ISBN 978-1-4741-0907-9

Law Commission
Reforming the law

Data Sharing between Public Bodies
A Scoping Report

Law Commission

Data Sharing between Public Bodies A Scoping Report

Law Com No 351

Law Com No 351

The Law Commission

(LAW COM No 351)

DATA SHARING BETWEEN PUBLIC BODIES: A SCOPING REPORT

Presented to Parliament pursuant to section 3(2) of the Law Commissions Act 1965

Ordered by the House of Commons to be printed on 10 July 2014

HC 505

This publication is available at www.gov.uk/government/publications

Print ISBN 9781474109079
Web ISBN 9781474109086

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

ID 04071405 07/14 41831 19585

Printed on paper containing 75% recycled fibre content minimum

THE LAW COMMISSION

The Law Commission was set up by the Law Commissions Act 1965 for the purpose of promoting the reform of the law.

The Law Commissioners are:

The Right Honourable Lord Justice Lloyd Jones, *Chairman*
Professor Elizabeth Cooke
David Hertzell
Professor David Ormerod QC
Nicholas Paines QC

The Chief Executive of the Law Commission is Elaine Lorimer.

The Law Commission is located at 1st Floor, Tower, 52 Queen Anne's Gate, London SW1H 9AG.

The terms of this report were agreed on 1 July 2014.

The text of this report is available on the Law Commission's website at http://lawcommission.justice.gov.uk/areas/data-sharing.htm.

THE LAW COMMISSION

DATA SHARING: A SCOPING REPORT

CONTENTS

THE LAW COMMISSION

DATA SHARING BETWEEN PUBLIC BODIES: A SCOPING REPORT

To the Right Honourable Chris Grayling, MP, Lord Chancellor and Secretary of State for Justice

PART 1: PRESENTING THE ISSUES

CHAPTER 1 INTRODUCTION

INTRODUCTION

1.1 Data sharing affects us all. As Lord Mance explained in a recent Supreme Court case

> Information is the key to sound decision-making, to accountability and development; it underpins democracy and assists in combatting poverty, oppression, corruption, prejudice and inefficiency. Administrators, judges, arbitrators, and persons conducting inquiries and investigations depend upon it; likewise the press, NGOs and individuals concerned to report on issues of public interest. Unwillingness to disclose information may arise through habits of secrecy or reasons of self-protection. But information can be genuinely private, confidential or sensitive, and these interests merit respect in their own right and, in the case of those who depend on information to fulfil their functions, because this may not otherwise be forthcoming.[1]

1.2 This report analyses the responses to the Law Commission's Scoping Consultation Paper, *Data Sharing Between Public Bodies,* in order to decide whether there are inappropriate legal or other hurdles to the transfer of information between public bodies and, potentially, between public bodies and private bodies engaged in public service delivery. We go on to consider whether law reform would mitigate or resolve the problems identified.[2]

1.3 We conclude that there are problems with the form of the law relating to data sharing that could usefully be addressed. We have also found evidence of problems which are not directly due to the form of the law, but could be alleviated by law reform.

[1] *Kennedy v The Charity Commission* [2014] UKSC 20, [2014] 2 WLR 808.

[2] Data Sharing Between Public Bodies (2013) Law Commission Consultation Paper No 214, available at http://lawcommission.justice.gov.uk/areas/data-sharing.htm (last visited 1 July 2014). Subsequent references will be in the form "Consultation Paper, para X".

1.4 The protection of privacy is fundamental to any data sharing regime. Any law reform proposals must reflect a proper understanding of the role and importance of privacy rights and of the disclosure of information in society today. The protection of privacy is an imperative in itself. In addition, confidence on the part of public bodies and of the public as a whole, in the data sharing regime, is vital to making it work.

RECOMMENDATIONS

1.5 In this report we make three principal recommendations.

Recommendation 1

1.6 We recommend that a full law reform project should be carried out in order to create a principled and clear legal structure for data sharing, which will meet the needs of society. These needs include efficient and effective government, the delivery of public services and the protection of privacy. Data sharing law must also accord with emerging European law and cope with technological advances. The project should include work to map, modernise, simplify and clarify the statutory provisions that permit and control data sharing and review the common law.

Recommendation 2

1.7 The scope of the review should extend beyond data sharing between public bodies to the disclosure of information between public bodies and other organisations carrying out public functions.

Recommendation 3

1.8 The project should be conducted on a tripartite basis by the Law Commission of England and Wales, together with the Scottish Law Commission and the Northern Ireland Law Commission.

1.9 We consider that the project could usefully include consideration of the functions of the Information Commissioner in relation to data sharing, including the Commissioner's enforcement role. The work of other bodies providing advice and guidance should be explored to improve the consistent application of data sharing law across government and in public service delivery more widely.

1.10 The investigation should also include consideration of "soft law" solutions such as codes of practice, as well as advice and guidance, training of staff, and ways of sharing best practice in the management of data sharing between public bodies.

BACKGROUND

1.11 This scoping project emerged from proposals by Chief Police Officers and was approved by the Lord Chancellor as part of the Law Commission's Eleventh Programme of Law Reform.[3]

1.12 Early investigations suggested that there are significant problems in

[3] Eleventh Programme of Law Reform (2011) Law Com No 330.

understanding the Data Protection Act 1998 and other law governing how information may be shared. Views on both the express and the implied meaning of statutory provisions vary from person to person and from time to time. Guidance is not always clear and sometimes conflicts. We could see that there are problems in practice. What we could not initially see was a clear problem with the law itself. However, the existence of these differing interpretations suggests either that the law is not sufficiently clear or that circumstances have changed since the law was made, so that clarification or modernisation are needed. We concluded that a scoping project should be conducted, in order to find out whether there are hurdles to data sharing which would be removed or mitigated by law reform. We agreed to report back to Government on our findings, after which the UK Government and devolved administrations could decide whether to refer a full law reform project to the Law Commissions of England and Wales, Scotland and/or Northern Ireland.

LIAISON WITH GOVERNMENT

1.13 We have liaised with the Cabinet Office and Ministry of Justice during this project, and will deliver the report to both in order for Ministers to decide what steps to take next. The Ministry of Justice has lead responsibility for policy on data protection and data sharing across government. The Cabinet Office has responsibility for the effective running of government, including government efficiency, transparency and accountability. The Cabinet Office is developing policy and considering certain targeted reforms to the law on data sharing, which will be published in due course.[4] We have also consulted widely with other Government departments.[5]

THE CONSULTATION PROCESS

1.14 This project commenced in April 2013. We reviewed the national and European legal framework for data protection and data sharing and carried out pre-consultation meetings with representatives from the Information Commissioner's Office, various government departments, public bodies and others with an interest in data protection and privacy law. Our investigations for this project were concerned as much with people's experience and understanding in practice, as with the interpretation of the law. Consultation was, therefore, essential to developing an understanding of the issues.

1.15 We published a consultation paper on 16 September 2013, providing an overview of the law, asking 22 questions. Our questions were phrased in broad, fairly general terms, in order to find out what consultees thought the relevant issues were and to ask about their experiences.

1.16 The public consultation period ran for three months until 16 December 2013 and we accepted some late submissions. We attended 50 consultation meetings and events and received 87 formal written consultation responses.

[4] The Cabinet Office has entered into an open policy-making process to develop its proposals. Information on that project may be found at: http://datasharing.org.uk/ (last visited 1 July 2014).

[5] A list of consultation responses may be found at Appendix A to this report and a list of consultation meetings may be found at Appendix B.

1.17 We are very grateful to all those who submitted consultation responses or attended meetings. In particular, we are very grateful to those who organised events specifically for the purposes of discussing our consultation paper.

Written responses

1.18 We received 87 written responses from a wide range of consultees, including:

(1) The UK Government and non-departmental public bodies;

(2) The Scottish Government;

(3) The Welsh Government;

(4) Public bodies;

(5) Private bodies engaged in public service delivery;

(6) Professional and representative bodies;

(7) Local government officials;

(8) Health and social care professionals;

(9) Data protection practitioners;

(10) Third sector bodies;

(11) Legal practitioners;

(12) Legal academics and social scientists interested in information law;

(13) Members of the public.

1.19 A full list of formal written responses can be found in Appendix A.

1.20 In this report we refer to "data protection practitioners" to include a variety of people making data protection and data sharing decisions or advising on data protection and data sharing. These include: data protection officers, information governance officials in local or national government or other public bodies, lawyers advising on information governance, and consultants commentating and providing training in this field or writing about it.

Consultation events and meetings

1.21 We attended some 50 consultation events and meetings across England and Wales with a range of stakeholders, including:

(1) Central and local government officials;

(2) Public bodies;

(3) Police;

(4) Health and social care professionals;

(5) Data protection professionals;

(6) Privacy interest groups;

(7) Legal practitioners;

(8) Academics.

1.22 A full list of events and meetings attended can be found in Appendix B.

1.23 The purpose of this report is to set out our analysis of the existing problems and the further work needed in order to reform the law on data sharing. We have integrated our analysis of consultation responses into this report.

CURRENT LAW

1.24 The main elements of the current law are set out in the Consultation Paper. If a full law reform project proceeds, a more detailed description and mapping of the statutory and common law will be necessary. What follows here is a brief introduction to the types of information we are concerned with and the sources of law regulating data sharing. It is only intended to introduce some of the key legal concepts and provisions. [6]

Types of data

1.25 There are different types of information which may be shared between public bodies or between public bodies and other bodies or individuals engaged in public service delivery. We are concerned with personal data, whether identified or de-identified.[7]

Personal data

1.26 Personal data are regulated by the Data Protection Act 1998. The Act transposes the 1995 European Union Directive on Data Protection. Personal data are defined as

> Data which relate to a living individual who can be identified –
>
> (a) from those data; or
>
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

[6] For a fuller explanation see Consultation Paper, in particular, chs 3 (Restrictions on Data Sharing) and 4 (The Power to Share Data). There are few substantive text books on information law in the United Kingdom. We have found the practitioners' text written by Rosemary Jay helpful: R Jay, *Data Protection Law and Practice* (4th ed 2012).

[7] "Data" are defined in s 1 of the Data Protection Act 1998.

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.[8]

1.27 Personal data include sensitive personal data, which are defined in the Act as information relating to the racial or ethnic origin; political opinions, religious or other beliefs; membership or otherwise of a trade union; physical or mental condition; sexual life of a person and the commission or alleged commission of any offence or the disposal or sentence in any such proceedings by a court.[9]

Anonymised data

1.28 Anonymisation is a process intended to make it impossible to identify the individual concerned from the data. Anonymised data may be presented in an aggregated form, for example as statistics giving an approximate number of people diagnosed with cancer each year in the United Kingdom, or they may be randomised, so that certain facts are changed to hide the identities of the data subjects. They may be presented on an individual level, but with a unique identifier, for example describing patient 1234 as a male, aged 70, a non-smoker, of African ethnicity and in socio-economic group AB. This is sometimes known as pseudonymisation or key-coding. Such data is anonymous if the recipient does not have and is unlikely to obtain the information necessary to reverse the key coding to re-identify the data.

1.29 There is always a risk that the combination of information held about an anonymised data subject may enable them to be identified, or that it may be possible to re-identify the individual by combining other data with the anonymised data. The more specificity applied to the individual, the more likely that it will be possible to identify them. It will tend to be the case that the more truly anonymous the information, the less detailed information that may be extrapolated from it.

1.30 If the individual cannot be identified from those data or those data combined with other data in the controller's possession or likely to come into their possession, then anonymised data are not personal data and are not subject to the controls which apply to personal data.[10] There is a sliding scale of risk that it will be possible to re-identify the individual concerned.[11]

Other information

1.31 As we explained in the Consultation Paper, there are many other types of information which are not and have never been personal data. This includes

[8] Data Protection Act 1998, s 1; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), Official Journal L 281 of 23/11/1995 p 31.

[9] Data Protection Act 1998, s 2.

[10] Data Protection Act 1998, sch 1, part 2, para 4 provides that where personal data contains a general identifier, such as a number or code relating to an individual, those data must comply with any conditions required by the Secretary of State for processing general identifiers. Otherwise, they will not satisfy the requirement to process data fairly. This provision assumes that anonymised data (where a general identifier is used) may still be personal data.

[11] See ch 6 below for further discussion of anonymised data.

information about public service performance, financial information about public or private bodies, or information about plants, animals, buildings, air quality, nuclear or wind power, the weather and so on. The information might be "raw" or "source" data, including datasets within the meaning of the Freedom of Information Act 2000.[12] Such data might include analysis, such as risk assessment or predictions, or official statistics within the meaning of the Statistics and Registration Service Act 2007.[13]

Powers to share data

1.32 Before considering whether there are any restrictions on data sharing, a public body must have a power to share data.[14]

Private and third sector organisations

1.33 Private organisations are free to act without having to point to a statutory or common law power to do so, subject to restrictions in the law, or in their constitution, as set out in articles of association or memoranda. No explicit source of power to share data is needed.

Public bodies

1.34 A public body can only act when it has the legal power to do so and can only act within its powers.[15] Public bodies derive their powers from legislation or from the common law. Government departments headed by a Minister of the Crown, such as the Department for Work and Pensions or the Ministry of Justice, have common law powers, including powers derived from the Crown under the royal prerogative. They also have powers derived from legislation. Other public bodies, such as Her Majesty's Revenue and Customs and local authorities, were created by Acts of Parliament. They are creatures of statute and all of their powers derive from legislation.[16]

Gateways

1.35 Legislative powers to share information are often referred to as "gateways". They may be express powers, conferring power to share information, perhaps for a particular purpose, or with a particular public body. Alternatively, the power may be implied, where data sharing is reasonably incidental to an express power to do something else. Throughout this report we use the term "gateway" to describe a statutory provision empowering (or, more rarely, requiring) a public body to disclose information held by it to another, usually also public, body. These provisions can be accompanied by criminal offences of unauthorised disclosure on the part of staff of the disclosing body and sometimes of unauthorised further disclosure by staff of the recipient body. They can contain provisions circumscribing the categories of information that may be disclosed and/or the

[12] Freedom of Information Act 2000, s 11(5).

[13] For further examples, see Consultation Paper, paras 1.17 to 1.19.

[14] This is discussed in more detail in ch 4 of the Consultation Paper and the resulting issues for effective data sharing are discussed in the rest of this report.

[15] See, for example, H W R Wade and C F Forsyth, *Administrative Law* (10th ed 2009) p 17.

[16] Common law powers are discussed in ch 5 below and examples from the Department for Work and Pensions are given in ch 9.

circumstances in which, or purposes for which, it may be disclosed.

Express statutory gateways

1.36 Express gateways may be contained in primary legislation, which may also provide for the creation of further powers to share information under subordinate legislation.[17] Gateways tend to be permissive, creating a discretion to share information, but not an obligation.[18] Where a gateway is permissive, other factors may weigh against disclosure. If disclosure will be costly, or will not benefit the data holder, but will only benefit the recipient, there may not be adequate incentives to share. Alternatively, gateways may require the public body to disclose information. Gateways may also place restrictions on whom the information may be shared with, the purposes for which information may be shared, and on onward disclosure or use. [19]

1.37 Gateways tend to restrict as well as permit data sharing. Provision may define:

(1) who may request or be supplied with the information;

(2) who may act on behalf of the relevant authority;

(3) from whom the information may be requested;

(4) the purposes for which the information may be used; these may be narrowly defined, or they may be broader; for example the information may be used for the purpose of carrying out the organisation's functions under the Act; or the purposes for which the information may be used may be limited to those set out in a notice given by the holder to the recipient;

(5) the level of necessity required before the information may be requested or disclosed; this might be limited to "necessity" or what is "necessary or expedient" or be as wide as "such documents as he may reasonably require" for the purposes of carrying out functions under the Act, or more specifically defined functions; [20]

(6) the type of information which may be used or required and information that may *not* be used or required, such as information not obtained for an

[17] For example, the Statistics and Registration Service Act 2007, s 47 gives the power to the Minister of the Cabinet Office to make regulations for the purpose of authorising a public authority to disclose information to the Statistics Board where the disclosure would otherwise be prohibited by law or the authority would not otherwise have power to make the disclosure. See, for example, Statistics and Registration Service Act 2007 (Disclosure of Pupil Information) (England) Regulations 2009, SI 2009 No 277.

[18] See, for example, Serious Crime Act 2007, s 68 permitting the disclosure of information to prevent fraud: "A public authority may, for the purposes of preventing fraud or a particular kind of fraud, disclose information as a member of a specified anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation."

[19] Barriers to data sharing other than the law are discussed below in ch 7. Statutory gateways are discussed in ch 4 and detailed examples are explored in ch 8, on Her Majesty's Revenue and Customs, and ch 9, on the Department for Work and Pensions.

authorised purpose, or which is prohibited by the Data Protection Act 1998;[21]

(7) the amount of information that may be processed, which may include a proportionality requirement;[22]

(8) criminal offences for the misuse of information, or for any failure to furnish information or for providing false information;[23]

(9) any procedural requirements, such as prior consultation of a particular body or required matters to consider before reaching a decision,[24] or prescribed forms;[25]

(10) limitations on onward disclosure of the information, which might include a requirement to obtain consent and compliance with the proportionality principle; [26]

(11) practical requirements as to how the document may be dealt with, such as restrictions on photocopying or disposal.[27]

Implied statutory gateways

1.38 The nature and extent of a public authority's statutory powers must be found by interpreting Parliament's intention in the relevant legislation. Those powers may be implied. This is discussed in more detail in the Consultation Paper.[28]

1.39 Many Acts of Parliament that define the functions and powers of public bodies include incidental powers which are drafted broadly enough to cover information transfer. Section 1 of the Localism Act 2011 creates a very broad power, which is a "general power of competence" for local authorities:

> A local authority has power to do anything that individuals generally may do.

1.40 This power is extensive and may be exercised

[20] National Audit Act 1983, s 8(1) "such documents as he may reasonably require"; Criminal Appeals Act 1995, s 17(2)(b) "where it is reasonable to do so"; Crime and Disorder Act 1998, s 115(1) "necessary or expedient".

[21] See, for example, Local Government Finance Act 1992, sch 2, para 11(1A).

[22] Anti-Terrorism, Crime and Security Act 2001, s 19(3).

[23] See, for example, Commissioners for Revenue and Customs Act 20015, s 19; Statistics of Trade Act 1947, s 4(1). Offences relating to information held by Her Majesty's Revenue and Customs are discussed in ch 8 below.

[24] National Audit Act 1983, s 8(5).

[25] See, for example, Local Government Finance Act 1992, sch 2, para 11(3).

[26] For an express requirement to comply with the proportionality test, see Anti-Terrorism, Crime and Security Act 2001, s 19(3). For a statutory consent requirement, see Financial Services and Markets Act 2000, s 348.

[27] Immigration and Asylum Act 1999, s 20(2A).

[28] Consultation Paper, paras 4.26 to 4.33.

for, or otherwise than for, the benefit of the authority, its area or persons resident or present in its area.[29]

1.41 The courts will infer powers reasonably incidental to the purposes of the legislation. The disclosure of data is often incidental to other statutory functions. For example, in order to satisfy a duty to co-operate, public bodies may well have to share information. In another example, the proper functioning of a regulatory body might require implied powers to disclose comments that were made to a regulated public body in confidence.[30]

1.42 Legislation may provide that information collected for one purpose may be used for another purpose.[31] Where there is no such express provision, the courts will be slow to imply powers to use information obtained for one purpose for a different purpose.[32]

1.43 In addition to obligations under the Human Rights Act 1998 to interpret statutes so as to comply with the European Convention on Human Rights, legislation should be interpreted so as not to breach fundamental rights at common law.[33]

1.44 The decision of the Administrative Court in *R(W) v Secretary of State for Health* provides a recent example of the complexities of interpreting implied and common law powers. Mr Justice Silber held that it was lawful for National Health Service bodies to pass non-medical information about non-resident recipients of National Health Service treatment who owed outstanding debts for health service charges to the Secretary of State for Health, who in turn could lawfully pass this information to the Secretary of State for the Home Department so that the Home Department could apply immigration sanctions for the failure to pay those charges. The court held that the legal basis for the first transfer of information existed under the general powers of National Health Service foundation trusts and National Health Service Trusts[34] to do anything that is necessary or

[29] A more common example of a broad power may be found in such s 5A of the Fire and Rescues Services Act 2004: "(1) A relevant fire and rescue authority may do— (a) anything it considers appropriate for the purposes of the carrying-out of any of its functions (its "functional purposes"), (b) anything it considers appropriate for purposes incidental to its functional purposes, (c) anything it considers appropriate for purposes indirectly incidental to its functional purposes through any number of removes."

[30] *Woolgar v Chief Constable of Sussex Police* [2000] 1 WLR 25.

[31] Commissioners for Revenue and Customs Act 2005, s 17 provides that information acquired by the Revenue and Customs in connection with a function may be used by them in connection with any other function. However, this is subject to any other statutory restrictions on its use.

