and be based on an adherence to one or more of the privacy theories identified in Chapter 3 of this report. Having a stated rationale would not only provide regulators and the courts with a 'touchstone' when it comes to questions of statutory interpretation, but also provide lawmakers with a structure for future amendments and complementary legislation.

[63] For the recent Australian attempt to grapple with the journalistic exemption from privacy law, see ALRC (2008), vol. II, pp. 1439-73.

[64] Potential opportunities to consider this arise through the forthcoming Freedom Bill and consultations on changes in the DPA and the EU Directive.

[65] If FOI laws and their enforcement machinery are included in any reform, the separate Scottish FOI arrangements would also have to be addressed.

Contacts

England

Equality and Human Rights Commission Helpline
FREEPOST RRLL-GHUX-CTRX
Arndale House, The Arndale Centre, Manchester M4 3AQ
Main number: 0845 604 6610
Textphone: 0845 604 6620
Fax: 0845 604 6630

Scotland

Equality and Human Rights Commission Helpline
FREEPOST RSAB-YJEJ-EXUJ
The Optima Building, 58 Robertson Street, Glasgow G2 8DU
Main number: 0845 604 5510
Textphone: 0845 604 5520
Fax: 0845 604 5530

Wales

Equality and Human Rights Commission Helpline
FREEPOST RRLR-UEYB-UYZL
3rd Floor, 3 Callaghan Square, Cardiff CF10 5BT
Main number: 0845 604 8810
Textphone: 0845 604 8820
Fax: 0845 604 8830

Helpline opening times:
Monday to Friday 8am–6pm.
Calls from BT landlines are charged at local rates, but calls from mobiles and other providers may vary.

Calls may be monitored for training and quality purposes.
Interpreting service available through Language Line, when you call our helplines.

If you require this publication in an alternative format and/or language please contact the relevant helpline to discuss your needs. All publications are also available to download and order in a variety of formats from our website.
www.equalityhumanrights.com

www.equalityhumanrights.com

This report examines the threats to information privacy that have emerged in recent years, focusing on the activities of the state. It identifies two principal areas of concern: the state's handling of personal data, and the use of surveillance by public bodies. The report finds that the existing approach to the protection of information privacy in the UK is fundamentally flawed, and that there is a pressing need for widespread legislative reform. The report argues for the establishment of a number of key 'privacy principles' that can be used to guide future legal reforms and the development of sector-specific regulation.

Equality and Human Rights Commission