[32] *Marcel v Commissioner of Police for the Metropolis* [1991] 2 WLR 1118; *Morris v Director of the Serious Fraud Office* [1993] Ch 372, Marcel was recently applied in *Tchenguiz v Director of the Serious Fraud Office* [2013] EWHC 2128 (QB), [2014] 1 WLR 1476 where the court considered whether the terms of the Criminal Justice Act 1987 prohibit the Serious Fraud Office from giving disclosure of relevant documents or whether there is an absolute bar on disclosure under the Criminal Justice Act 1987. The High Court held that the Serious Fraud Office may not disclose voluntarily but must point to a statutory gateway.

[33] *R v Secretary of State for the Home Department ex parte Simms* [2000] 2 AC 115 at [131], Lord Hoffman; *R v Secretary of State for the Home Department, ex parte Leech* [1994] QB 198 at 211, Lord Hoffman; *R (Daly) v Secretary of State for the Home Department* [2001] UKHL 26; [2001] 2 AC 532 at 537 and 538.

[34] National Health Service Act 2006, s 47 and sch 4 respectively.

expedient for the purposes or in connection with their functions, in this case imposing and recovering charges under regulation 3 of the Charging Regulations.[35] Similarly, the legal basis for disclosure from the Secretary of State for Health to the Secretary of State for the Home Department was found in the power of the Secretary of State to do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of any function conferred by the Act,[36] read with the Secretary of State's general function of promoting an effective healthcare system.[37] The court also held that the Secretary of State had common law powers to so pass the information.[38]

Non-statutory data sharing powers

1.45 Ministers of the Crown and Ministerial Departments of Government also exercise power under royal prerogative, what is sometimes known as the "third source of authority" and the "Ram Doctrine". This is discussed in the Consultation Paper and we consider recent developments before the courts in Chapter 5 below.[39]

1.46 The Ram doctrine, third source and prerogative powers may overlap, but are not one and the same. Nor are any of these sources of power clearly defined.

Royal Prerogative

1.47 Royal prerogative powers are the non-statutory powers that the Crown retained after the monarch's powers were restricted, following the Restoration in the 17th century. They belong to the Crown but are generally exercisable by the government, or a specific minister. The precise character and extent of the prerogative is a matter of debate.[40]

The Ram memorandum

1.48 The Ram Doctrine is so called after legal advice given to the Government of the day in 1945 by Sir Glanville Ram, First Parliamentary Counsel, that a Minister of the Crown

[35] National Health Service (Charges to Overseas Visitors) Regulations 2011, SI 2011 No 1556.

[36] National Health Service Act 2006, s 2.

[37] National Health Service Act 2006, s 1.

[38] *R (W, X, Y and Z) v Secretary of State for Health and Secretary of State for the Home Department* [2014] EWHC 1532 (Admin), 15 May 2014.

[39] Consultation Paper, paras 4.34 to 4.59.

[40] There is no agreed definition or agreed consensus on the nature and extent of prerogative powers. Lord Fraser, in *Council for the Civil Service Unions v Minister for the Civil Service ("the GCHQ Case")* [1985] AC 374 approved A Dicey's description: "The prerogative is the name for the remaining portion of the Crown's original authority … the residue of discretionary power left at any moment in the hands of the Crown, whether such power be in fact exercised by the King himself or by his ministers." Others have interpreted prerogative powers more strictly to "only those governmental powers which are unique to the Crown." See *De Smith's Judicial Review* (7th ed 2013) para 3-030.

> may, as an agent of the Crown, exercise any powers which the Crown has power to exercise, except in so far as he is precluded from doing so by statute.[41]

1.49 The House of Lords' Constitution Committee considered the extent of ministerial powers derived from Sir Granville Ram's legal advice. The Committee concluded that the Ram Memorandum is not a source of law, but merely legal advice and described the Ram Doctrine as a "troubling legal fallacy", which is misunderstood by Government to mean that Ministers may do anything a natural person may do, unless prohibited by statute. The Committee agreed with the Attorney General's evidence:

> I think that Sir Granville Ram was emphasising that the Crown is not a creature of statute. Therefore, it has inherent powers that it can exercise, apart from prerogative powers, as if it were a natural person. But … it is circumscribed by public law; by propriety; by human rights … I do not think that Whitehall thinks the Government can do everything a private individual can do, because it is circumscribed by those very things I have just listed. [42]

1.50 The Crown can enter into contracts, employ staff, buy and sell property, settle a trust, and perform other management functions.[43] These powers are subject to the ordinary law, including legislation and general public law, the law of confidence, contract and the legal rights of other persons. The exercise of such powers is subject to the supervisory jurisdiction of the courts by way of judicial review and subject to the Human Rights Act 1998.[44] Common law powers are discussed in more detail in Chapter 5 below.[45]

Third source of power

1.51 This phrase was coined in a series of academic articles by Professor B V Harris to describe powers of government that do not come from statute or the royal prerogative. Harris developed his theory of the role and extent of this third source of power. He considered the relationship between these powers and Government's accountability and susceptibility to the supervisory jurisdiction of the courts in light of theories of "common law constitutionalism" or fundamental

[41] This advice was made public in answer to a Parliamentary question in 2003: Hansard (HC), 25 February 2003, col WA 12.

[42] House of Lords, Constitution Committee, *Thirteenth report: The Pre-emption of Parliament* (24 April 2013). It may be found at: http://www.publications.parliament.uk/pa/ld201213/ldselect/ldconst/165/16502.htm (last visited 1 July 2014).

[43] *R (New London College Ltd) v Secretary of State for the Home Department* [2013] 1 WLR 2358. This case is discussed in more detail below in ch 5 and in the Consultation Paper, paras 4.50 to 4.55.

[44] *Entick v Carrington* 95 ER 807; (1765) 2 Wils KB 275; *A-G v De Keyser's Royal Hotel Limited* [1920] AC 508; *R v Home Secretary ex parte Fire Brigades Union* [1995] 2 AC 513; to be read with *R v Secretary of State for the Home Department, ex parte Northumbria Police Authority* [1989] QB 26.

[45] See also Consultation Paper, paras 4.34 to 4.59.

rights as protected by a common law constitution.[46] Ministerial departments sometimes seek to rely on the third source for powers to share information in support of their statutory or common law functions. As we discuss in Chapter 5 below, the extent of the third source powers, and even their existence, have been questioned.[47]

Relationship between different data sharing provisions

1.52 One of the complaints made about the law on data sharing is that it is often difficult to know what the law is, because of the number and range of sources of law. It is also difficult to know which law takes precedence on any particular issue. Statutory provisions interact with other legal requirements and the hierarchy is not always clear and is often difficult to understand.

1.53 Some gateways expressly override certain other statutory provisions.[48] Some expressly do not override certain other statutory provisions.[49] Some provide for secondary legislation to prescribe any particular restrictions.[50] Some gateways provide for certain common law duties or other obligations to be overridden, such as confidentiality.[51] There may be provision in other legislation providing that data sharing does not breach certain specified legal restrictions.[52]

1.54 A statutory gateway may impliedly override other provisions. The introduction of statutory powers can supersede a common law power covering the same ground, so the common law may be eroded by the development of statutory gateways. Whether a particular statutory provision supersedes the common law is a matter of statutory construction, with the result that uncertainty can overshadow the use of common powers in areas where Parliament has also passed statutory

[46] B V Harris, "The third source of authority for Government action" (1992) 108 *Law Quarterly Review* 626; B V Harris, "The "third source" of authority for Government action revisited" (2007) 123 *Law Quarterly Review* 225; and BV Harris, "Government "third source" action and common law constitutionalism" (2010) 126 *Law Quarterly Review* 373.

[47] House of Lords, Constitution Committee, *Thirteenth Report: The Pre-emption of Parliament* (24 April 2013), which may be found at http://www.publications.parliament.uk/pa/ld201213/ldselect/ldconst/165/16502.htm (last visited 1 July 2014).

[48] Employment and Training Act 1973, s 4(3) provides that "nothing in section 9 of the Statistic of Trade Act 1947 (which restricts the disclosure of information obtained under that Act) shall prevent or penalise…(c) the disclosure by the Secretary of State …to a board of relevant information."

[49] Offender Management Act 2007, s 14(6)(b).

[50] Local Government Finance Act 1982, s 18.

[51] Regulations made under the National Health Service Act 2006, s 251 allow disclosure in breach of the duty of confidence. The Health and Social Care Information Centre may require any health or social care body to provide information under the Health and Social Care Act 2012, s 259. "The provision of information under this section— (a) does not breach any obligation of confidence owed by the person providing it, but (b) is subject to any express restriction on disclosure imposed by or under another Act."

[52] For example, the Copyright, Designs and Patents Act 1998, s 50 provides "(1) Where the doing of a particular act is specifically authorised by an Act of Parliament, whenever passed, then, unless the Act provides otherwise, the doing of that act does not infringe copyright." This is in addition to any other defence of statutory authority available under any other enactment.

gateways to share data.[53]

Restrictions on data sharing

1.55 Data sharing is restricted by the extent of a public body's powers to share information, as discussed above. It is also restricted by the limits of any data sharing gateway. In addition, data sharing is restricted by European law, in the form of the 1995 Data Protection Directive, implemented by the Data Protection Act 1998, by European human rights law, and by international human rights law. European law will also be interpreted in light of the Charter of Fundamental Rights of the European Union.[54]

Data Protection Act 1998

1.56 The Data Protection Act 1998 implements the 1995 European Union Data Protection Directive and transposes it into UK law. The 1998 Act does not create statutory gateways for data sharing. The person or organisation must already have the power to share the information before considering any restrictions under the Data Protection Act. It regulates the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.[55] The Act is intended to comply with Article 8 of the European Convention on Human Rights. [56]

1.57 Data sharing is a type of data processing. The Data Protection Act requires personal information to be processed in accordance with eight data protection principles, subject to exemptions set out in section 4. The data protection principles are set out in Schedule 1 Part I of the Act and explained in Part II of Schedule 1. The Act also requires prior notification in most cases.[57] The principles apply equally to both public and private bodies processing personal data.

1.58 The principles are as follows:

> 1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
>
> (a) at least one of the conditions in Schedule 2 is met, and
>
> (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

[53] *A-G v De Keyser's Royal Hotel Ltd* [1920] AC 508; *R v Secretary of State for the Home Department, ex parte Northumbria Police Authority* [1989] QB 26.

[54] Official Journal C 83/389 of 30.03.2010.

[55] The long title of the Data Protection Act 1998 is "An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information."

[56] For a more detailed discussion of the data protection principles see Consultation Paper, paras 3.9 to 3.52.

[57] Under Data Protection Act 1998, s 17 it is generally unlawful to process personal data unless the data controller maintains an appropriate entry in the national register of data controllers, maintained by the Information Commissioner's Office. Certain exceptions are set out in the Act.

2. 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.

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

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

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

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

7. 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.

8. 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.

1.59 Schedule 2 provides the conditions for processing to be legitimate.[58] These may be divided into two categories: where the data subject consents or where processing the data is necessary for one of the listed reasons. [59] These are: performance of a contract; compliance with a legal obligation; the protection of the data subject's "vital interests"; public functions exercised in the public interest; legitimate interests pursued by the data controller or third parties, except where the processing would prejudice the rights and freedoms or legitimate interests of the data subject. In addition, the Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

1.60 Schedule 1 prohibits the processing of sensitive personal data, except where at least one condition in Schedule 3 is met. Exemptions in Schedule 3 are more restricted. They include: *explicit* consent of the data subject; necessary processing for a listed purpose, including employment law; non-profit organisations; information already made public by the data subject; legal proceedings; the administration of justice or functions of Parliament or Ministerial functions; preventing or detecting fraud; medical purposes undertaken by a health professional; the promotion of racial or ethnic equality; or processing under an order made by the Secretary of State.[60]

[58] Sch 2 transposes art 7 of the Data Protection Directive.

[59] "Necessity" incorporates a proportionality test: *Chief Constable of Humberside v Information Commissioner* [2009] EWCA Civ 1079; [2010] 1 WLR1136, *applying* Case C-524/06 *Huber v Germany* [2008] ECR I-9705.

[60] See for example, Data Protection (Processing of Sensitive Data) Order 2006, SI 2006 No 2068.

Law of confidence

1.61 The common law duty of confidence protects private information from disclosure. Breach of confidence protects a variety of information, including personal, commercial, artistic and governmental information. The information may be in any form.

1.62 The main elements of an actionable breach of confidence are that information is disclosed where the information was not in the public domain and the information was imparted in confidence in the context of a confidential relationship. Since the Human Rights Act 1998 came into force, the law has developed to include breaches where disclosure would be in breach of article 8 of the European Convention on Human Rights in the absence of a confidential relationship.[61]

1.63 Confidentiality may be waived by consent. Alternatively, disclosure may be lawful if it is necessary in the public interest.

1.64 In addition to the legal duty of confidence, there may be professional duties of confidence, subject to professional regulation. The relationship between doctor and patient, for example, is founded strongly upon a professional relationship of confidence which goes beyond the common law duty of confidence.[62]

1.65 A more detailed explanation of the law of confidence may be found in Chapter 3 of the Consultation Paper and the issues raised for data sharing are discussed in Chapter 5 below.[63]

Other legal restrictions

1.66 Data sharing may also be restricted by, amongst others, contractual terms, employment law, intellectual property law (including copyright), duties of care in negligence and fiduciary duties.

Data processors and controllers

1.67 The 1998 Act refers to data processors and controllers as well as joint controllers and controllers in common, but does not define them. These categories are far from easy to understand in practice. In a meeting with Timothy Pitt-Payne QC, he explained that identifying the relationship between partners can be very difficult for the parties. For example, it must be decided whether the situation involves controller, processor, joint controller, two controllers, or controllers in common. This raises question of responsibility and accountability and, in practice, identifies who must perform due diligence on security.[64]

Data controller

1.68 A data controller is defined in section 1(1) of the Data Protection Act 1998 as

[61] The leading case on confidentiality in the post-Human Rights Act era is *Campbell v MGN Limited* [2004] UKHL 22; [2004] 2 AC 457.

[62] See, for example, General Medical Council, *Confidentiality* (2009).

[63] Consultation Paper, paras 3.65 to 3.100.

[64] Consultation meeting no 38 – Timothy Pitt-Payne QC, 11 King's Bench Walk Chambers.

> a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Section 1(1) must be read in the light of section 1(4) which provides:

> Where personal data are processed only for purposes for which they are required by or under any enactment to be processed, the person on whom the obligation to process the data is imposed by or under that enactment is for the purposes of this Act the data controller.

1.69 There is no definition in the Act or in the Data Protection Directive of a joint controller or a controller in common. The Information Commissioner's Guide to Data Protection says

> In relation to data controllers, the term "jointly" is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term "in common" applies where two or more persons share a pool of personal data that they process independently of each other.[65]

1.70 The Information Commissioner's Guide provides two examples. In the first example, a network of town-centre CCTV cameras is operated by a local council jointly with the police. Both are involved in deciding how the CCTV system is run and what the images it captures are used for. The council and the police are joint data controllers in relation to personal data processed in operating the system. In the second example, a government department sets up a database of information about every child in the country. It does this in partnership with local councils. Each council provides personal data about children in its area, and is responsible for the accuracy of the data it provides. It may also access personal data provided by other councils (and must comply with the data protection principles when using that data). The government department and the councils are data controllers in common in relation to the personal data on the database.

1.71 Rosemary Jay points out in her text book, *Data Protection Law and Practice*, that the guidance does not address circumstances where there is split determination, so that, for example, one party determines the purpose of the processing and the other determines the manner.[66]

Data processor

1.72 A data processor is defined, in relation to personal data, as

> any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

1.73 In order for a public or private body to be a data controller, they must determine both the purposes for which the data are processed and the manner in which

[65] Information Commissioner's Office, *Guide to Data Protection*, para 24. The guide is available at: http://ico.org.uk/for_organisations/data_protection/the_guide (last visited 1 July 2014).

[66] R Jay, *Data Protection Law and Practice* (4th ed 2012).

they are processed. The extent of control will determine whether the body is a controller, rather than a processor. The Information Commissioner's Guide to Data Protection says

> … We take the view that having some discretion about the smaller details of implementing data processing (ie the manner of processing) does not make a person a data controller… So, when deciding who is a data controller, we place greatest weight on purpose – identifying whose decision to achieve a "business" purpose has led to personal data being processed.[67]

1.74 The Information Commissioner goes on to provide by way of example a scenario described to us in consultation by Birmingham City Council. The Commissioner says

> A Government department decides to help people in fuel poverty (the broad purpose). It also decides to use benefit records, which are clearly personal data, to identify who it will target (arguably, the broad manner). It then commissions a private-sector company to do certain matching according to clear criteria, but allows the company to use some discretion in deciding how they do this (eg what software to use). In this example, the department would be the data controller and the company would be a data processor, even though it decides the details of the processing method.[68]

Human Rights Act 1998 and the European Convention on Human Rights

1.75 Data protection is not specifically provided for in the European convention on Human Rights, but is protected under Article 8, as part of the qualified right to respect for private and family life, home and correspondence. A decision-maker must consider whether information-sharing will breach a person's right to privacy and family life and whether any such breach is justified in that it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing 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.[69]

DEVELOPMENTS IN DATA SHARING LAW AND PRACTICE

Policy initiatives and guidance

1.76 In addition to the Information Commissioner's Data Sharing Code of Practice, published in May 2011, and other Information Commissioner's Office guidance, consultees have told us of a large number of government reviews and initiatives to improve data sharing between public bodies. These include the Caldicott *Information Governance Review* in 1996-7 and Caldicott II *To Share or Not to*

[67] Information Commissioner's Office, *Guide to Data Protection*, para 28, available at http://ico.org.uk/for_organisations/data_protection/the_guide (last visited 1 July 2014).

[68] Information Commissioner's Office, *Guide to Data Protection*, para 29, available at http://ico.org.uk/for_organisations/data_protection/the_guide (last visited 1 July 2014).

[69] Human rights law is discussed in more detail in ch 3 below.

Share in 2013 in health, the Thomas Walport Review and unsuccessful data sharing provisions in the Coroners and Justice Bill 2009, and more targeted data sharing initiatives, such as the Multi Agency Information Sharing Hubs trialled in Leicestershire County Council. The Government has recently established a Data Sharing Centre of Excellence to support the development of best practice. The Department for Work and Pensions is responsible for a successful cross-government scheme, run by local authorities called *Tell Us Once*. This scheme allows the registration of a birth or death to trigger automatic disclosure to other agencies, with consent. A full list of the initiatives referred to in consultation responses may be found in Appendix C to this report.

1.77 The Coroners and Justice Bill was a significant and unsuccessful attempt to reform the law of data sharing. In 2009, the Government of the day proposed wide powers for Ministers to create statutory gateways by way of subordinate legislation, without full scrutiny by Parliament. Significant privacy concerns were raised and the opposition in Parliament eventually resulted in the proposals for a wide statutory gateway being withdrawn.[70]

1.78 The sheer number and frequency of such projects has not always benefitted clarity and understanding of the law. There is confusion about what effect each has. Many overlap or may even cancel each other out. Policy development in this area should be rationalised and clear principles agreed. A better system should be developed for ensuring that guidance is pitched at the right level of detail and complexity, as well as to the right audience.

Current law reform projects

1.79 The world has not stood still during the period of our review. There are constant developments in data sharing law and practice and some significant changes are expected. At the time of writing, negotiations on a draft European Union Regulation and Directive are ongoing. In addition, the Cabinet Office has been developing proposals for primary legislation.

Domestic law reform

1.80 The Government is developing policy on how to reform certain areas of law on data sharing. This work is divided into three areas: research and statistics; creating tailored public services for individuals; and fraud and debt. The research and statistics reforms could provide the Office for National Statistics with alternatives to the census; allow the Office for National Statistics to access data from a range of public authorities where the power to share data does not currently exist; and provide new opportunities to share sets of linked data with trusted third parties for the purposes of research.[71] The second strand involves the creation of a permissive power to share data between defined public agencies for the purpose of improving the delivery or targeting of public services. The final strand aims to permit specified organisations to share information for the purposes of the prevention, detection, investigation and pursuance of fraud,

[70] Legislative Scrutiny: Coroners and Justice Bill, *Report of the Joint Committee on Human Rights (2008-09)*, HL 57, HC 362.

[71] Anonymised data and data sharing for research purposes are discussed in ch 6 below.

error and debt.[72]

Draft European Union Data Protection Regulation

1.81 The draft European Union Data Protection Regulation arose from a review of the 1995 European Union Data Protection Directive. In January 2012, the European Commission proposed a comprehensive reform of the European Union's data protection rules, promising to strengthen online privacy rights in response to technological developments and globalisation. The European Commission also wanted to create a single law to do away with the fragmentation and administrative burdens it saw as resulting from differential implementation of European Union law in the various member states, with the intention of boosting the digital economy of Europe.[73]

1.82 A draft compromise text of the Data Protection Regulation was agreed by the LIBE (Civil Liberties, Justice and Home Affairs) Committee of the European Parliament in autumn 2013 and then approved by the full plenary of the European Parliament in a vote on 12 March 2014.[74] However, the text of the instrument has yet to be agreed by the Council. There are significant issues still to be resolved. One of the controversial proposals is that a single decision-maker in one member state should determine transnational data protection cases (a "one-stop shop"), rather than each national regulator having jurisdiction.

1.83 The UK Government has expressed concerns about increased red tape and

[72] Information about the Cabinet Office's open policy process, engaging with UK Government and civil society is available at: http://datasharing.org.uk/ (last visited 1 July 2014). Current projects include the Department for Communities and Local Government's Troubled Families Programme (https://www.gov.uk/government/policies/helping-troubled-families-turn-their-lives-around) (last visited 1 July 2014), discussed later in this paper, and the Department for Energy and Climate Change's steps to tackle fuel poverty, implementing recommendations made in John Hill, *Getting the Measure of Fuel Poverty*, Centre for Analysis of Social Exclusion, London School of Economics and Political Science (March 2012) available at: https://www.gov.uk/government/publications/final-report-of-the-fuel-poverty-review (last visited 1 July 2014). This independent review of fuel poverty was promised in the Government Spending Review of October 2010: https://www.gov.uk/government/publications/spending-review-2010 (last visited 1 July 2014).

[73] Council of the European Union, Proposal for a regulation 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 (General Data Protection Regulation), Essential elements of the one-stop-shop mechanism, Brussels 4 December 2013: http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%20170 25%202013%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F1 3%2Fst17%2Fst17025.en13.pdf (last visited 1 July 2014). The original draft Regulation and supporting documents may be found at: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm (last visited 1 July 2014). A number of competing drafts of the Regulation have been published since that time, including the European Parliament's draft and the most recent draft before the European Council. The European Union press release may be found at: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/139938.pdf (last visited 1 July 2014).

[74] The draft as approved by the European Parliament on 12 March 2014 may be found at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last visited 1 July 2014).

increasing burdens on small businesses.[75]

1.84 The European Commission describes the key aims of the Regulation to be:

(1) A single set of rules on data protection, valid across the European Union with the aim of removing administrative requirements, such as notification requirements for companies.

(2) Increased accountability.

(3) Instead of the current obligation of all companies to notify all data protection activities to data protection supervisors – a requirement that has led to unnecessary paperwork and costs businesses €130 million per year – the Regulation provides for increased responsibility and accountability for those processing personal data. For example, companies and organisations must notify the national supervisory authority of serious data breaches as soon as possible (if feasible within 24 hours).

(4) That organisations will only have to deal with a single national data protection authority in the European Union country where they have their main establishment. Likewise, people can refer to the data protection authority in their country, even when their data is processed by a company based outside the European Union. Wherever consent is required for data to be processed, it is clarified that it has to be given explicitly, rather than impliedly.

(5) That people will have easier access to their own data and be able to transfer personal data from one service provider to another more easily (right to data portability). This is intended to improve competition among services.

(6) A "right to be forgotten" which will help people better manage data protection risks online: people will be able to delete their data if there are no legitimate grounds for retaining it.

(7) That European Union rules must apply if personal data is handled abroad by companies that are active in the European Union market and offer their services to European Union citizens.

(8) That independent national data protection authorities will be strengthened so they can better enforce the European Union rules at home. They will be empowered to fine companies that violate European Union data protection rules. This can lead to penalties of up to €1 million or up to 2% of the global annual turnover of a company.[76]

1.85 The Draft Regulation is likely to have an impact on the vast majority of organisations and businesses in the European Union, as well as many located

[75] The Prime Minister's concerns have been widely reported. See for example Financial Times, *Victory for tech giants on EU data laws,* 25 October 2013.

[76] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last visited 1 July 2014).

outside of the European Union, requiring increased resources to prepare for the forthcoming changes to data protection and privacy compliance.

1.86 Together with a proposed police and criminal justice directive, the Draft Regulation forms the European Commission's revised data protection framework proposal, which is intended to replace current data protection laws across the European Union with a single regulation.

Draft European Union Directive

1.87 A new police and criminal justice directive will apply general data protection principles and rules for police and judicial cooperation in criminal matters. The rules will apply to both domestic and cross-border transfers of data. The directive is still in the early stages of its development. In March 2014, the European Parliament formally adopted the draft directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities[77]

REFORM OF THE DATA PROTECTION ACT 1998?

1.88 Consultees raised several issues relating to the Data Protection Act regime, including issues of clarity and interpretation. A full review of the Data Protection Act 1998 would be outside the scope of this project, because it is a transposition of European Union Law under the 1995 Data Protection Directive. Any new European Union data protection regulation or directive will impact on the law in the United Kingdom, but is unlikely to change fundamentally the law on when data can be disclosed and to whom. The developing European Union framework provides a good opportunity to review the law on data sharing in the United Kingdom, in time to take into account any changes in European Union law before they come into effect.

1.89 There are two areas in the Data Protection Act 1998 which could benefit from review. These are the enforcement mechanisms, in particular the framework for issuing monetary penalties, and the lack of controls on the processing, including sharing, of anonymised information. Consultees also raised questions about the meaning of the term “necessary” where necessity is a requirement under the data protection principles in the 1998 Act. Consideration could usefully be given to clarifying this.

1.90 Any full law reform project would be conducted within the limits of European law, and the development of recommendations would take into account developing European Union law in the form of the draft Regulation as well as any relevant Directive.

THE INTERNATIONAL TRANSFER OF DATA

1.91 Data sharing involving public bodies can have wider cross-border components. This results partly from globalised trade and industry and partly from the nature of

[77] The draft Directive may be found at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:HTML (last visited 1 July 2014).

cloud computing and global IT communication systems.[78] The current data protection regime permits processing within the European Union and allows the transfer of personal data outside the European Union in defined circumstances.

1.92 However, some of the programmes that seek to facilitate transfer outside the European Union have come under criticism, such as the "safe harbor program" in the United States.[79] There are also questions about the ability of public bodies outside the United Kingdom to require information to be disclosed or to access servers and other computer systems.[80] There may be limits on the ability of UK public bodies to prevent the use of servers based in the European Union where they contract with private service providers, particularly as a result of the freedom of services rules in the European Union and European Union procurement law. This is increasingly significant as a large proportion of public services are performed by private service providers.

1.93 Any reform project should take into account these developments and how they might impact on the project, though we do not recommend that international data transfer should fall within the scope of the project.

THE MEANING OF "DATA SHARING BETWEEN PUBLIC BODIES"

1.94 The Scoping Consultation Paper was entitled *Data Sharing Between Public Bodies*. A number of consultees pointed out that "data sharing" is a misleading label for the practices with which we are concerned. The term "data" is perceived to have a narrower meaning than "information". The Data Protection Directive and Data Protection Act 1998 are only concerned with information relating to an individual, which is processed, or intended to be processed, wholly or partly by automatic means, such as a computer, or information which forms part of, or is intended to form part of, a 'relevant filing system'. Information is a wider term which describes more accurately what is transferred under the provisions that we have reviewed. The phrase "data sharing" can produce a disproportionate focus on data protection law, which is only one of several important applicable strands of law. The term "sharing" suggests a two-way process of exchange or pooling of information.[81] The phrase "data sharing" also has a demonstrated negative effect on public confidence.[82]

1.95 The London Fire Brigade, for example, criticised the term "data sharing" for

[78] For a discussion on the issues raised by the storage of information on the internet in cloud services, see W Kuan Hom, Christopher Millard and Ian Walden, "The problem of 'personal data' in cloud computing: what information is regulated?—the cloud of unknowing", (2011) 1 *International Data Privacy Law* 211 to 228.

[79] The "Safe Harbor Program" is a certification process for companies in the United States to demonstrate that they comply with "Safe Harbor Principles" mirroring the data protection principles under the 1995 Directive. This enables the transfer of data which would otherwise be prohibited by the Directive as a transfer to a third country.

[80] For example, if information is stored on a server located in France, French law could determine which French bodies can require that information.

[81] For a discussion of the distinction between data and information, see Rob Wilson, James Cornford, Sue Baines and John Mawson, "New development: Information for localism? Policy sense-making for local governance" (2011) *Public Money and Management* 295, 296, citing John Seely Brown and Paul Duguid, *The Social Life of Information* (2000).

[82] Consultation response no. 18 – Marion Oswald, University of Winchester.

obscuring important differences between four different types of disclosure:

(1) Non-personal data;

(2) Personal data where full consent to disclose has been given;

(3) Personal data without direct consent, shared in a one-off unique situation;

(4) Personal data without direct consent, shared as a routine (automated).

1.96 The scope of our research was originally limited to disclosure "between public bodies". It soon became clear that to draw a distinction between public and private bodies is not always appropriate. Publicly funded functions are often delivered by a range of different organisations, including public bodies, limited or public companies, social enterprises and staff co-operatives. In housing, local authorities still provide some social housing, but a local authority may also discharge a duty to house by offering suitable housing association or private rented accommodation, or the housing services may be delivered by co-operative or mutual service delivery organisations, which are subsidiaries of the local authority.[83] Rent for any of these may be paid by housing benefit. In the health sector, private firms such as Virgin Health provide urgent health care centres at some hospitals, GP co-operatives at others, and the local NHS hospital trust at others. In education, there are private schools, free schools, academies and community schools. Concerns have also been expressed more widely that changing public service delivery models may undermine existing statutory schemes concerning information disclosure.[84]

1.97 Each of these organisations may collect data on its service users and each may be a data controller, in the terms of the Data Protection Act 1998, not merely a data processor.[85] It is not, however, always clear which body is a controller or processor and therefore who is responsible for ensuring appropriate measures are in place to protect data. If data are to be gathered in order to prevent harm, assess and improve service delivery and account for public expenditure, information will have to be provided by all of these types of organisation.

1.98 Consideration might also be given to whether controls on data sharing should be the same for public and private organisations, depending upon what sort of

[83] Information on the Government's policy on mutualisation and discussions on it may be found in the reports by and evidence submitted to the House of Commons Communities and Local Government Select Committee on Mutual and Co-operative approaches to delivering local services at: http://www.parliament.uk/business/committees/committees-a-z/commons-select/communities-and-local-government-committee/inquiries/parliament-2010/co-op-council/ (last visited 1 July 2014). The inquiry report was published in November 2012 and Government responded in April 2013.

[84] Concerns were voiced by the Public Accounts Committee in relation to the Freedom of Information Act 2000 and transparency: http://www.publications.parliament.uk/pa/cm201012/cmselect/cmpubacc/1201/120102.htm (last visited 1 July 2014). The Campaign for Freedom of Information has recently called for a Freedom of Information (Contractor Information) Bill: http://www.cfoi.org.uk/2014/06/mps-urged-to-bring-contractors-information-under-foi-act/ (last visited 1 July 2014).

[85] The terms "data processor" and "data controller" come from the Data Protection Act 1998 and are briefly explained under the heading "Current law" above.

information is being shared and for what purpose. If, for example, sharing is in the public interest, should a private company be able to refuse to disclose the information on the grounds that it is commercially sensitive? If a private company wishes to share, in return for payment, information gathered in the course of providing a public service, do the principles in the Data Protection Act 1998 provide adequate protection, or should the company be required to find a legal power to share the information in the same way that a public body would? These are questions that we think require further consideration in order to meet the changing models of service delivery.

ISSUES OTHER THAN THE LAW

1.99 Problems with the law only provide a partial explanation of why public bodies and the individuals working within them do not disclose information to each other when they have the legal power to do so, or do disclose when they do not have the necessary power. In consultation, we heard of many issues relating to incentives and disincentives and these are discussed in Chapter 7: "Problems other than the law".

1.100 The Information Commissioner's Office observed in its consultation response that although there seems to be "a fairly widely held belief that data sharing is being prevented by a defect in the law" the experience of the Information Commissioner's Office was that the problems were "generally cultural, based on a misunderstanding of what the law does allow or the result of inter-organisational distrust, budgetary restraints, incompatible IT systems and so forth".[86] Although we accept the role that management and training must play in data sharing, misunderstanding and confusion about what the law requires can also point to a need to simplify or codify the law to address its complexity and make it more accessible to practitioners.

1.101 Any effective solutions to the problems of data sharing must include an understanding of how the relationships between the individuals and organisations concerned work best. The investigation should also include consideration of "soft law" solutions such as codes of practice, as well as advice and guidance, training of front line staff, and ways of sharing best practice and management of data sharing between public bodies.

1.102 A great deal of work is already being carried out to improve best practice and understanding of systemic data sharing issues: by the Information Commissioner's Office through the creation of the Data Sharing Code; by the Independent Information Governance Oversight Panel led by Dame Fiona Caldicott and through the creation of the National Health Service Information Governance Toolkit; by local authorities such as Leicestershire County Council, which is being developed through the establishment of the Government's Centre of Excellence for Information Sharing; by organisations such as the United

[86] Consultation response no. 21 – Information Commissioner's Office.

Kingdom Anonymisation Network, and by academics.[87]

1.103 Law reform alone will not provide the necessary solutions, but law reform can work together with and assist changes in culture and practice, for example by developing structures which facilitate good and flexible working relationships in local areas.

SUMMARY OF OUR FINDINGS

1.104 We have come to the conclusion that there are both unnecessary obstacles to useful and legitimate data sharing and a lack of a clear and principled approach to proper safeguards for privacy. There is also a lack of transparency. Some of the obstacles stem from the law, and some from other sources, such as institutional attitudes, and incentives or disincentives to share.

1.105 There are too many statutory "gateways"[88] designed to meet a specific, and sometimes time-limited, need. Sometimes when a new project arises, a new gateway is enacted to facilitate it, whether or not it is legally required. Some gateways are narrow, others broader; some mandatory, others permissive; some express, others implied; some include limitations on onward sharing or use, others do not.[89] In some cases, there are several gateways through which the same bodies might make the same disclosure. The restrictions attached to the gateways and the penalties available are not always consistent.

1.106 Public bodies prefer to use a narrow, specific gateway rather than to rely on wide statutory (such as the Localism Act 2011)[90] or common law powers, even if these provide the powers required. However, the current law is complex and difficult to understand, allowing inconsistent interpretations sometimes inspired by the incentives or culture of the decision-making body. This often results in a narrow interpretation of powers or obligations to disclose data to others, but a wider interpretation of the powers or obligations of others to share data with one's own organisation.

1.107 These gateways are spread across a number of pieces of legislation, making them difficult to find and to interpret. For example, there are over 60 statutory gateways permitting the Department for Work and Pensions to disclose information to others, and far more provisions governing the onward sharing and use of information disclosed by the Department. These gateways are found in over 20 separate pieces of legislation. This contributes to a widespread lack of

[87] See, for example, the work of Dr Rob Wilson, Professor Mike Martin of Newcastle University and others on the importance of understanding relationships in developing effective information sharing: Dr Rob Wilson, Gregory Maniatopoulos and Ian McLoughlin, "Innovating Relationships: Taking a co-productive approach to the shaping of telecare services for older people" (2012) *Information, Communication and Society* 1; and the development of the Northumbria University postgraduate degree in information law rights and practice, together with the Ministry of Justice; and the work of the University of Winchester's Centre for Information Rights.

[88] The meaning of a "gateway" is discussed under the heading "current law" above at paras 1.35 to 1.44.

[89] Consultation Paper, ch 4 describes the various types of power to share information and gives examples of each.

[90] Section 1 of which empowers a local authority to do anything that individuals generally may do.

knowledge and understanding on the part of staff of public bodies of the circumstances in which information may be disclosed, to whom and for what purposes.

1.108 Most gateways are permissive, not mandatory. Permissive gateways leave a discretion whether or not to disclose information with the body that holds it, in circumstances in which the body may have no or insufficient incentive to disclose. The recipient may have a real and legitimate need for the information, but no power to require disclosure. We need to explore the creation of obligations to disclose and the issues this might produce.

1.109 There are significant concerns about data security. The Government may use data for purposes the subject would not want, and individuals fear detrimental action on the basis of data the subject does not know Government – or a particular arm of Government – has. There is the risk that staff might leak data, for example by mislaying data disks or laptop computers in public places, or might unlawfully pass it to another, or that the Government's IT systems might be unlawfully accessed or make errors. Any review of information disclosure must address data security concerns, and consider appropriate safeguards, protection, prevention, deterrence and enforcement action.[91]

1.110 For example, the Data Protection Act 1998 operates a "binary" approach to the classification of data, with rigid concepts of "personal" and on the other hand "anonymised" data. The eight data protection principles which the Act applies to the processing of personal data do not apply at all to anonymised data. This accords with the 1995 Data Protection Directive.[92] Since the decade in which those instruments were drafted, technological advances have made it increasingly difficult to protect the subjects of anonymised data from being re-identified whilst at the same time supplying sufficient information to make a dataset useful. For example, a set of data on the outcomes of treatment for heart disease treated at a particular hospital is likely to be much more useful if the data include matters such as age, body weight, socio-economic data, ethnic background, other diseases or relevant medical interventions.

1.111 In order to provide richer data without revealing the identity of individuals, personal data may be pseudonymised or coded, allowing data to be considered at an individual level but without identifying the person concerned. However, the more information that is provided about an anonymous or pseudonymised individual, the easier it becomes to detect their real identity by comparing the dataset supplied with other datasets. Modern rapid data processing techniques make such comparisons increasingly easier and cheaper to perform. The UK Anonymisation Network and the Information Commissioner's Anonymisation Code recommend that anonymity be seen as a sliding scale of risk management, not a binary construct.[93] A possible objective for the law might be to provide appropriate tests to ensure that anonymised and pseudonymised data are

[91] See for example *Database State* (2009) a report commissioned by the Joseph Rowntree Reform Trust after Her Majesty's Revenue and Customs lost two discs containing a copy of the entire child benefit database in October 2007.

[92] Data Protection Directive 95/46/EC, Official Journal L 281 of 23/11/1995 p 31.

[93] Information Commissioner's Office, *Anonymisation: Managing Data Protection Risk Code of Practice* (November 2012).

sufficiently secure for the sensitivity of the data concerned. The law should provide appropriate safeguards against the possibility of re-identification, as well as appropriate penalties to deter, and remedies in the case of, re-identification.

1.112 Information technology is continuing to develop rapidly. We cannot predict what technology might be able to do in 10 years' time, nor indeed where public opinion might then rest. The public's use of information technology and the voluntary publication of personal information have developed significantly in recent years with the development of social and professional networking online. Any review must develop an approach which caters as far as possible for changes in technology and takes account of the proliferation of publicly available personal information, some of it made available voluntarily.

DEVOLUTION AND A TRIPARTITE PROJECT

1.113 Data sharing raises issues in Scotland and Northern Ireland as it does in England and Wales. Data sharing poses issues in areas of Scots law, in areas of delegated responsibility and in reserved matters. Data sharing necessarily occurs across territorial boundaries within the United Kingdom.

1.114 This scoping project has been conducted by the Law Commission of England and Wales. The Scottish and Northern Irish Law Commissions have been informed of the project and the devolved administrations have been invited to contribute to the consultation process.

1.115 Any full law reform project should, we consider, be conducted as a tripartite joint project by all three Law Commissions.

Differences in powers to share data

1.116 Both Scotland and Northern Ireland have a similar multitude of legislative gateways for information disclosure and use as England and Wales. But the devolved legislatures and administrations lack the common law powers and inherent powers of Crown Ministers and the Westminster Parliament. There are also some additional information disclosure duties to strengthen accountability to devolved executives and legislatures. This has an impact on the necessary scope and role of express and implied statutory powers of the executives to share data.

1.117 Scotland has a variety of individual gateways. Scotland, like England and Wales, has permissive gateways, including those permitting sharing for the purposes of another body's functions.[94] There are also powers to make regulations for the provision of information and wrongful disclosure offences to support controls on information use and disclosure.[95]

1.118 Our research suggests that the Scottish Parliament has enacted a higher proportion of mandatory gateways than in England and Wales. There may be differences of approach to investigate and consider, in particular the role of information disclosure duties to support accountability to Scottish Ministers and

[94] See, for example, Public Health (Scotland) Act 2008, s 117; Charities and Trustee Investment (Scotland) Act 2005, s 24.

[95] See, for example, Climate Change (Scotland) Act 2009, s 79; Water Industry (Scotland) Act 2002, s 62; Fire (Scotland) Act 2005, s 32.

the Scottish Parliament.

1.119 There are duties to provide information triggered by order,[96] requirement[97] or applying a reasonable requirement test.[98] There are duties of the Scottish Ministers to collect certain information from local authorities.[99] There are duties to provide information collected following all necessary inquiries in relation to certain child safeguarding powers to a principal reporter.[100] Listed public bodies have a duty to provide information on the exercise of their functions to the Scottish Parliament.[101] There is a broad duty to share advice and support service information.[102] There is also provision, in some gateways, for a third party to determine the duties of public bodies under a test of reasonable requirement of information.[103]

1.120 Similarly, Northern Ireland has a variety of purpose-based permissive gateways,[104] mandatory powers to require information,[105] duties to cooperate including information sharing provisions,[106] and other controls on the use of information backed by wrongful disclosure offences.[107]

1.121 The powers of public bodies, and therefore the scope of implied gateways, are also likely to differ in important ways affecting data sharing. For example, the broad power under section 1 of the Localism Act 2011 only extends to England and Wales.[108]

Sharing across administrations

1.122 The United Kingdom government has many powers to disclose information to bodies in Scotland and Northern Ireland. Any full review of data sharing gateways

[96] Post-16 Education (Scotland) Act 2013, s 20.

[97] Transport (Scotland) Act 2005, s 18.

[98] Police and Fire Reform (Scotland) Act 2012, s 84.

[99] Housing (Scotland) Act 2010, s 145.

[100] Children's Hearings (Scotland) Act 2011, s 60.

[101] Public Services Reform (Scotland) Act 2010, s 32.

[102] Patient Rights (Scotland) Act 2011, s 19. Advice and support information is information about the organisation, procedures and specific services of a relevant body and such other relevant matters as providers of the patient advice and support service may reasonably request.

[103] See, for example, Flood Risk Management (Scotland) Act 2009, s 44.

[104] See, for example, Marine Act (Northern Ireland) 2013, s 8; Commissioner for Older People Act (Northern Ireland) 2011, s 20(2); Charities Act (Northern Ireland) 2008, s 24.

[105] See, for example, Inquiry into Historical Abuse Act (Northern Ireland) 2013, s 9; Assembly Members (Independent Financial Review and Standards) Act (Northern Ireland) 2011, s 8.

[106] See, for example, Safeguarding Board Act (Northern Ireland) 2011, s 10(3).

[107] See, for example, Goods Vehicles (Licensing of Operators) Act (Northern Ireland) 2010, s 46; Rates (Amendment) Act (Northern Ireland) 2009, s 10.

[108] Localism Act 2011, s 239.

will have implications for those data flows.[109]

Devolved matters

1.123 Data protection is reserved to the United Kingdom Parliament. However, in a number of devolved areas, such as social care, data sharing in relation to that area is within the powers of the devolved administration, subject to the Data Protection Act 1998.

1.124 Powers to share data concern all areas of administrative action, as they concern the machinery for government. Any full review will therefore fall across many areas of the legislative competence of the Scottish Parliament, Welsh Assembly or Northern Ireland Assembly.[110] For example, local government, public administration, education and training and social welfare are all devolved in Wales.[111] In relation to Scotland, a broad range of the scope of a Law Commission data sharing project would not be limited to matters reserved to the UK Parliament.[112] In Northern Ireland, as examples, health, education and social services are all devolved.[113]

Judicial review in relation to data sharing in Scotland

1.125 Scots law of judicial review does not make the same rigid distinction between public and private bodies as in England and Wales. In Scotland, the test for whether judicial review is available is that set out by Lord Hope in *West v Secretary of State for Scotland*. A "tripartite test" is applied, identifying the decision-maker, the person affected and the body which conferred the decision-making power. As Lord Hope explained:

> (a) The Court of Session has power, in the exercise of its supervisory jurisdiction, to regulate the process by which decisions are taken by any person or body to whom a jurisdiction, power or authority has been delegated or entrusted by statute, agreement or any other instrument.
>
> (b) The sole purpose for which the supervisory jurisdiction may be exercised is to ensure that the person or body does not exceed or abuse that jurisdiction, power or authority or fail to do what the jurisdiction, power or authority requires.

[109] For example, the Construction Products Regulations 1991, regs 24 to 25 allow Her Majesty's Revenue and Customs to disclosure indirect tax information to any district council in Northern Ireland for given purposes; the Commissioner for Children and Young People (Scotland) Act 2003, s 9 allows Her Majesty's Revenue and Customs to disclose certain information to the Commissioner for Children for Scotland when required to do so by the Commissioner.

[110] Scotland Act 1998, s 29; Government of Wales Act 2006, s 94; Northern Ireland Act 1998, s 6.

[111] Government of Wales Act 2006, sch 7.

[112] Scotland Act 1998, sch 5.

[113] Northern Ireland Act 1998, s 4 and schs 2 and 3.

> (c) The competency of the application does not depend upon any distinction between public law and private law, nor is it confined to those cases which English law has accepted as amenable to judicial review, nor is it correct in regard to issues about competency to describe judicial review under Rule of Court 260B as a public law remedy.[114]

1.126 In addition, a petitioner in Scotland may seek an order for specific performance of a statutory duty, under section 45(b) of the Court of Session Act 1988.[115]

1.127 A full project would need to take full account of the ways in which Scottish judicial review might influence information disclosure differently from England and Wales, especially where service delivery is multi-sector.

Data sharing protocols

1.128 In Wales and Scotland, significant steps have been taken towards improving information sharing between public bodies, by introducing the Wales Accord on Sharing Personal Information and the Scottish Accord on Sharing Personal Information respectively.[116] The Welsh Deputy Minister for Social Services describes the Wales Accord as "a practical and tested consent-based approach to multi-agency sharing for all public service organisations". The Care Bill and Social Services and Well-Being (Wales) Bill both include duties to co-operate which have data sharing implications. The Information Commissioner's Office published guidance in the form of the Northern Ireland Information Sharing Agreement for multi-agency risk assessment conferences (MARAC) in December 2012. The value of these as precedents for England deserves to be considered, and this is best done by the Scottish Law Commission as well as ourselves.

OUTLINE OF THIS REPORT

1.129 This report is divided into 11 chapters in three parts.

Part 1: Presenting the issues

Chapter 1: Introduction

1.130 This includes a summary of the report, our conclusions and recommendations.

Chapter 2: When should personal information be disclosed?

1.131 This chapter considers the consultation responses on the issues raised in Chapter 2 of the Consultation Paper, on practical advantages of and principled

[114] *West v Secretary of State for Scotland* 1992 SC 385 (IH) at 412 to 413, 1992 SLT 636, reported as *West v Scottish Prison Service* 1992 SCLR 504.

[115] See Act of Sederunt (Rules of the Court of Session 1994) 1994, SI 1994 No 1443, r 58.3(1).

[116] The Wales Accord on the Sharing of Personal Information, supported by the Welsh Government, 4th version released May 2013, may be found at http://www.waspi.org/ (last visited 1 July 2014) and the Scottish Accord on the Sharing of Personal Information, first developed together with Fife Council, may be found at http://www.fife.gov.uk/topics/index.cfm?fuseaction=page.display&p2sid=10AE7B78-AD72-9AA9-D5D1D820E8120019&themeid=2B892409-722D-4F61-B1CC-7DE81CC06A90 (last visited 1 July 2014).

concerns about data sharing. Views differed as between, for example, public bodies wishing to make the disclosure of information easier in order to improve public service delivery, those with professional duties of confidentiality concerned about undermining patient-professional relationships, and lobby groups seeking to improve transparency, protect individual privacy and develop self determination in data control, based on consent.

Part 2: Problems under the current law

1.132 This part is divided into three chapters, examining problems in the current law.

Chapter 3: Overlapping legal regimes

1.133 This chapter considers the difficulty of working out which laws apply and which take precedence in a field where there are numerous overlapping legal regimes. These include the European Union Data Protection Directive 1995; the Data Protection Act 1998; express and implied statutory gateways; the common law, including private law rights of confidentiality; the Human Rights Act 1998, particularly with regard to Article 8 of the European Convention on Human Rights. Its obligations, and the balancing of interests required to reach a proportionate decision are important in this field and apply to all decisions made by bodies subject to the Human Rights Act 1998.

Chapter 4: Statutory gateways

1.134 Consultation responses on the existing morass of statutory gateways are discussed. These suggest that public officials dealing with information requests welcome specific gateways with controls on onward disclosure, because these tend to provide both clarity as to what information they may share and when, and also security of the data in the hands of the recipient. Such gateways can, however, operate as barriers to effective disclosure arrangements, as they are time bound, affect the interpretation of other powers, and tend to be interpreted restrictively. Permissive gateways also give control to the data discloser, who may have insufficient incentives to disclose to another where that disclosure furthers the recipient's purposes, rather than the discloser's. Lastly, statutory gateways are often held up as providing accountability as they have been scrutinised by Parliament, but research on Parliamentary debates suggests that they can receive very little scrutiny.

Chapter 5: Common law powers

1.135 Consultees' views on the common law powers of government departments to disclose data are considered, along with their erosion by statute. This chapter looks at the changing approach to the "third source" of power, and what is sometimes called the "Ram Doctrine" (the proposition that government departments can do anything reasonably ancillary to their functions, but which has been interpreted at times as a proposition that government can do anything that a private individual can do, except where constrained by any public law restriction). Prerogative powers also exist, and may provide the power to share information in some cases.

1.136 This chapter also considers consultation responses on the private rights of confidentiality and the careful balance needed between maintaining the trust which confidentiality creates and deciding when it might be overridden by other

obligations to disclose data.

Chapter 6: Anonymised data

1.137 "Big data", "open data" and research data in an anonymous or pseudonymised form are discussed here. Consultees expressed great hopes for, and also concerns about, personal information presented in an anonymous or pseudonymised form. Data that are too limited in their scope may have adverse effects on research based on them, yet with more data the risk of re-identification becomes increasingly significant. The definition of data as "anonymous" may be inappropriately crude; rather there may be a sliding scale of risk of re-identification. Developments include the use of safe havens for the transfer of information.[117]

Chapter 7: Barriers other than the law

1.138 Consultees gave a number of important reasons affecting decisions on information disclosure, irrespective of the availability of legal powers. These are important factors to be borne in mind in considering how to improve data sharing. Such non-legal problems might also be capable of being alleviated by law reform.

Part 3: Data sharing in practice

1.139 Two case studies are examined in some detail to illustrate the variety of examples of data sharing powers of and restrictions on two large government departments: Her Majesty's Revenue and Customs, a statutory department; and the Department for Work and Pensions, a ministerial department. The Troubled Families Programme provides a third example of a different kind. This is a cross-government programme, which has encountered data sharing hurdles, illustrating the legal impediments in place and the imperfect solutions found.

Chapter 8: Her Majesty's Revenue and Customs

Chapter 9: The Department for Work and Pensions

Chapter 10: The Troubled Families Programme

Part 4: Next steps

Chapter 11: Developing solutions

1.140 This chapter concludes our scoping report. Initial ideas are discussed with a view to further exploration in a full review of the law on the transfer of information for public purposes; and the scope of such a review is proposed.

[117] Sometimes referred to as a safe setting or secure data access facility, safe havens are physical or virtual environments where access to identifiable data may be controlled. Identifiable data from two or more sources can be linked, matched or processed by authorised researchers within the secure setting, enabling anonymised data to be produced. See http://www.esrc.ac.uk/_images/ADT-Improving-Access-for-Research-and-Policy_tcm8-24462.pdf (last visited 1 July 2014).

CHAPTER 2
WHEN SHOULD PERSONAL INFORMATION BE DISCLOSED?

INTRODUCTION

2.1 In the Consultation Paper we described the advantages of and the risks and concerns surrounding data sharing.

2.2 Any decision to share information must be balanced against the importance of protecting individual privacy. Privacy, control over personal information and autonomy are closely related. They are central to a liberal democratic society. There are also concerns about the quality and security of data held by public bodies, problems which are compounded when information is disclosed to others.[1]

2.3 At its best, data sharing can benefit individuals, organisations and wider society. Improved information sharing can inform policy-making; improve public services; assist with emergency planning and response; and provide large evidence bases for the purposes of research. Wider sharing has the potential to offer significant efficiency savings to Government, and therefore, the public purse. Sharing could also improve transparency in public services. The lack of transparency is a key criticism of current data sharing practices.

2.4 Expressions of concern about data sharing do not necessarily deny the potential benefits, but express a concern that, even if the benefits are achieved, they come at a high cost. Data sharing can interfere with the right to privacy;[2] lead to increased publicity for individuals with risks of negative or prejudicial treatment; increase the risk of data loss and identity theft; create a fear of state intrusion upon individuals' lives; and undermine intimacy and people's ability to manage different social relationships themselves. There are also concerns about the quality and accuracy of data held by public bodies and the effect of the dissemination of inaccurate information.

2.5 The different concerns, approaches and considerations articulated to us in consultation are important; it is necessary to address them if any reform project is to be conducted successfully.

TRANSPARENCY, TRUST AND CONFIDENCE

2.6 Consultees emphasised that the concerns of members of the public about data sharing relate as much to the transparency of the data sharing process as they do to the precise nature of the data disclosed or the identity of the recipient. Many people's concerns are ultimately about both accountability and control.

2.7 In consultation, many organisations spoke of the importance of maintaining the

[1] Consultation Paper, ch 2.

[2] Whether expressed as "informational self-determination" or the "right to be left alone".

trust of the public.[3] This included trust in the protection of privacy and confidentiality, as the British Medical Association and others working in the field of health and social care emphasised.[4] If patients or social services clients do not trust their doctor or social worker, they will not feel confident in disclosing the information which is essential to treating them appropriately. Systems of health care and social services provision are based upon public trust, which could be extremely difficult to rebuild if lost.

2.8 At the time of writing, the Government's programme to create a central database of information gathered from data held by general practitioners has been challenged on the grounds, amongst other things, of its lack of transparency. It is argued that patients would not have sufficient information about to whom their personal information might be disclosed to and for what purposes.[5]

2.9 MedConfidential, Big Brotherwatch, Privacy International, Open Rights Group and others all emphasised the need to create greater transparency in data sharing systems: a person disclosing information to a professional needs, they told us, to know to whom the information might be passed and what they are going to use it for, to whom else the recipient might disclose the information and the purposes for which that further recipient might use it.[6] Concerns were also raised by local government consultees about the lack of proper audit trails and recorded reasons for information disclosure, reducing transparency.[7] A group of academic researchers suggested that more could be done to ensure individual procedural rights of notification of, objection to, and consultation in respect of proposed data sharing.[8]

2.10 Consultation indicated to us that there are a wide variety of public attitudes to data sharing and varying levels of public trust. Understanding the relationship between public trust and confidence and effective data sharing is an important part of developing workable reform. It is also an important consideration in striking the appropriate balance between privacy and the public interest. Many consultees discussed the importance of public trust and confidence and the difficulty of establishing effective data sharing in the face of a lack of public trust and confidence.

2.11 However, it can be difficult to identify and measure public attitudes and to be certain of what surveys and opinion polls reliably reveal about public opinion.

[3] For example, this was recorded by DAC Beachcroft in a series of seminars that they convened with stakeholders from the health and social care sector. Consultation response no. 49 – DAC Beachcroft Solicitors seminar.

[4] Consultation response no. 22 – British Medical Association.

[5] See the Health Select Committee's hearing on this project on 25 February 2014, shortly after the Government announced its decision to delay implementation of care.data in order to provide an opportunity to resolve widespread concerns: http://www.parliament.uk/business/committees/committees-a-z/commons-select/health-committee/news/14-02-25-cdd-ev/ (last visited 1 July 2014).

[6] Consultation meetings no. 32 – Open Rights Group, Privacy International, Mydex, MedConfidential.

[7] Consultation response no. 35 – Dr Ashley Savage, Dr Richard Hyde, Mr Jamie Grace and Ms Bansi Desai.

Studies of attitudes towards privacy show differences of attitude related to "culture, age, gender, and other demographic factors".[9] Reported levels of trust vary depending on whether an individual is asked whether public bodies should "collect and use" personal information or whether they should "share" personal information.[10] Use of the term "data sharing" appears itself to reduce public trust and confidence. Trust is fragile and easily undermined by breaches of data security.[11] Trust and confidence are also undermined where there is a perception that information is supplied for profit, even if the benefit goes to public services.[12] Polls suggest, however, that concerns about information sharing are rising.[13]

2.12 Although such studies are useful and informative, they are insufficient to establish whether a given set of proposals will attract and maintain the level of public trust and confidence required to ensure the proposals are effective. Open Rights Group explained in consultation that it is hard to second-guess public attitudes about data sharing or privacy.[14] We think this is a reason for full and widespread consultation on any reform proposals in relation to data sharing.

2.13 In summary, whilst the argument that there is a need for high levels of trust and confidence was frequently made to us in consultation, levels of trust and confidence are hard to verify empirically. There are also different forms of trust.

2.14 Individuals may have different attitudes as regards their trust in the overall system, trust in individual officials they deal with, trust in different institutions and trust in particular sectors, for example local government or the NHS. It is also difficult to measure in advance or predict the impact of particular proposals upon public trust and confidence. The relationship between trust and confidence and particular proposals is a complex one, sometimes affected by the presentation of

8 Consultation response no. 35 - Dr Ashley Savage, Dr Richard Hyde, Mr Jamie Grace and Ms Bansi Desai.

9 Ian Brown, "Privacy attitudes, incentives and behaviours" (2011) at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1866299 (last visited 1 July 2014).

10 University of Winchester, Centre for Information Rights, *Attitudes to Sharing Personal Data with the Public Sector*, http://www.winchester.ac.uk/academicdepartments/Law/Centre%20for%20Information%20Rights/Documents/Attitudes%20to%20Sharing%20Personal%20Data%20with%20the%20Public%20Sectorinfographic%20v1.pdf (last visited 1 July 2014).

11 University of Winchester, Centre for Information Rights, *Attitudes to Sharing Personal Data with the Public Sector*, http://www.winchester.ac.uk/academicdepartments/Law/Centre%20for%20Information%20Rights/Documents/Attitudes%20to%20Sharing%20Personal%20Data%20with%20the%20Public%20Sectorinfographic%20v1.pdf (last visited 1 July 2014).

12 University of Winchester, Centre for Information Rights, *Attitudes to Sharing Personal Data with the Public Sector,* http://www.winchester.ac.uk/academicdepartments/Law/Centre%20for%20Information%20Rights/Documents/Attitudes%20to%20Sharing%20Personal%20Data%20with%20the%20Public%20Sectorinfographic%20v1.pdf (last visited 1 July 2014).

13 Demos, *Private Lives: a People's Inquiry into Personal Information* (2010) p 21.

14 Consultation meeting no. 32 - Open Rights Group, Privacy International, MyDex, MedConfidential.

proposals and the reception of them by the media and civil society.[15] It is also not clear that all data sharing arrangements require comparable levels of public trust to function effectively; for example, those involving the use of pre-existing datasets or datasets where the collection of data is compulsory (for example vehicle licensing) can *function* without reliance upon public trust. A high level of trust may nonetheless be important in such cases, both in order to maintain public trust and confidence generally, to the benefit of other information sharing arrangements which are more dependent on public trust and confidence, or because maintaining the trust and confidence of citizens is important in itself in a democratic state.

2.15 Public trust and confidence is therefore an important consideration for reasons both pragmatic and of principle, and a consideration to which it is necessary to remain constantly alert in any law reform project in relation to data sharing.

INFORMING THE PUBLIC

2.16 There is, it seems to us, a perceived lack of transparency about sharing. Many consultees expressed the view that the public are not well-informed about data sharing practice and law.[16] We found that public bodies themselves are often not well informed on the topic. This is a recurrent problem. There is a need for a comprehensive mapping exercise to understand what powers actually exist and how they are used to share data. There is no comprehensive account of powers to share data either inside or outside of Government.

2.17 The Independent Information Governance Oversight Panel and others responded that many individuals are not currently well informed enough to express objections to the use of their information.[17] Other consultees responded that there was a need to inform and educate the public about data sharing. A group of academic researchers suggested that public education about the benefits of information sharing would both help to remedy the lack, they perceived, of public trust in public bodies and empower individuals to speak out about concerns.[18]

2.18 Some public bodies complained of public misconceptions and unfair stereotyping, which hinder proper debate about reform in this important area. Welwyn Hatfield Borough Council maintained that public bodies are unfairly stereotyped as untrustworthy and that poor public understanding plays a part in this. West Midlands Fire and Rescue told us that people falsely assume that data are already shared to greater extent than actually occurs. This view was reiterated by health service consultees.

2.19 The extent of public awareness is also important when considering the

[15] Although there is no agreed definition of "civil society", the term is widely used to encompass non-governmental organisations and others representing the interests of citizens. For a discussion of this term, see Mike Edwards (2005) "Civil society", The Encyclopedia of Informal Education, www.infed.org/association/civil_society.htm (last visited 1 July 2014).

[16] For example, consultation meeting no. 24 – Northumbria University Information Law Centre Conference attendees.

[17] Consultation response no. 65 – Independent Information Governance Oversight Panel.

[18] Consultation response no. 35 – Dr Ashley Savage, Dr Richard Hyde, Mr Jamie Grace and Ms Bansi Desai.

appropriate general approach to data sharing. For example, a system which is heavily dependent on individual consent requires a high level of public awareness and understanding to work effectively.

GETTING THE PRIORITIES RIGHT

2.20 In consultation, we sought to understand consultees' views on the appropriate prioritisation between the public interest in privacy and any public interest in disclosure. We asked:

> Do you think that the current law strikes the right balance between the ability of public bodies to share data and the need to protect privacy or other rights of data subjects?[19]

2.21 Most consultees regarded the law as allowing the correct balance to be struck if used appropriately. Disagreement about or misunderstanding of the law was, however, apparent in a large number of responses. Some consultees noted the difficulty of making complex balancing decisions in fast moving or dynamic situations, such as those experienced by the emergency services, and expressed a concern about the appropriateness of a system that required officials to do so.[20] Others expressed particular criticisms.

2.22 Health sector consultees and others, made the important point that it was wrong to portray the desirability of data sharing on the one hand, and privacy on the other, as opposing forces to be balanced. The reality was that the protection of privacy is very much in the public interest, as it gives individuals the confidence to provide information that is necessary to provide, plan and improve services. Appropriate and robust privacy protections should be at the heart of reforming the law applicable to data sharing. Privacy protection can improve effective data collection and use.[21]

2.23 Some consultees attributed an important role to consent. For example, the City of London Police Economic Crime Directorate stressed in a consultation meeting that they considered it important that UK policing is based upon consent. They expressed concern about the effect on trust and confidence in the police if obligations to share information were introduced. Others, including the Insolvency Service Intelligence Team and the Social Landlords Crime and Nuisance Group, argued in favour of a general presumption in favour of sharing accompanied by explicit exceptions. [22]

2.24 Some privacy advocates expressed concern in consultation that our consultation paper had taken too "organisation-centric" an approach to data sharing, focussing on the benefit of data sharing to organisations. We agree that it is vitally important to take into account individual rights and interests when considering data sharing. It is also important to consider organisational benefits. Individuals

[19] Consultation Paper, ch 5, question 6.

[20] See for example Fire and Rescue responses.

[21] For example, consultation meeting no. 20 – Health and Social Care Forum attendees.

[22] Consultation meeting no. 14 – City of London Police Economic Crime Directorate; consultation response no. 19 – The Insolvency Service; consultation response no. 29 – Social Landlords Crime and Nuisance Group.

have an interest in informed and effective government. We need to consult further on how to accommodate and reconcile both sets of interests.[23]

Failures to strike the right balance

2.25 Consultees gave a number of examples of failure to strike the right balance in data sharing. Some pointed, for example, to problems with the structure of the law that prevented some sharing that would be in the public interest.

2.26 Consultees told us that powers to disclose or require disclosure were sometimes in the wrong hands. Some consultees supported the introduction of mandatory disclosure in appropriate circumstances. The Office of National Statistics, for example, contrasted the law in England and Wales with that in Ireland, where there is an obligation to comply with a request from the Chief Statistician to disclose information.[24]

2.27 The Veterinary Medicines Directorate maintained that strict interpretation of the law can prevent sharing in the public interest. For example, the Directorate had been unable to disclose information about certain medicines for which a Special Import Certificate was granted because to do so would involve disclosing the personal details of vets. The information would have assisted the requesting body's understanding of the need for medicines and of related animal health issues in their area.[25]

2.28 Shropshire Fire and Rescue Service responded that the law did not strike the right balance, in giving insufficient weight to the provision of appropriate services and to intervention to prevent harm to individuals and organisations.[26] Sheffield City Council maintained that, in some cases, the public interest should override the protection of personal data.[27] It considered that people should not be able to hide behind anonymity to avoid meeting their responsibilities, for example in relation to debt or other legal duties.

2.29 Any legal framework should be sufficiently flexible to allow it to accommodate the demands upon, and resources of, a wide variety of types and sizes of organisation, including private sector providers of public services. Although non-governmental organisations are not subject to the same level of regulation, they vary enormously from the smallest charity assisting with the delivery of a publicly funded service to the largest multinational providers of services such as government information technology systems or prison security. A one-size-fits-all approach may be unsuitable.

ADVERSE CONSEQUENCES OF UNAUTHORISED DISCLOSURE

2.30 In consultation, we heard examples of failures leading to an unauthorised or unlawful disclosure of information. If information is disclosed when it should not

[23] Consultation meeting no. 32 – Open Rights Group, Privacy International, MyDex, MedConfidential.

[24] Consultation response no. 55 – Office for National Statistics.

[25] Consultation response no. 7 – Veterinary Medicines Directorate.

[26] Consultation response no. 6 – Shropshire Fire and Rescue.

[27] Consultation response no. 80 – Sheffield City Council.

be, there may be very serious consequences, including serious harm in some cases.[28] It is important that procedures seek to prevent unauthorised disclosures resulting in a disproportionate response from the relevant public body, such as a policy not to disclose becoming the default position or refusing to share without an unnecessarily high level of security.

2.31 More widely, many consultees identified the effects of unauthorised disclosures as being reputational loss, fines, potential criminal liability and an increase in anxiety about sharing and reluctance to share, sometimes with the effect that not sharing comes to be seen as a no-risk default option.

2.32 For example, the London Borough of Camden reported that formal sanctions, especially monetary penalties, inevitably have an adverse effect on sharing, especially in the context of requirements to make significant financial savings. Substantial fines have attracted significant press attention. This has created more focus on the risks than the benefits of sharing.[29]

2.33 Shropshire Fire and Rescue Service told us that the public have no confidence in information security, a situation which has been exacerbated by high profile reported cases of information security breaches, sanctions and information gathering stories in the media.[30] Most information providers, they maintained, adopt a "default" position of not sharing, since there is no sanction for refusing to share data. This leads to an inability to target and protect those most at risk, which in relation to the fire service has resulted in deaths.[31] A number of fire and rescue services also suggested that people can become reluctant to share information if they perceive that organisations are unable to manage information correctly.[32]

2.34 Organisations become more risk-averse and less willing to share within established information sharing frameworks following data security breaches. The public mistrust the capability of large organisations to manage personal data securely and are less willing to share personal data when requested.

2.35 A group of academic researchers explained that sanctions for unauthorised disclosure can reduce the confidence of whistle blowers so that they do not raise concerns. Over-sharing risk information can also over-stigmatise those seeking to engage with programmes of rehabilitation and reduce the effectiveness of those

[28] One example of a breach with the potential to cause serious harm we heard about in consultation was the inadvertent disclosure of current address information held by social services to an abusive ex-partner.

[29] Consultation response no. 37 – London Borough of Camden.

[30] Data sharing has been the topic of increased media scrutiny following HMRC data losses in 2008 and the disclosures and revelation by Edward Snowdon of information intelligence gathering by the United States of America's Central Intelligence Agency. See, for example the series of articles in The Guardian http://www.theguardian.com/world/the-nsa-files (last viewed 1 July 2014.

[31] Consultation response no. 6 – Shropshire Fire and Rescue.

[32] Consultation response no. 10 – West Midlands Fire and Rescue Service; consultation response no. 14 – East Sussex Fire and Rescue; consultation response no. 15 – Kent Fire and Rescue Service.

efforts.[33]

2.36 The Insolvency Service Intelligence Team responded that, although they had not had the experience of making an unauthorised disclosure, they feared that the experience would generate a greater degree of restriction on sharing as a matter of internal policy.[34] Perversely, 'not sharing' is too often regarded as the no risk default position. Sue Richardson noted that practitioners express a greater fear about the consequences, especially sanctions, of sharing inappropriately than of protecting inappropriately.[35]

2.37 The Independent Information Governance Oversight Panel expressed the view that anxiety within organisations about information sharing results from instructions issued by managers in an attempt to protect their organisation from fines for breaching data protection laws. This leads to a 'risk-averse' approach to information sharing, which prevents professional staff at the front line co-operating as they would like.[36]

IMPROVED PRACTICE FOLLOWING UNAUTHORISED DISCLOSURE

2.38 Some consultees also pointed to positive outcomes within organisations following sanctions for unauthorised disclosure. These included the raising of awareness within the organisation, encouraging due consideration of data protection in the future and ensuring robust systems are put in place.

2.39 For example, Somerset County Council responded that most instances of data protection breaches in the public sector were due to human error or bad practice by controllers.[37] It said that reputational damage and fines heighten awareness of the need for technical and administrative controls but should not affect appropriate data sharing. Cheshire Fire and Rescue agreed that high profile data losses have had a positive outcome in raising awareness of data security risks and requirements.[38] Wakefield District Council also responded that a positive effect of formal sanctioning is that it results in a heightened awareness of data security, helping to reinforce training and heighten awareness among staff about information sharing, safe data transfer and information security.[39] Birmingham City Council observed that the possibility of fines has meant that systems and processes are more likely to be in place and to be documented and recorded and that therefore a more robust approach to data sharing can be developed.[40]

[33] Consultation response no. 35 –. Dr Ashley Savage, Dr Richard Hyde, Mr Jamie Grace and Ms Bansi Desai. An example of this is the disclosure of risk information relating to mental health conditions. The stigma resulting from such a disclosure can either reduce the quality of service given in itself or, if the individual recognises a difference in treatment, undermine the provision of service where an individual becomes uncooperative.

[34] Consultation response no. 19 – The Insolvency Service.

[35] Consultation response no. 41 – Sue Richardson, University of Bradford.

[36] Consultation response no. 65 – Independent Information Governance Oversight Panel.

[37] Consultation response no. 1 – Somerset County Council.

[38] Consultation response no. 26 – Cheshire Fire and Rescue Service.

[39] Consultation response no. 50 – Wakefield Metropolitan District Council.

[40] Consultation response no. 69 – Birmingham City Council.

WHEN SHOULD INFORMATION BE SHARED?

2.40 In consultation, all those we spoke to expressed the view that there are some circumstances where personal information should be disclosed to a public body without the consent of the individual concerned. On the other hand, nobody we spoke to argued that personal information should be freely available to anyone, without any restrictions on disclosure or use. Within these limits, a wide range of views were expressed.

2.41 There are three broad categories of reason for wanting to disclose information to another public body:

(1) Reasons based on the need to share information to prevent harm to an individual or enable a body to make a decision relating directly to an individual;

(2) Reasons based on the need to share information to provide an identified and targeted public good or benefit;

(3) Reasons based on the need to share information to create a greater database of available information without an identified end use but in the belief that the database will later prove useful.

2.42 Consultees generally supported information sharing which could be shown to be proportionate to the purpose of preventing imminent harm to the individual concerned or another. Issues then arose over what should happen to that information once the harm had been averted. Most consultees also supported information disclosure for the purpose of making a decision directly related to the individual concerned, for example in order to provide a service or investigate a crime. However, some took the view that information should only be disclosed with consent.

2.43 The second category of information disclosure – for the purpose of providing an identified and targeted public good – was more controversial. Examples of information sharing in this category include carrying out clinical audits to measure the outcomes of particular medical practices in a hospital, or a local authority gathering information on vulnerable groups in order to decide where to target particular services over the next spending period.

2.44 The final group of reasons was the most controversial, but the line between gathering data for an identified purpose and for unspecified future use can become blurred. Information can be gathered for one purpose but then, particularly once matched, can clearly disclose something else, raising the question of how far it then becomes legitimate to use the information for a second purpose.

2.45 Information lawyer Rosemary Jay explained that the reasons given for information-sharing could be broadly divided into three categories: the sharing of information for clearly identified and defined purposes; the sharing of information where there is available evidence that it would be useful to do so for an identified and defined purpose; and finally instances where information sharing is sought for unclear or purely speculative potential benefits. Rosemary Jay cautioned that sharing personal information on a purely speculative basis may very likely pose a

threat to individual rights, and that the focus should be on identifying concrete needs that are currently unsatisfied and ensuring that decisions to share are evidence-based decisions. [41]

THREE APPROACHES TO INFORMATION SHARING

2.46 Attitudes expressed during the consultation reflected three broad models for approaching the regulation of data sharing issues: a consent based approach; a purpose-based approach and a risk-based approach. Many responses reflected a combination of more than one of these – hybrid models. We set these out approaches out and explore the questions they raise and problems associated with them below.

The consent-based approach

2.47 A consent-based approach holds that data sharing between public bodies is only acceptable where the individual to whom the information relates has consented to its disclosure. It advocates processes, controls and safeguards designed to ensure that the individual is in control of the information about them held by different public bodies and the uses to which it can be put.

2.48 A consent-based approach is most apparent in the law of confidentiality and in consent-based processing requirements under data protection law. A consent-based approach is very popular with members of privacy rights groups, some of whom are developing and using a notion of "informational self determination" to inform their approach.[42]

The purpose-based approach

2.49 A purpose-based approach holds that information should be shared between public bodies for a defined set of purposes and that controls and safeguards should be directed towards ensuring that sharing does not extend beyond those purposes. The purposes for which sharing is permitted may be various, defined in broad or narrow terms and relate to individual benefit, wider public interest, or good administration generally, including efficiency. Those three aims are themselves interrelated. For example, both providing services to individuals and ensuring efficient administration can be in the public interest.

2.50 A purpose-based approach can be seen in the drafting of express legislative gateways and is implicit in the logic of implied powers to share where doing so is incidental to the performance of a public function or duty.[43]

[41] Consultation meeting no. 17 – Rosemary Jay, Hunton and Williams LLP, in her personal capacity.

[42] The phrase "informational self determination" has its roots in a decision of the German Constitutional Court on the constitutionality of the 1983 Census: BVerfGe 65, 1. The decision has been extremely influential in the development of European data protection legislation. "Informationelle Selbstbestimmung" consists of the "capacity of the individual to determine in principle the disclosure and use of his or her personal data" subject to cases of overriding public interest. The concept was developed from the general right to personality under the German Basic Law.

[43] For a brief description of express statutory gateways, see ch 1, under the heading "Current law". For a fuller discussion, see ch 4 and examples in chs 8 and 9.

The risk-based approach

2.51 A risk-based approach would not seek to limit data sharing between public bodies to a set of purposes. Instead, it would permit the disclosure of information where risks associated with that disclosure fall below an acceptable level for the individual or individuals concerned by the disclosure. Controls and safeguards are directed towards confining the risk to individuals below the acceptable level.

2.52 A risk-based approach can be seen in the use of privacy impact assessments and approaches to the appropriate measures required by the seventh data protection principle.[44]

QUESTIONS RAISED BY THE APPROACHES

The consent-based approach

2.53 Consent-based approaches raise a number of questions. It must be decided what is to count as consent, how informed it must be, how explicit it must be and to what extent notions of implied or deemed consent are appropriate. For example, it is necessary to ask whether consent is to be assumed subject to an opt-out or whether it is limited to opt-in arrangements. It needs to be considered whether consent, once given, can be withdrawn, and whether consent to data sharing and use is one-off or continuing.

2.54 It is also difficult to decide when information is "about" or "related to" an individual, including how remotely "related" to an individual the information must be before it is no longer necessary to seek consent. Information may also be related to several distinct individuals who may desire conflicting things to be done with "their" information, such as family records.

2.55 Operating a consent-based approach also makes it necessary to decide as a matter of policy what the individual is to be taken to be consenting to: in particular how specific to a particular use of information the consent should have to be. For example it would need to be considered whether consent can appropriately be taken at an abstract level, such as to use for example health-related information "for the Department of Health's purposes", or whether specific consent should be obtained for disclosure of information to particular recipients or use of it for particular purposes.

2.56 Systems of obtaining and recording consent are by their nature resource-intensive. There are also a number of practical questions concerning how consent is to be recorded and used.[45]

[44] The data protection principles prescribed in Data Protection Act 1998 sch 1, part 1 and explained in sch 1, part 2 are listed above at para 1.58. The Information Commissioner's Office advocates a risk-based approach to the appropriate level of information security required to be compliant with the Data Protection Act 1998. See Information Commissioner's Office, *Guide to Data Protection*, p 82.

[45] Information as to whether individuals have consented to the disclosure of information or not can be revealing in itself; it may be possible draw inferences from the grant or refusal of consent to share particular information. The logic of a consent-based approach is that the fact of refusal of consent should not be disclosed or used without the subject's consent. There are therefore difficult questions about the collection, storage and use of the "consent data" themselves.

2.57 Finally, a consent-based approach raises questions about individuals who lack the capacity to consent: how they should be treated, who can give consent on their behalf and what safeguards and accountability mechanisms should be in place.

The purpose-based approach

2.58 In developing a purpose-based approach, the core question is for what purposes information should be shared. In the modern State, this is an immensely complex question. The sheer size and number of public bodies, the number of public functions they perform and the number of different ways that information can be used mean that an attempt to define all the purposes for which information can be shared and used raises a very large number of questions.

2.59 It also raises the question of how the limits on information transfer are to be controlled and enforced. Mechanisms for enforcement include judicial review, tribunals, independent regulators with a range of enforcement tools, criminal sanctions for wrongful use, and civil remedies and enforcement for unlawful use.

The risk-based approach

2.60 A risk-based approach similarly raises a large number of questions.

2.61 First, it is necessary to answer how risk is to be understood in relation to data sharing. This requires a set of concrete harms to individuals resulting from data sharing to be identified. It could also identify broader harms to other public interests, such as trust in institutions which require the cooperation of individuals.[46] It also requires an understanding of the magnitude of such harms and the probability of such harms occurring. This requires complex value and practical judgments to be made.

2.62 One must then decide how to set the acceptable level of harm, what standards are to be applied and how they are to be set or enforced. It is necessary to ask whether such levels and standards should be different in different fields and circumstances. In setting those standards or levels, it is necessary to ask how far the evaluation should include considerations of cost and administrative expediency.

2.63 There are particular questions where the risks associated with data sharing do not fall uniformly upon the whole population. A risk-based approach would require the decision-maker to decide where the public interest lies.

2.64 There are institutional questions about who decides what the acceptable level of risk is and how far that requires experience or expertise and, if so, what kinds of and level of experience or expertise. The mechanisms that are required to establish and manage risk must be agreed, in particular who participates in those processes and how far they are understood as technical or democratic in nature.

2.65 It is also necessary to consider how this can that be achieved in a way that is transparent, fair and open.

[46] As is the case in relation to doctor-patient confidentiality.

2.66 Further questions arise where a risk-based approach needs to deal with unknown risks, risks that are difficult to identify or risks where there is disagreement over their existence or extent. For example, it may be necessary to determine how far a risk-based approach should rely on a precautionary principle. The use of a precautionary principle would need to be considered in relation to information disclosure because the concept has been developed in public health and environmental law and may not operate in the same way in relation to information flows.

2.67 Finally, once those questions are decided, it is necessary to consider how, and how far, the risk should be minimised or managed, including what body or bodies make decisions as to the appropriate management of risk and what other factors are balanced against risk minimisation, such as the costs of reducing the risk, without introducing double counting.[47]

PROBLEMS WITH THE APPROACHES

The consent-based approach

2.68 There are practical difficulties in managing consent given the scale of the system. The costs of such a system are also high, not only to the State but to individuals who must, to a far greater extent, actively manage their consent. This might result in shifting the administrative burden from government to individuals, but not reducing it overall. It could also reduce accountability where individuals lack the time, incentives or expertise to make numerous informed decisions. Consent can also be collected easily through "tick box" terms and conditions: many individuals do not read and consider these provisions or privacy notices.

2.69 As the American Council of Advisors on Science and Technology note:

> The conceptual problem with notice and consent is that it fundamentally places the burden of privacy protection on the individual. Notice and consent creates a non-level playing field in the implicit privacy negotiation between provider and user. The provider offers a complex, take-it-or-leave-it set of terms, while the user, in practice, can allocate only a few seconds to evaluating the offer.[48]

2.70 Consent is also an inappropriate test where the State needs to act to the detriment of individuals in the pursuit of the public interest. Cases where it is

[47] These issues in the regulation of risk are subject to a broad and detailed literature across administrative law. For a good treatment of the subject, drawing upon insights from the regulation of environmental and public health risk, see E Fisher, *Risk, Regulation and Administrative Constitutionalism* (2007) in which Fisher argues that debates about the regulation of risk cannot be understood merely as clashes between scientific and democratic approaches but must be approached as debates about the proper role of public administration in relation to decision-making about risk. Fisher proposes two paradigms for risk regulation, which all attempts to deal with risk reflect to greater or lesser degrees: rational-instrumental and deliberative-constitutive paradigms. These paradigms reflect different approaches to the proper role of law and administration.

[48] Executive Office of the President of the United States of America, President's Council of Advisors on Science and Technology, *Report to the President: Big Data and Privacy – A Technological Perspective* (May 2014), available at: http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (last visited 1 July 2014).

plainly inappropriate to give an individual the right to refuse consent to the use of data about them include policing, child protection or fraud prevention. There are cases where it is appropriate for the State to hold information about citizens without consent. This point is conceded even by strong advocates of a consent-based approach.[49]

The purpose-based approach

2.71 The chief problem with a purpose-based approach is that it introduces enormous complexity to the legislative framework, best demonstrated by the massive multiplication of legal gateways to share data, each of which is a detailed set of legislative provisions. It is difficult to future-proof such legislative frameworks against legal, technological and institutional change. The sheer scale of the task is also problematic.

The risk-based approach

2.72 This approach raises real problems with the adequacy of risk assessment processes and methods and the fact that it can conceal some of the value judgments made in the process. A high quality risk assessment places a heavy administrative and technical burden on compliance, with attendant costs.

HYBRID MODELS

2.73 A possible approach to the regulation of data sharing could follow a hybrid model, combining elements of the different approaches.[50] A full reform project would need to consider how these approaches could be combined to encourage appropriate data sharing and use, with sufficient safeguards and mechanisms to address the issues and difficulties we identify. This is clearly a substantial piece of work that will require both careful analysis of the existing legal regime and consideration of the alternative models and options for reform, while receiving wide consultation input to inform that process and build a consensus around proposed solutions.

NEW PUBLIC MANAGEMENT

2.74 Some consultees argued that a proper approach to data sharing could not be separated from a consideration of "new public management" theories in government and public services delivery. "New public management" describes a variety of policies that have sought to make government more efficient and modern through market-orientated management techniques, such as subjecting public services to market forces, introducing competition, setting targets or measuring performance indicators.

2.75 New public management raises issues for data sharing because it seeks to introduce market-orientated behaviours and incentives which may not interact

[49] Consultation meeting no. 32 – Open Rights Group, Privacy International, My Dex, MedConfidential.

[50] In fact the current legal regime is a hybrid of the three models with a dominance of purpose-approach and important space for risk-based and consent-based approaches in particular fields. Individual projects also incorporate hybrid models, such as attempts to tackle fuel poverty through identifying eligible individuals by sharing data without consent and then offering further services with information sharing on a consensual basis.

effectively with the legal regime governing data sharing. It may change the behaviour of public bodies in seeking the public interest and thereby reduce the effectiveness of data sharing, for example where the pressure of competition and measurement reduces the willingness of a body to use permissive powers to share data because it will incur the cost and risk in doing so while not benefitting from the improvement in the delivery in public service, because its role is not properly acknowledged or measured.

2.76 New public management also raises issues for data sharing because the techniques employed by new public management can fragment service delivery and do not necessarily promote the relationships needed for appropriate data sharing.[51]

[51] See generally, R Wilson, G Maniatopoulos, M Martin, I McLoughlin, "Innovating Relationships" (2012) *Information, Communication and Society*; R Wilson, J Cornford, S Baines, J Mawson, "New Development: Information for Localism? Policy Sense-making for Local Government" (2011) *Public Money and Management*, 295; R Wilson, M Martin, S Walsh, P Richter, "Re-Mixing Digital Economies in the Voluntary Community Sector? Governing Identity Information and Information Sharing in the Mixed Economy of Care for Children and Young People" (2011) *Social Policy and Society*, 379; R Wilson, S Baines, J Cornford, M Martin, "'Trying to do a Jigsaw without the Picture on the Box': Understanding the Challenges of Care Integration in the Context of Single Assessment for Older People in England" (2007) *International Journal of Integrated Care*, 1; S Baines, R Wilson, S Walsh, "Seeing the full Picture? Technologically Enabled Multi-Agency Working in Health and Social Care" (2010) *New Technology, Work and Employment* 19.

PART 2
PROBLEMS UNDER THE CURRENT LAW

INTRODUCTION

In this part of the report we consider the problems faced by people and organisations trying to decide whether to disclose information under the current law. First, consultees reported complexity and confusion caused by the existence of the number of different overlapping legal regimes. These include European law, national legislation, the Human Rights Act and European Convention on Human Rights and the common law, including different rules for public and private bodies. Second, there are large numbers of express and implied statutory gateways, of varying breadth and protected by a wide range of different safeguards and controls. Third, the common law may include an ill-defined "third source" of law for the Crown. There are also legal and professional obligations in relation to confidentiality. Lastly, non-legal issues have a significant impact on practice and on the interpretation of legal obligations and limitations.

CHAPTER 3
OVERLAPPING LEGAL REGIMES

INTRODUCTION

3.1 In this chapter, we discuss the number and variety of overlapping legal regimes which must be considered when making decisions about data sharing. Subsequent chapters discuss the number and complexity of the web of statutory gateways, the common law powers of government and the duty of confidence.

3.2 The law applicable to information disclosures by public bodies is fragmented and complex. In this chapter, we explore problems with the current law experienced by consultees, including problems relating to express and implied statutory gateways for disclosure. Later in the report we examine two statutory regimes in detail: those applying to Her Majesty's Revenue and Customs and the Department for Work and Pensions. We also look at the Troubled Families Programme, a cross-government project requiring extensive data sharing.

3.3 It became clear from consultation meetings and responses that the existence of so many different legal and regulatory questions arising around information disclosure is itself a burden on appropriate information sharing. It creates legal costs and uncertainty. Although some burdens are necessary and appropriate, there are real questions over whether the current framework meets the need for balancing the public interest in protecting privacy and the public interest in effective information disclosure between public bodies.

THE NUMBER AND VARIETY OF DIFFERENT LEGAL REGIMES

3.4 Consultees explained that the number of different legal regimes adds to the complexity of data sharing, requiring practitioners to conduct a number of nuanced balancing exercises.

3.5 In making a decision on the disclosure of information, a public body must consider the following areas of law and regulation:

(1) Does the disclosing public body have the power to disclose the information?

(2) Does the recipient public body have the power to receive the information?

(3) Additional statutory controls on information disclosure.

(4) The common law of confidentiality.

(5) The Human Rights Act 1998 and the right to respect for privacy and family life under Article 8 of the European Convention of Human Rights.

(6) The operation of the Data Protection Act 1998 and the underlying 1995 Data Protection Directive, including the codes, guidance and enforcement policy of the Information Commissioner's Office.

(7) Additional professional or sector-specific duties and obligations arising from rules or codes adopted by professional, disciplinary or regulatory bodies.

3.6 Northumbria University provided a detailed and useful explanation of this problem:

> The current law on data sharing is complex due to the interplay between many different legal regimes. A public authority wishing to share information must first be able to identify the legal basis for doing so. It must then consider whether or not such sharing involves the use of personal data and if so consider if the sharing complies with the eight data protection principles. Exemptions to those principles may apply and can be difficult to interpret. There is a lack of Court guidance on the interpretation of the Act as there is little litigation in the data protection field and most that does exist arises as a result of challenges to section 40(2) refusals under [the Freedom of Information Act 2000].
>
> Secondly, even if data protection issues can be addressed then the authority must go on to consider whether or not the sharing would infringe Article 8 [of the European Convention on Human Rights] and if so whether or not it can be justified under Article 8(2). While there is greater judicial guidance on how Article 8 applies to information sharing and disclosure, particularly in the field of public protection and police work, such decisions involve a significant amount of nuanced judgment.
>
> Thirdly the information may also or alternatively be subject to a common law duty of confidence. Such considerations arise in relation to information around individuals but also for non personal commercially confidential information.

> Many of the decisions on such arrangements are being made by non-legal staff in information management, governance or IT departments. While legal advice may be available within the authority the experience of our students suggests that in many cases this is rarely a core area of business and there may well not be a legal advisor dedicated to providing specialist advice in this area. Confusion can often arise over which piece of legislation takes priority in a particular case.
>
> Given the number of different, often competing, issues a public authority must consider before it embarks on any data sharing initiative we consider there would be significant benefits in simplifying the regime data sharing between organisations.[1]

3.7 Some consultees described supposed conflicts between the legal regimes in cases where there were in truth no conflicts on a correct reading of the law. These provided useful illustrations of the difficulty consultees sometimes had in understanding the relevant law. One pointed to the relationship between legislation permitting data sharing in controlled circumstances, such as the Data Protection Act 1998 or Freedom of Information Act 2000, and legislation containing statutory bars prohibiting disclosure of certain information. The consultee said that the relationship was "unclear". However, if a statutory prohibition exists, sharing is clearly not lawful. The first data protection principle under the Data Protection Act 1998 is to process data fairly and lawfully. Data disclosure in the face of a statutory prohibition would be in breach of the first data protection principle, and would not, therefore, be permitted.

3.8 Concerns were also expressed about the disclosure of unsubstantiated complaint information held by Trading Standards Departments, which could be libellous, or other information held by a Council that was confidential.

3.9 Sue Richardson of Bradford University accepted that the law did seem unclear, uncertain and complex from a practitioner's perspective, but argued that the law was necessarily this way as it cannot prescribe for every situation since data sharing decisions are context-specific and depend on numerous variables.[2]

3.10 Other problems identified were the complex and fragmented regulatory landscape, the divergence and multiplicity of interpretations, and the lack of clear guidance with resulting divergent practice.

3.11 For example, a group of academic researchers told us that there was sufficient clarity in the law but that the problem lies in the policies and procedures adopted by regulatory and enforcement bodies.[3] They noted that the regulatory landscape is both complex and fragmented. There are differences, they told us, in the way information obtained by whistleblowers is handled by regulators who pass concerns on to other regulators or enforcement bodies. The law around

[1] Consultation response no. 76 – Northumbria University. Leeds City Council and others made similar points.

[2] Consultation response no. 41 – Sue Richardson, University of Bradford.

[3] Consultation response no. 35 – Dr Ashley Savage, Dr Richard Hyde, Mr Jamie Grace and Ms Bansi Desai.

international information sharing is in their view fragmented, and could be seen by some regulators as insufficiently clear, although they did not see this as preventing sharing. They found it difficult to discern the procedural rights of individuals, following from the application of principles of natural justice and human rights, where they may have an opportunity under existing law to prevent or at least limit the way that data are shared. For example, the procedural rights of NHS patients to notification, objection and meaningful consultation in the way their health data might be used in research or strategic planning projects.

PROFESSIONAL OR SECTOR-SPECIFIC DUTIES AND OBLIGATIONS

3.12 Information sharing is variously regulated by the courts, the Information Commissioner's Office, sectoral or professional regulators such as the General Medical Council and Royal Colleges, as well as industry regulators or enforcement bodies, such as Ofwat.[4] Consultees expressed the view, in relation to the General Medical Council and Ofwat and more generally, that often a professional or industry regulator can have a greater impact on behaviour in its sphere than the courts or the Information Commissioner's Office.[5]

3.13 Some consultees felt that the approach and strategy of different bodies with regulatory or legal oversight of data sharing, such as the Information Commissioner's Office or the courts, could differ and therefore create uncertainty. For example, one consultee doubted that the Information Commissioner would apply the same level of scrutiny as the courts in the event of a data breach.[6] Another consultee felt that decisions of the courts themselves were not clear and consistent in relation to data sharing.[7]

3.14 The rules that professional bodies apply to particular sectors can be more onerous and specific than general data protection law requires.

3.15 A key example is the regulation of the medical profession, where patient confidentiality and the management of records are the subject of codes, guidance and professional discipline. It is the norm for professional, regulatory and disciplinary bodies to have rules on the handling of information by regulated individuals within the professions and regulated sectors. This creates another layer of complexity for individuals making decisions about information disclosure.

DATA PROTECTION LAW

3.16 The Data Protection Act 1998 is the implementation in the United Kingdom of the 1995 Data Protection Directive. Fundamental recasting of the Data Protection Act 1998 would, therefore, be beyond the scope of a law reform project limited to the United Kingdom. However, it is important to understand the problems experienced by consultees in applying the 1998 Act and also to consider those areas where there might be scope for improvement within the freedom of action

[4] Ofwat is the statutory water services regulation authority.

[5] For example, consultation meeting no. 7 – Amberhawk Conference attendees.

[6] Consultation meeting no. 24 – Northumbria University Information Law Centre Conference attendees.

[7] Consultation meeting no. 24 – Northumbria University Information Law Centre Conference attendees.

allowed by the Directive.

Difficulties with the Data Protection Act 1998

3.17 Several consultees did not find the Data Protection Act 1998 readily understandable. This has an effect on the clarity of guidance based upon it. The tests for identifying a data controller and processors, gauging necessity and other compatible purposes all give rise to legal uncertainty.

3.18 A number of examples were provided by consultees.

3.19 The Association of Independent Healthcare Organisations told us that the Data Protection Act 1998 was generally perceived to prevent sharing information rather than to ensure that information is shared safely and not withheld. Guidance has attempted to counter this perception, including the Information Commissioner's Data Sharing Code and the second Caldicott Report on information sharing in the National Health Service.[8]

3.20 There is a lack of understanding of the meaning of "controller" and "processor" under the 1998 Act. This is exacerbated where there are joint controllers or controllers in common. Difficulties arise where, for example, cloud services are used or in healthcare where numerous bodies, such as general practitioners, NHS Trusts and the Department of Health, hold patient information and there is confusion over the relationships between them in relation to that information.[9]

3.21 Consultees found the "necessity" test under the data protection principles difficult.[10]

3.22 One consultee considered that the decision of the Administrative Court in *R (Lord) v Secretary of State for the Home Department* could create difficulties for data sharing for anti-fraud data matching exercises.[11] The case concerned the scope of the exemption under section 29(1) of the Data Protection Act 1998 for processing information for the purpose of the prevention or detection of crime or the apprehension or prosecution of offenders. The provision exempts processing in any case to the extent to which the application of data protection provisions to would be likely to prejudice those matters. Mr Justice Munby interpreted the phrase "in any case" to mean "in any particular case" and "likely" to indicate a very significant chance. This interpretation of necessity could make anti-crime

8 Information Commissioner's Office, *Data Sharing Code of Practice* (May 2011): Caldicott Review, *Information: To share or not to share? The Information Governance Review* (2013)

9 Consultation meeting no. 22 – Independent Healthcare Advisory Services. Cloud services are storage spaces provided over the internet, so that information can be uploaded by the service user, stored by the cloud storage provider online and made accessible to the user via the internet from any location. Information uploaded in the United Kingdom may be stored in the United Kingdom or elsewhere, and the cloud service provider may buy cloud services from other organisations. For a discussion of the legal issues cloud services pose for data protection, see W Kuan Hon, C Millard and I Walden, "The problem of 'personal data' in cloud computing: what information is regulated?—the cloud of unknowing", (2011) 1 *International Data Privacy* 211 to 228.

10 The data protection principles are discussed in the Consultation Paper at para 3.23 to 3.48 and are set out above in ch 1.

11 [2003] EWHC 2073 (Admin); [2004] Prison LR 65, Munby J.

data sharing exercises, where only a proportion of cases will result in the detection of crime, very difficult. Leeds City Council went on to say

> In relation to the 2nd data protection principle, whilst there has been much debate about what 'incompatible' means, and how far other purposes can reasonably be said to be compatible, this does seem unduly technical and semantic, although it is acknowledged that the second principle is derived from the requirements of Directive 95/46/EC, Articles 6 and 7. It does also seem difficult to reconcile this requirement with the conditions for fair and legitimate processing which permit processing which is necessary for a range of public purposes, and without the consent of the data subject. In any event, it does seem that the root issue (which the Article 8 requirements address more directly) should really be whether any processing of whatever nature (irrespective of the purpose the data was expressed to be collected for) can be justified on one of the permitted grounds for interference, and is proportionate.[12]

3.23 Another consultee considered that there is misunderstanding regarding the research exemption in the Data Protection Act and when it is appropriate to apply it.[13]

3.24 Another said there was a need for guidance on the process of assessing what pseudonymised or de-identified data can be re-identified for the purposes of the Act. There would be value in an analytical toolkit to allow people to evaluate the likelihood of reidentification in a consistent manner. Such guidance would be more meaningful where it focuses on practical examples and scenarios.[14] The UK Anonymisation Network, in a consultation meeting, observed that anonymisation is more of a risk management exercise than the Data Protection Act recognises, in drawing a distinction between anonymous and identifiable data. The Network maintained that there is no such thing as truly anonymous data. The aim must always be to produce data which are anonymous enough in proportion to their sensitivity.[15]

3.25 Health and social care professionals, in a response compiled by DAC Beachcroft Solicitors, expressed concern about different approaches to sharing data for health and for social care purposes in different pieces of legislation. Sharing for "medical purposes" in Schedules 2 and 3 of the Data Protection Act could be interpreted very differently. For example, schedule 3(8) of the Act refers only to medical purposes and does not extend to use of data for social care purposes, even for the same individual as part of the same package of care. Social workers are not included in the definition of "health professional" in section 69(1)(h) of the Data Protection Act. Section 251 of the National Health Service Act 2006, on the other hand, enables data to be shared for the purposes of "the management of health and social care services". The gateway provided in the National Health Service Act is wider than the controls provided by the Data Protection Act,

[12] Consultation response no. 17 – Leeds City Council.

[13] Consultation response no. 74 – Scottish Government.

[14] Consultation meeting no. 7 – Amberhawk Conference.

[15] Consultation meeting no. 42 – UK Anonymisation Network.

leaving those interpreting the law with a confusing set of rules to apply.[16]

3.26 Birmingham City Council thought it was not clear how the Data Protection Act 1998 works in conjunction with legal provisions in other statutes that potentially enable data sharing. The uncertainty largely concerns the interpretation of consent: whether it is explicit or implied, the amount of data that can be shared and the purpose. There is also uncertainty as to whether shared data can be used for compatible purposes and what obligations are placed upon the data controller(s) when making decisions of that nature. A further complication arises from difficulty in understanding when to establish data sharing agreements for the ad hoc sharing of data. Birmingham City Council provided a case study in relation to this.

Birmingham City Council case study: tracing vulnerable children

3.27 This concerned information held by the Council for one purpose which another department in the Council wished to use for a different purpose. The Council gave this as an example of uncertainty as to whether data which have been shared for one purpose may then be used for can be shared for another purpose and of the confusion which can be exacerbated by the terms of data sharing agreements.

> A large number of requests were being received from the Council's Children's Social Care Department requesting information from the [Council's] Revenues [Department] in order to trace families. A data sharing agreement was set up to facilitate these requests. Due to the fact that a considerable amount of information was held by the Council on behalf of the [Department for Work and Pensions], the Council was not able to share this information with the Council's Children's Social Care department. The information could only be shared from the Council's Revenues Department data and not the [Department for Work and Pensions] data, even though it was held on the same computer system.
>
> Since setting up the agreement, the number of requests has increased substantially, up to 10 requests a day can be received from the Council's Children's Social Care Department.
>
> Over time the number of staff making use of the agreement appears to have increased, and the reasons have become more varied. It appears that this agreement is now being used for any information required by Council's Children's Social Care Department rather than specifically to trace missing families.

[16] DAC Beachcroft convened a series of seminars with stakeholders from the health and social care sector. Consultation response no. 49 – DAC Beachcroft Solicitors seminar.

> The officers are also requesting increasing amounts of information, rather than specific information. Dates of birth are frequently requested, despite the fact that the Council's Children's Social Care Department have been made aware that this is exclusively the [Department for Work and Pensions'] data rather than the [Council's] Revenues [Department] information, and not covered by the agreement.
>
> The agreement was initially intended to save time by negating the need to investigate the reasons and the Data Protection Exemptions (section 29 or section 35) on every request, but the increased volume of requests it has generated now requires more staff time to deal with. Approximately one day per week of staff time is used answering these enquiries.[17]

3.28 The Data Protection Act 1998 places additional burdens on information disclosure. In particular, it insists on a high level of security for personal data and upon organisational measures to ensure compliance with the data protection principles. Sometimes this can prevent the use of certain types of information disclosure system, for example, where the cost of adequate security makes the project unviable. There is, however, broad support for holding public bodies to a high level of data protection, especially as regards data security. There are examples of public bodies that have achieved successful sharing in the context of a high level of data protection assurance. It seems that the problems experienced by public bodies are the organisational, management, and training problems associated with providing a high level of data protection. This is an important part of good information disclosure practice.

3.29 The solution to such difficulties seems to lie in communicating good practice and systems, providing adequate resources for training and security systems and balancing internal disciplinary messages with explicit recognition of the need to share in appropriate circumstances. It can also be a question of establishing and maintaining good working relationships with other public bodies and developing an understanding of the information needs and limitations of other bodies as well as the public body's own needs. There is a case for mainstreaming data protection decision-making so that the officials responsible for data protection compliance and finding solutions to enable sharing are co-ordinated at a higher level. Data protection is often treated as an afterthought with the effect that public bodies fail to plan effectively.

A review of the Data Protection Act 1998?

3.30 We have noted above that the content of the Data Protection Act 1998 is largely prescribed by the 1995 Data Protection Directive.[18] There are, however, areas which might benefit from review. These are the framework for issuing monetary penalties and the treatment of processing, including anonymised information, and the interpretation of the term "necessary" where necessity is a requirement under

[17] Data Protection Act 1998, ss 29 (personal data processed for the purposes of crime detection or apprehension or taxation) and 35 (disclosures required by law or made in connection with legal proceedings etc).

[18] Data Protection Directive 95/46/EC.

the data protection principles in the 1998 Act. Anonymisation is discussed in Chapter 6.

Monetary penalty notices

3.31 The Information Commissioner's Office has a power to issue fines of up to £500,000 for serious breaches of the Data Protection Act or the Privacy and Electronic Communications Regulations.[19] Fines issued by the Information Commissioner's Office are significant. With two exceptions, both in the private sector, all fines have exceeded £50,000. No fine has reached the maximum of £500,000. The largest fine to date is £325,000.[20]

3.32 During our scoping consultation, we heard that monetary penalty notices are a source of considerable anxiety for data protection practitioners.[21] It may be that monetary penalty notices have a "chilling effect" on appropriate data sharing. The risk of monetary penalty notices certainly weighs heavily in the minds of practitioners. It may be therefore that monetary penalty notices are partly responsible for the risk aversion reported to us in consultation.

3.33 There is no requirement in the Data Protection Directive to create a system of monetary penalty notices. Other Member States have created alternative systems.[22]

THE LEGAL FRAMEWORK

3.34 The Information Commissioner has the power to issue monetary penalties under sections 55A of the Data Protection Act 1998.

3.35 A monetary penalty notice may only be issued where the Commissioner is satisfied that there has been a serious contravention of section 4(4). Section 4(4) provides that it is the "duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller". The contravention must be of a "kind likely to cause substantial damage or substantial distress". Section 55A only applies if the contravention is deliberate or if the data controller failed to take reasonable steps to prevent a contravention that the data controller knew or ought to have known that there was a risk of occurrence and the occurrence would be of a kind likely to cause

[19] SI 2003 No 2426. These regulations relate to direct marketing, defined in Data Protection Act 1998 s 11 as 'the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals'.

[20] This fine was imposed on Brighton and Sussex University Hospitals NHS Foundation Trust for the insecure disposal of a large number of computer hard drives containing unencrypted sensitive personal information, many of which were later sold at auction.

[21] See para 1.20 above for definition of "data protection practitioners".

[22] For example, the French Data Protection Authority makes use of on-site inspection, Nordic data protection systems rely on a more consultative regulatory strategy and the UK Information Commissioner's Office is the only Data Protection Authority to make use of undertakings in its enforcement strategy. Maximum levels of monetary penalty are also set differently in different Member States. For example, the French Data Protection Authority has a cap of €150,000 (approximately £120,000) for the first penalty and €300,000 (approximately £250,000) for repeated breaches, the German Data Protection Authorities can impose a monetary penalty of up to €300,000, whereas the UK Information Commissioner's Office can impose penalties of up to £500,000. See http://www.out-law.com/en/articles/2013/july/data-protection-enforcement-in-uk-france-and-germany-explained/ (last visited 1 July 2014).

substantial damage or substantial distress. A monetary penalty cannot be imposed on a data processor.

INFORMATION COMMISSIONER'S OFFICE POLICY AND GUIDANCE

3.36 The Information Commissioner's Office guidance on monetary penalty notices describes the Commissioner's underlying objective in imposing a monetary penalty as being to promote compliance with the Data Protection Act 1998 and the 2003 Regulations.[23] The possibility of a monetary penalty notice should encourage compliance and act as a deterrent against non-compliance.[24] The guidance notes that it will "only be appropriate in the most serious situations". The Information Commissioner's Office takes account of the sector involved and the size, financial and other resources of a person before determining the amount of the monetary remedy. The Information Commissioner's Office seeks to promote compliance as "integral to carrying out any business activity". Its guidance provides that "a penalty would not be imposed on an employee who was simply acting on the instructions of his employer".[25] The guidance states that as "a general rule a person with substantial financial resources is more likely to attract a higher monetary penalty than a person with limited resources for a similar contravention".[26]

3.37 The Information Commissioner's Office provides the following example of serious contraventions leading to a data breach: a failure to take adequate security measures, use encrypted files or devices, and have in place operational procedures or guidance, which together result in the loss of a compact disc holding personal data.

3.38 The Information Commissioner's Office similarly provides the following examples of what might constitute reasonable steps: a risk assessment, appropriate policies, procedures, practices or processes, advice and guidance to staff, and evidence that a person had recognised the risks of handling personal data and had taken steps to address them.

3.39 The Commissioner is required to issue guidance, including guidance on the circumstances in which he would consider it appropriate to issue a monetary penalty notice and how he will determine the amount of the penalty.[27] The Guidance provides that the presence of one or more of the following factors will make it more likely that a monetary penalty notice will be issued. This list is not exhaustive:

(1) Seriousness, including the nature of personal data, duration and extent of the contravention, the number of individuals actually or potentially

[23] Information Commissioner's Office, *Information Commissioner's Guidance about the issue of monetary penalties prepared and issued under section 55C(1) of the Data Protection Act 1998* (2012) available at: http://ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ico_guidance_on_monetary_penalties.pdfP5 (last visited 1 July 2014), subsequently referred to as the Information Commissioner's Office, Monetary Penalty Guidance.

[24] Information Commissioner's Office, *Monetary Penalty Guidance*, p 5.

[25] Information Commissioner's Office, *Monetary Penalty Guidance*, p 10.

[26] Information Commissioner's Office, *Monetary Penalty Guidance*, p 11.

affected, whether it concerns an issue of public importance, or whether the breach is the result of deliberate or negligent behaviour.

(2) A deliberate contravention – deliberate or premeditated, aware of and did not follow Information Commissioner's Office advice, series of similar contraventions and no action to rectify the cause.

(3) The discloser knew or ought to have known of the risk.

(4) Other considerations – the need to maximise deterrent effect, refusal without reasonable cause to submit to voluntary assessment or audit.

(5) A monetary penalty notice would be less likely where the breach was outside a person's direct control, or where there was genuine doubt or uncertainty. Ignorance is, however, not a defence.[28]

THEMES IN MONETARY PENALTY NOTICES ISSUED

3.40 We reviewed the notices issued before the end of 2013. Some 44 monetary penalty notices had been issued for contraventions of section 4(4) of the Data Protection Act 1998 since the coming into force of section 55A on 6 April 2010. Forty two of these were imposed on public bodies and only two on private bodies. Twenty two were issued in response to the sending of personal data in error to unintended recipients. Eight were issued in response to the theft or loss of unencrypted electronic devices. Seven monetary penalty notices were issued in response to other types of theft or loss. Four monetary penalty notices were issued in response to the disclosure of personal data as a result of errors or insecure servers on the internet. Four monetary penalty notices were issued in cases of insecure disposal or storage of personal data. One monetary penalty notice was issued in a case of inaccuracy. All but one related to a contravention of the 7th data protection principle. Breaches of the 3rd or 4th data protection principle were taken into account in setting the level of the fine in a small number of cases. The one case of serious contravention of the 4th data protection principle occurred in the private sector, although it is of a kind that could occur in public bodies which use data matching techniques on databases of personal data.[29]

3.41 In consultation meetings, people reported fears that organisations would be fined and that they would be held personally responsible by their employers or held personally criminally liable by the Information Commissioner. Consultees also confused the nature of responsibility under the 1998 Act and thought that a monetary penalty order could be imposed against them personally for their actions in the course of their employment.

3.42 Such fears are ill-founded. The monetary penalty notices issued up to the end of 2013 were imposed for breaches of security, not for value judgments. The key failures that expose public bodies to monetary penalty notices are thefts or losses

[27] Data Protection Act 1998, s 55C.

[28] Information Commissioner's Office, *Monetary Penalty Guidance*, pp 18 to 20.

[29] The data protection principles are set out above at para 1.58

of highly sensitive personal data, especially involving unencrypted devices or unlocked containers; serious decommissioning failures resulting in the exposure of sensitive personal data; inadvertent disclosure to unintended recipients by in email, fax or letter in circumstances where inadequate training, procedures or security systems were in place; inadvertent disclosure online or inadequate website security. The reported cases concern errors flowing from inadequate systems of training, information governance policies and training or security systems. The Information Commissioner's Office takes into account the means of the data controller and whether the fine will have an impact on the public purse.

NEW SENTENCING POWERS

3.43 The Criminal Justice and Immigration Act 2008 gave the Secretary of State power to provide, by order to amend section 55 to include provision for a sentence of imprisonment, a fine or both on conviction for unlawful obtaining of personal data, pursuant to section 55 of the Data Protection Act 1998. No such orders have been made to date.[30]

CASE STUDY: BRITISH PREGNANCY ADVISORY SERVICE, INFORMATION COMMISSIONER, 28 FEBRUARY 2014

3.44 In a recent example, occurring outside the period of our survey, the British Pregnancy Advisory Service was issued with a monetary penalty notice under section 55A(3) where the data controller knew or ought to have known that there was a risk that a contravention would occur, which was likely to cause substantial damage or distress, but failed to take reasonable steps to prevent it. An attacker used an automated tool to identify website vulnerabilities, gained unauthorised access to the British Pregnancy Advisory Service's website and defaced the website. The organisation is a provider, amongst other things, of abortion services and the attacker was motivated by opposition to abortion. The British Pregnancy Advisory Service was not aware that its website retained personal contact details of inquirers who had asked to be called back. The Information Commissioner found that it was not necessary to retain these details after the inquirer had been called back. The organisation had failed to take adequate steps to ensure that administrative passwords were stored securely or that standards of communication confidentiality were met. They also failed to carry out appropriate security testing and did not keep the software supporting the website up to date. The Information Commissioner held that this was a breach of the seventh data protection principle:

> 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.[31]

3.45 The decision found that there had been breaches of paragraphs 9, 11 and 12 of Part II of Schedule 1 to the 1998 Act. The breach was serious because the organisation was unaware that personal data were held on the website, with the

[30] Criminal Justice and Immigration Act 2008, s 77. A discussion on the history of this amendment and what has happened since it came into force may be found in R Jay, *Data Protection Law and Practice* (4th ed 2012) para 21-38 to 21-32.

[31] Data Protection Act 1998, sch 1, pt 1.

result that the personal contact details of 9,900 people were unprotected from an attack of the sort which occurred, in the context of the highly personal and sensitive services provided by the organisation. This contravention was of a kind likely to cause substantial damage or distress, although fortunately the attacker was caught quickly and the information recovered before further use could be made of it. Had the information been disseminated further, additional distress or substantial damage could have been caused. The Information Commissioner also noted that the organisation decided not to inform the affected people about the security breach so as not to cause further distress, which was an acceptable decision to make in the circumstances. The fifth data protection principle was also breached as the information was kept for much longer than necessary.

3.46 The Commissioner found that the organisation had sufficient resources to pay a monetary penalty of up to the maximum level without undue financial hardship. He also took into account mitigating factors, including: that the website was attacked by a criminal, convicted of offences under the Computer Misuse Act 1990; the organisation acted quickly to obtain an injunction to prevent further dissemination; the breach was reported to the Commissioner's Office voluntarily and remedial action taken; the organisation is a charity as well as an NHS provider; it had suffered significant reputational damage as a result of the breach and reports of it in the media.

3.47 A monetary penalty of £200,000 was imposed.

3.48 We have concluded that there is an unfounded fear of Information Commissioner's Office enforcement action, especially in relation to monetary penalty notices.

3.49 As Northumbria University explained

> Concerns arise from individual public sector staff members about personal liability when mistakes occur. While there is a degree of misinformation about the prospect of being prosecuted under the Data Protection Act 1998 there is also a high degree of concern about disciplinary implications for errors. This can lead to a culture of caution and acts as a further inhibitor to the sharing of information. Combined with a lack of familiarity with the legal regimes and a lack of ready access to specialist legal advice it becomes very easy to adopt an overly cautious stance on information sharing.[32]

CONCLUSIONS

3.50 The fear of monetary penalty notices expressed in consultation results in a restrictive approach to data sharing. We concluded that the fears expressed in consultation were misplaced or disproportionate and were preventing lawful data sharing. It is not at all clear, however, that monetary penalty notices have a deterrent effect on large private organisations from breaching the data protection principles. Such organisations may make an economic assessment to calculate the cost of the risk of incurring the maximum penalty against the profit to be made.

[32] Consultation response no. 76 – Northumbria University.

3.51 A review of how to counter these fears and misunderstandings of monetary penalty notices could include a review of the system of monetary penalties itself, including costs and benefits.

Necessity

3.52 The 1995 Data Protection Directive and the Data Protection Act both impose tests of "necessity". For example, section 35 of the 1998 Act exempts personal data from the non-disclosure provisions where the disclosure is necessary for the purpose of any legal proceedings, obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

3.53 "Necessity" has not been interpreted by the courts as meaning strictly necessary in the sense that there was possible alternative. The Court of Justice of the European Union has held that "necessity" extends beyond necessity for the application of the legislation and includes choosing an option which allows the relevant legislation to be more effectively applied.[33]

3.54 It may not be possible to change the wording of the 1998 Act itself, but it is worth considering how to make clear to data protection practitioners that "necessity" in this context does not carry its ordinary and natural meaning. Its meaning is autonomous and may not be the same as that in other contexts, such as "necessary in a democratic society" under the European Convention on Human Rights.[34]

HUMAN RIGHTS LAW

Human Rights Act 1998 and the European Convention on Human Rights

3.55 As we explained in Chapter 1, data protection is provided for under the European Convention on Human Rights as part of the qualified right to privacy and family life, under Article 8 of the Convention. Any decision by a public body on whether to share data will require an assessment of the impact on the data subject's right to privacy and family life.

3.56 The courts have considered the impact of Article 8 on data sharing. The decisions are nuanced and require some interpretation. The House of Lords gave guidance on how to determine whether the publication of confidential information breached the right to privacy in *Campbell v MGN Limited.* The majority held that model Naomi Campbell's right to privacy had been breached by the publication of information about her treatment for drug addiction and photographs of her leaving self-help group meetings, and that the infringement was not justified by any public interest in her as a public figure. The court first had to consider whether the information was confidential, then whether its disclosure was in breach of article 8(1) and then whether that breach was justified under article 8(2).

3.57 Lord Hope of Craighead explained that the issue of whether the right of privacy

[33] *Huber v Germany* [2008] ECR I-9705 Case C-524/06 at para 66, applied by the Court of Appeal in *Chief Constable of Humberside v Information Commissioner* [2009] EWCA Civ 1079 [2010] 1 WLR 1136

[34] *Handyside v United Kingdom* (1979-80) 1 EHRR 737: interference must be necessary in a democratic society – a reasonable and proportionate response to the need which justifies the interference.

had been infringed was resolved by considering not the mind of the reader of the information but

> of the person who is affected by the publicity. The question is what a reasonable person of ordinary sensibilities would feel if she was placed in the same position as the claimant and faced with the same publicity.[35]

3.58 He adopted the objective test applied by Mr Justice Nicholson in *P v D*

> The factor that the matter must be one which would be highly offensive and objectionable to a reasonable person of ordinary sensibilities prescribes an objective test. But this is on the basis of what a reasonable person of ordinary sensibilities would feel if they were in the same position, that is, in the context of the particular circumstances. I accept that P has the stated feelings and consider that a reasonable person of ordinary sensibilities would in the circumstances also find publication of information that they had been a patient in a psychiatric hospital highly offensive and objectionable.[36]

3.59 The House of Lords held that, if the information was confidential, it was necessary to carry out a balancing exercise in each case, before deciding whether publication was permissible. Lord Hope quoted with approval Sedley LJ in *Douglas v Hello! Limited*

> Everything will depend on the proper balance between privacy and publicity in the situation facing the court.[37]

3.60 Section 6 of the Human Rights Act 1998 makes it unlawful for a public authority, as defined in the Act, to act in a way which is incompatible with a Convention right. This requirement does not apply to private bodies as such. A private body may, however, be subject to the Human Rights Act to the extent it is carrying out functions of a public nature.

3.61 Though undoubtedly important, an excessive focus on human rights alone can distract from realising the full potential of the broader legislative schemes and provisions to facilitate or restrict data sharing between public bodies. In *Kennedy v Charity Commission*,[38] Lord Mance, with whom Lords Neuberger and Clarke agreed, was critical of the "tendency to see the law in areas touched by the [European] Convention [on Human Rights] solely in terms of the Convention rights".[39] This tendency risked failing to survey the broader statutory and common law framework, in this case the general powers of the Charity Commission to disclose information under the Charities Act 1993 interpreted in light of a

[35] [2004] 2 AC 457.

[36] [2000] 2 NZLR 591 at 601. In *P v D*, the claimant was a public figure who was told that publicity was about to be given about the fact that he had been treated at a psychiatric hospital.

[37] [2001] QB 967 at 1035.

[38] [2014] UKSC 20; [2014] 2 WLR 808.

[39] [2014] UKSC 20; [2014] 2 WLR 808, para 46.

"common law presumption in favour of openness".[40]

Hybrid bodies

3.62 The decisions of the higher courts suggest that a detailed examination of the functions under challenge is necessary in order to determine when a private body might be acting as a public authority. In *Aston Cantlow v Wallbank*, the House of Lords held that a parochial church council was not a public authority for the purposes of section 6 of the Human Rights Act. Lord Nicholls held

> What, then, is the touchstone to be used in deciding whether a function is public for this purpose? Clearly there is no single test of universal application. There cannot be, given the diverse nature of governmental functions and the variety of means by which these functions are discharged today. Factors to be taken into account include the extent to which in carrying out the relevant function the body is publicly funded, or is exercising statutory powers, or is taking the place of central government or local authorities, or is providing a public service.[41]

3.63 In R (on the application of Heather) v Leonard Cheshire Foundation[42] a charitable housing association was held not to be a public authority, but in Poplar Housing and Regeneration Community Association Ltd v Donoghue, Lord Woolf CJ held

> while activities of housing associations need not involve the performance of public functions in this case, in providing accommodation for the defendant and then seeking possession, the role of Poplar is so closely assimilated to that of Tower Hamlets that it was performing public and not private functions.[43]

3.64 On the other hand, in *Cameron v Network Rail Infrastructure Ltd (formerly Railtrack Plc)* the High Court held that Network Rail (and its predecessor Railtrack plc) was not a "hybrid" public authority for the purposes of the Human Rights Act in its capacity as the "infrastructure controller" within the meaning of the Railways (Safety Case) Regulations 2000 and the owner and controller of the railway where the Potters bar rail accident occurred.[44] This first instance decision on a preliminary point was not appealed. In *Network Rail Ltd v Information Commissioner* the Information Tribunal held that Network Rail was not subject to either the Freedom of Information Act 2000 or the Environmental Information Regulations 2004, as it was not a public authority for the purposes of either.[45]

3.65 Apart from the Human Rights Act, the activities of a private body may be subject

[40] [2014] UKSC 20; [2014] 2 WLR 808, para 47.

[41] *Aston Cantlow and Wilmcote with Billesley Parochial Church Council v Wallbank and Another* [2003] UKHL 37; [2004] 1 AC 546, para 12.

[42] [2002] EWCA Civ 366; [2002] 2 All ER 936

[43] [2002] QB 48.

[44] [2006] EWHC 1133 (QB), [2007] 1 WLR 163.

[45] See also *R (on the application of Heather) v Leonard Cheshire Foundation* [2002] 2 All ER 936 (a charitable housing association was not a public authority) and *Poplar Housing and Regeneration Community Association Ltd v Donoghue* [2002] QB 48.

to public law, and to the supervisory jurisdiction of the courts by way of judicial review, if the body is performing a "public function".[46]

Conclusions

3.66 A full law reform project will need to include those private bodies carrying out out-sourced public functions including public service delivery. Obligations under the Human Rights Act 1998 may apply to public functions which are outsourced to private bodies or those obligations may remain with the public bodies contracting services out.

Charter of Fundamental Rights of the European Union

3.67 Article 7 of the Charter provides a right to respect for private and family life, home and communications. In addition, article 8 creates a distinct right of each person to the protection of personal data concerning him or her and a requirement that such data

> be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3.68 Article 8 also requires that compliance be subject to control by an independent authority.

3.69 The status of the Charter in United Kingdom law remains a matter of contention.[47] Article 6 of the Treaty on European Union provides that the Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights "which shall have the same legal value as the Treaties", but that the provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties. Article 51 of the Charter provides that the Charter applies to member states only "when implementing European Union law".[48] A Protocol to the Treaty on European Union provides, amongst other things, that nothing in the Charter creates justiciable rights in the United Kingdom or Poland except insofar as such rights were provided for in national law. The Court of Justice of the European Union clarified the effect of the Protocol in *R (NS) v Secretary of State for the Home Department* where it held that the Protocol did not exempt Poland

[46] *R v Panel on Takeovers and Mergers, ex parte Datafin plc* [1987] QB 815; *R v Criminal Injuries Compensation Board, ex parte Lain* [1967] 2 QB 864. See also *YL v Birmingham City Council* [2007] UKHL 27; [2001] 1 AC 95, *R(Beer) v Hampshire Farmers Markets Ltd* [2003] EWCA Civ 1056; [2004] 1 WLR 233.

[47] In *R (on the application of AB) v Secretary of State for the Home Department* [2013] EWHC 3453 (Admin); [2014] CMLR 22, Mostyn J said, in comments which did not form part of the legal reasoning for his judgment, that the Charter of Fundamental Rights, and in particular the right to protection of personal data under art 8, was now binding in United Kingdom law even though it had not been incorporated into law in the United Kingdom by the Human Rights Act 1998.

[48] The "plain" meaning of art 51 has been given a broad interpretation by the Court of Justice of the European Union in Case C-617/10 *Aklagaren v Fransson* [2013] 2 CMLR 46 where the court interpreted "when implementing European Union law" as "acting within the scope of European Union law".

or the United Kingdom from the Charter.[49]

UNDERSTANDING THE CURRENT LAW

3.70 As mentioned above, poor understanding of the current law can lead to incorrect or restrictive interpretations of the law. Consultees were well aware of the issues this raises and provided some suggestions for improvement.

Consultation

3.71 In the consultation paper we asked:

> Question 2: Do those responsible for data sharing in your organisation have a good understanding of the law? If not, to what do you attribute this?[50]

3.72 Consultees identified a number of particular problems with understanding.

The distribution of knowledge

3.73 The distribution of knowledge in public bodies is not even. Many consultees, both in written responses and consultation meetings, explained that although lawyers and specialist data protection and information governance officials, including Caldicott Guardians in the NHS, have a good understanding of the law, there is a lack of understanding outside specialist teams.

3.74 The Independent Information Governance Oversight Panel explained that there is a lack of common cross-organisational understanding of the need to comply with all three key sources of law (Human Rights Act 1998, Data Protection Act 1998 and common law). For example, the panel explained that many individuals appear to believe that it is enough to comply with the Data Protection Act 1998 alone.[51]

3.75 Smaller organisations, such as fire and rescue services, have limited specialist expertise and experience compared to central government and larger public bodies, like the police or National Health Service, which have greater central coordination and support.

3.76 Data protection practitioners also appear to have more knowledge of the limits on their sharing than of the extent of their powers to share. Some consultees maintained that levels of knowledge of the requirements of the Data Protection Act 1998 are higher than levels of knowledge of the law that permits sharing. The Department of Health told us that training focuses more on keeping data secure than on sharing it appropriately.[52] Sheffield City Council considered that identifying the relevant legal basis for and the conditions applying to sharing can be more difficult than it ought to be, hence staff might be aware of some data

[49] Case C-411/10 [2011] ECR I-13905; [2013] 2 QB 102.

[50] Consultation Paper, para 5.5, question 2.

[51] Consultation response no. 65 – Independent Information Governance Oversight Panel, chaired by Dame Fiona Caldicott.

[52] Consultation meeting no. 29 – Department of Health.

sharing law, but not all of it.[53] Another consultee considered that organisations have a good understanding of the requirements in the 1998 Act for the collection and storing of data, but not such a good understanding of the law relating to sharing personal data.[54]

3.77 There is also an apparent problem with the distribution of knowledge, in that organisations do not know how the law can support sharing outside their core activities, for example how to share to support another's functions or to make appropriate use of existing information for secondary purposes. The Scottish Government explained

> Business areas tend to know the area of law within which they work. However business areas will not necessarily know how the law can support data sharing for research and statistical purposes because statutes rarely state explicitly that such data sharing is permitted and implied powers are relied upon instead.[55]

3.78 They added that specialist legal advice is often required.[56]

3.79 There are perceived gaps of knowledge in particular areas. For example, one consultee identified a knowledge gap in relation to pseudonymisation, pointing to limited guidance available on how to pseudonymise effectively, so as to prevent re-identification.

3.80 This is problematic in an area of law largely practised and applied by non-lawyers. Legal resources are scarce. One consultee explained that part of the problem was that although those responsible for data sharing do have a good understanding of the law, they are not always lawyers themselves.[57] Some local authority consultees explained that councils only have access to a small number of in-house legal staff and that such staff are rarely information law experts. Consultees complained that there is a general scarcity of lawyers with expertise in the field.[58]

Understanding the policy context

3.81 Legal teams were criticised by some consultees for failing to understand the policy context of data sharing projects. For example, the academic Sue Richardson observed that legal teams lacked an adequate understanding of the policy context in which their organisation is working in order to interpret the law in a constructive way, resulting in lost opportunities. There was a need, she said, for more careful advice. At consultation events, and in Birmingham City Council's response, we heard that the people with knowledge of data protection are often called in merely to draft the data sharing agreements, rather than having a direct

[53] Consultation response no. 80 – Sheffield City Council.

[54] Consultation meeting no. 21 – National Association of Data Protection Officers Conference attendees.

[55] Consultation response no. 74 – Scottish Government.

[56] Consultation response no. 74 – Scottish Government.

[57] Consultation meeting no. 7 – Amberhawk Conference attendees.

[58] Consultation meeting no. 24 – Northumbria University Information Law Centre Conference attendees.

involvement in the design and structure of the project to minimise the risk to data subjects. Data protection and the legalities of sharing personal data are, we were told, seen as an afterthought. This prevented legal input at a sufficiently early stage. One consultee, in a consultation meeting, emphasised the need for officials with strategic overview of both compliance and finding solutions to facilitate sharing. Too often compliance and problem solving roles were held by different individuals within an organisation.[59]

Limitations of the Information Commissioner's Office

3.82 As the United Kingdom's independent regulator for information rights, the Information Commissioner's Office has a wide range of responsibilities. By its own account, it seeks to promote good practice, to rule on complaints, to provide information to individuals and organisations and to take appropriate action when the law is broken. The Information Commissioner's Office has responsibility for the oversight and enforcement of the:

(1) Data Protection Act 1998.

(2) Freedom of Information Act 2000.

(3) Privacy and Electronic Communications Regulations 2003.

(4) Environmental Information Regulations 2004.

(5) INSPIRE Regulations 2009.

3.83 The Information Commissioner's Office offers several services in order to help organisations to improve their processing of personal data. The Information Commissioner's Office provides practical advice to organisations, conducts consensual audits of larger organisations, arranges advisory visits for small to medium-sized organisations and provides self assessment questionnaires to small organisations or groups within public authorities, to raise awareness of data protection issues.

3.84 The Information Commissioner's ability to support data sharing through advice is, however, limited. In the year 2012/13, 58 audits and 78 advisory visits were conducted. In addition, the Commissioner's Office publishes guidance.[60]

3.85 Some consultees wanted the Information Commissioner to be able to offer more bespoke advice and, in particular, firmer advice on whether a particular course of action would meet the various requirements of information law.[61] Birmingham City Council explained that there are occasions where a data sharing proposal is unusual or potentially controversial and the Council discusses the matter with the Information Commissioner to identify any problems with the proposal or the methods proposed to be used to permit the sharing of personal data. Birmingham City Council expressed concerns as to the ability of the Information

[59] Consultation meeting no.18 – Leicestershire County Council and Hinckley and Bosworth Borough Council.

[60] Information Commissioner's Office, *Data Sharing Code of Practice* (May 2011).

[61] For example, consultation meeting no. 21 – National Association of Data Protection Officers Conference attendees.

Commissioner's Office to provide such support in the future. In consultation meetings, a number of consultees observed how useful the Information Commissioner's Office could be in providing advice and reassurance to support appropriate sharing, but that its capacity to provide such a service was very limited.[62] Some consultees in meetings questioned whether it should be the role of a regulator to give advice on matters in respect of which it might have to take regulatory action.[63]

Training and education

3.86 Consultees regarded training and education as poor. Where there are training programmes, they complained of a compliance culture where completing training is viewed merely as a box-ticking exercise. Sue Richardson told us that in public bodies, the web-based e-learning packages favoured for almost all training were insufficient for a good understanding of the law or the development of sound professional judgment. They are referred to by data protection practitioners as a "sheep dip".[64]

3.87 The Independent Information Governance Oversight Panel found training and education to be often insufficient to give those responsible for data sharing a good understanding of the law.[65] The Panel explained:

> To address these concerns, the Review Panel concluded that there needs to be a fundamental cultural shift in the approach to learning about information governance across health and social care, to ensure appropriate sharing of information is seen as an enabler of better patient care. Health and social care professionals should be educated and not simply trained in effective policies and processes for sharing of information.[66]

FLEXIBILITY AND DECISION-MAKING

3.88 In the Consultation Paper, we asked:

> Question 3: Do you think that those responsible for data sharing are given enough leeway to exercise judgment or, in contrast, that there should not be as much flexibility when it comes to complying with the law?

3.89 Consultation responses showed a lack of confidence amongst decision-makers on the front line in interpreting the powers to disclose information. The reluctance of decision-makers to use flexible gateways and rely on judgment points towards a need for gateways that provide more structure for decision-makers. It might

[62] Consultation rmeeting no. 21 – National Association of Data Protection Officers Conference attendees.

[63] Consultation rmeeting no. 21 – National Association of Data Protection Officers Conference attendees.

[64] Consultation response no. 41 – Sue Richardson, University of Bradford.

[65] The Independent Information Governance Oversight Panel was established at the request of the Secretary of State for Health and is chaired by Dame Fiona Caldicott. The Panel conducted the Caldicott Reviews into information governance in health and social care.

[66] Consultation response no. 65 – Independent Information Governance Oversight Panel.

also support a need to find ways to increase the knowledge and confidence of decision-makers.

3.90 Many consultees felt they had enough or sufficient leeway, although a high number had criticisms of that flexibility.

The importance of context

3.91 The appropriateness of flexibility depended on the context of sharing. For example, Sue Richardson of Bradford University, explained that there needs to be as much flexibility as there is because of the variety of different situations faced by those needing to share information. Cheshire Fire and Rescue said that leeway to exercise judgement and flexibility must vary according to the situation, the data and relevant legislation. It noted that the culture and approach to data sharing is improving but is still difficult. It was important to maintain appropriate checks and balances and ensure privacy and individuals' rights. Several fire and rescue services, however, responded that there was enough leeway. Detailed legislation would be too prescriptive.

3.92 The seminars convened by DAC Beachcroft reported that reducing flexibility would not be advisable as more specific provisions could not keep pace with changes in the public sector and would reinforce an unhelpful and restrictive culture in data sharing. Restrictive flexibility would also result in the potential emergence of more criminal sanctions.

The desire for clarity

3.93 Many consultees expressed a desire for greater certainty, even if this meant a corresponding reduction in flexibility. Others wanted both.

3.94 Shropshire Fire and Rescue Service responded that there was not enough flexibility, especially where decisions were required quickly without the benefit of research and clarification, although there should be rigid and robust accountability mechanisms. The law sought to be too prescriptive. The lack of clarity in the law made officers nervous as they were unwilling to break the law inadvertently.

3.95 The Insolvency Service Intelligence Team told us that less flexibility would have advantages. Obtaining legal advice in every instance of doubt was not practicable and uncertainty means that those responsible are expected to exercise judgment to a degree beyond that which they considered desirable. The relative degree of certainty provided by a strict non-disclosure regime with explicit gateways was seen by them as advantageous, although the non-disclosure provisions of section 49 of the Companies Act 1985 sometimes prevent disclosures they believed to be in the public interest.

3.96 The Welsh Government responded that the Data Protection Act already provides a considerable amount of leeway to those who are responsible for data sharing. As a decision whether or not to share information must be made in context and on a case-by-case basis, this can lead to uncertainty as to how best to manage and decide between competing interests both for and against disclosure. In situations where consent is not being relied upon as a condition for processing, public authorities will usually need to balance an individual's right to privacy

against any legitimate interest that a recipient may have in receiving information. This can require public authorities to make a difficult judgement in circumstances where there is often no legal precedent or guidance dealing with a comparable situation for it to consider before arriving at its decision. This tension is compounded by the fact that if a public authority decides to share personal data it is very easy for a data subject to make a complaint to the Information Commissioner's Office or issue court proceedings.

3.97 The response from DAC Beachcroft invited us to consider proposing the amendment of the legislation so as to require the Information Commissioner to publish details of his consideration of Data Protection Act 1998 issues. It was said to be notable that case law from the courts in both data protection and confidentiality was lacking, so that these decisions would help to provide guidance.

Clarity and good practice

3.98 Some consultees responded that there were areas where the law was sufficiently clear and certain, such as sharing in emergencies or for civil contingency planning and response. There were also examples of good practice to reduce uncertainty, such as the Wales Accord on Sharing Personal Information (WASPI). One consultee explained that WASPI contained good templates that were easy to adapt to individual circumstances. This saved a lot of time for officials.

A PRINCIPLED APPROACH

3.99 The number of interacting legal regimes makes this a complex area of practice, but that is not unique in public law. What is different is that the provisions governing information disclosure tend to be a small part of a legal regime designed for other purposes and subject to the policy and legal requirements of those other purposes. When a data sharing gateway is developed, it is often an afterthought as part of the implementation of a much larger project. Data sharing lies across public law and interweaves with other areas. It has been difficult to develop a consistent and principled overarching approach.

3.100 In addition, this complex area of law applies to a field in which those working are predominantly not lawyers, with varying access to legal advice. Data sharing involves weighing competing public law principles. Marion Oswald of the University of Winchester described the law as principles-based, requiring a judgement to be made around concepts such as fairness or the public interest. We would add the need for proportionality and the balancing of privacy against the public interest in disclosure, required by Article 8 of the European Convention on Human Rights. [67].

CONCLUSIONS

3.101 Consultees asked for clarity. Data protection practitioners need to know the extent of their powers and their obligations, including acting in the public interest and the impact of article 8 rights and responsibilities, what discretion they have and what they need to take into account in order to reach an appropriate decision. They also need to understand the hierarchy of provisions. Lastly, they

[67] Consultation response no. 18 – Marion Oswald.

need to understand the safeguards, including monetary or criminal penalties.

3.102 The answer will lie in a variety of developments. More unified information-sharing protocols and multi-agency sharing hubs are being developed, where principles are agreed. Developing the right legal framework to support this will involve considering a principled approach to making data sharing decisions. It is not clear at this stage whether a more streamlined process would help or whether codification and simplification of the statutory and other applicable provisions support a principled approach. It is clear that any framework must take into account the balancing exercises required and ensure that appropriate safeguards are in place. There is a need for a proper review of the whole field of data sharing law and practice.

CHAPTER 4
STATUTORY GATEWAYS

INTRODUCTION

4.1 In Chapter 1, we explained the different types of gateways to share information. This chapter considers the plethora of statutory gateways for information disclosure as reported by consultees.

4.2 Two detailed case studies of Her Majesty's Revenue and Customs and the Department for Work and Pensions are provided in Chapters 8 and 9 below. These case studies help to illustrate the complexity of the statutory framework of gateways. Chapter 10 describes the issues experienced by one particular cross-government programme which required complex data sharing arrangements.

4.3 The large number of legislative gateways, spread across primary and secondary legislation, is difficult to navigate and creates complexity. There are express and implied gateways, permissive and mandatory gateways, gateways which restrict use or onward disclosure and gateways which do not. Some gateways also impose a criminal penalty for prohibited disclosure and/or for the misuse of data disclosed.

CONSULTATION

4.4 Consultees criticised legal gateways as unclear and for failing to keep up to date with changes in service provision and the information required by those changes.[1] One consultee responded that there was a need for clear legal gateways to facilitate sharing between public bodies.[2] Another responded that legal gateways contained in regulations can involve very complex provisions which can be difficult to interpret without legal training. This results in extra reliance on legal advice and increased uncertainty for practitioners.[3]

4.5 A consultee observed that legislation does not generally or clearly indicate the presence of data sharing provisions, maintaining that the time and effort required to identify the appropriate legal powers and address varying interpretations of them was disproportionate to the privacy risks involved.[4]

4.6 The seminars organised by DAC Beachcroft concluded that the culture around data sharing leads to a very strong preference for specific statutory powers. A predominant view holds that explicit powers are required. Accommodating this view has caused significant delay and additional cost. It was important to emphasise inherent powers to share data, although participants thought that the reliance on specific powers had become too embedded to be reversed by statements about inherent powers. Many people would not readily understand. It might therefore be necessary to increase the number of statutory gateways. Such

1 Consultation meeting no 27 – Birmingham City Council.

2 Consultation response no. 1 – Somerset County Council.

3 Consultation meeting no. 21 – National Association of Data Protection Officers Conference attendees.

4 Consultation response no. 74 – Scottish Government.

gateways should focus on the nature of the purposes, the key principles to be applied and safeguards available.[5]

4.7 A number of particular examples were given in consultation.

4.8 Marion Oswald commented on the "morass of overlapping legal regulation" in this field, referring to the plethora of statutory gateways permitting or mandating sharing, or disapplying restrictions on disclosure. She pointed to the overlap between section 34(2) of the Serious Organised Crime Act 2005 and section 337(1) of the Proceeds of Crime Act 2002 as an example. The sheer number and complexity of provisions relating to gateways can produce inadvertent conflicts or unintended consequences. For example, the Care Standards (Registration) (England) Regulations 2010, as originally enacted, prohibited Ofsted from disclosing parts of its children's homes register other than to a local authority in which a home is located, with the result that Ofsted was prevented from sharing that information with the police in relation to safeguarding. The Regulations were later amended to rectify this error.[6]

4.9 In another example, section 27 of the Children Act 1989 permits children's services to request help from health, education and housing agencies in discharging safeguarding duties. The section provides that "an authority whose help is so requested shall comply with the request if it is compatible with its own statutory or other duties and obligations and does not unduly prejudice the discharge of any of their functions". Marion Oswald considered that inconsistency was bound to follow, depending on the particular disclosing authority's attitude to risk.[7]

4.10 The Information Commissioner's Office pointed to a divergence of approach to the use of information obtained for council tax purposes under schedule 2 to the Local Government and Finance Act 1992, despite all local authorities working with the same legislation.

4.11 Merseyside Fire and Rescue Service pointed to difficulties in handling a variety of different gateways in complex secondary legislation, often the subject of changes and amendments.

4.12 The Welsh Government expressed concern about the ability of section 83 of the Children Act 1989 to accommodate sharing in a Ministry of Justice data sharing project arising from a recommendation of the Family Justice Review. Chester West and Chester Council responded similarly that there is difficulty in interpreting the scope of legislation in relation to safeguarding and the test of a "risk of significant harm" under the Children Act 1989. This can make it hard to persuade staff to share information early. In a consultation meeting, the NSPCC made similar comments.

[5] Consultation response no. 49 – a series of seminars organised by DAC Beachcroft Solicitors.

[6] SI 2010 No 2130, reg 7(5). This was amended by the Care Standards Act 2000 (Registration) (England) (Amendment) Regulations 2013, SI 2013 No 446, reg 2 to allow information on the register to be disclosed to the police for safeguarding purposes.

[7] Consultation response no. 18 – Marion Oswald, University of Winchester.

4.13 The General Pharmaceutical Council reported being subject to complex disclosure obligations under subordinate legislation.[8]

4.14 The Insolvency Service Intelligence Team described uncertainty where laws overlap or clash. They gave the example of section 68(3)(b) of the Serious Crime Act 2007, which provides that disclosure under the section does not breach any other restriction on the disclosure of information, however imposed. Similar clauses appear in a number of other pieces of legislation. The team explained that they had considered using this as a legal basis for sharing information that would otherwise be restricted by the non-disclosure provisions of section 449 of the Companies Act 1985. However, legal advice expressed a concern that section 449 imposed an absolute prohibition rather than a "restriction" on disclosure, which caused the team not to pursue data sharing with anti-fraud organisations. Home Office policy officials could not clarify the exact scope of the term "restriction". Without a definitive answer the only other option was to obtain advice from counsel, which was not done owing to the cost implications.

4.15 Karen Thompson also pointed to a lack of clarity in respect of the criteria that may be applied to determine whether or not inherent powers may be implied from statute and the extent to which these may or may not override the duty of confidence. Karen Thompson asked how far the duty of confidentiality was a common law fundamental right and whether it would impact on the construction of implied statutory powers to share data. It would in her view be helpful if those responsible for statutory drafting were required to include explicit statutory provisions, to distinguish in the drafting between information in general and personal and confidential data and to clarify, for example, that "expediency" has no place in relation to the use of personal and confidential data, given the "necessity" test in relation to both Data Protection and Human Rights requirements.[9]

4.16 The Department for the Environment, Food and Rural Affairs maintained that difficulty arises when considering requests for data under the Environmental Information Regulations 2004 read in conjunction with information control provisions, particularly those of the Data Protection Act 1998.[10]

DISCUSSION

4.17 The statutory framework reflects the piecemeal and ad hoc way in which it has developed. This has meant that the law has developed without consistent oversight and scrutiny, resulting in a complex web of statutory provisions. Express statutory gateways are often created to deal with a new issue or problem without systematic oversight. Such provisions often do not receive detailed

[8] In particular the Pharmacy Order SI 2010 No 231.

[9] Consultation response no. 79 – Karen Thomson, Information Governance lead at NHS England, responding in her personal capacity.

[10] The Environmental Information Regulations 2004, SI 2004 No 3391.

Parliamentary or other scrutiny in the passage of legislation.[11]

4.18 A public body must be able to point to a legal basis for information disclosure and information receipt. Receipt is usually unproblematic as a power to receive information will usually be implied, so long as the information is received for purposes that come within the lawful functions of that body. Consultees reported that it was often more difficult to identify the legal basis for information disclosure. This difficulty presents itself in a number of ways.

4.19 First, uncertainty over the scope of express statutory gateways can cause failures to share that would in fact be lawful. Accommodating rival legal interpretations can increase costs, for example where a more bureaucratic solution is required. Confusion can also increase external legal costs. Risk aversion can lead to the agreement of restrictive interpretations of the express powers available. Legal uncertainty can also become an excuse where one body is in reality unhappy to disclose for other reasons, which are consequently not adequately explored or negotiated.

4.20 Secondly, the existence of narrow express statutory gateways can be interpreted as casting doubt over the existence of general powers or implied gateways. Uncertainty and risk aversion lead to restrictive legal interpretations. Information disclosure powers implied from the general powers and functions of public bodies are avoided or only used in the clearest circumstances. There is evidence that some public bodies are reluctant to use general powers for information disclosure purposes. The general power of competence under the Localism Act 2011 provides a recent example.[12] Reluctance to use such powers stems from concern over the precise limits of the powers and the view that implied limitations could be found as a matter of statutory construction.

4.21 The introduction of statutory powers can supersede a common law power covering the same ground, so the common law may be eroded by the development of statutory gateways. Whether a particular statutory provision supersedes the common law is a matter of statutory construction, with the result that uncertainty can overshadow the use of common powers in areas where Parliament has also enacted statutory gateways to share data.[13] It is not always clear whether a given statutory regime runs in parallel with the common law or supersedes it as a matter of statutory construction. In addition, implied and common law powers to disclose information are rarely satisfactory in light of risk-averse interpretation of the law. The preference of public bodies, given this risk-averse culture, is for narrow, clearly drafted express gateways with explicit conditions and limitations. Wide powers to share information are, counter-

[11] The Welfare Reform Act 2012, s 127 introduced extensive powers for the Department for Work and Pensions and HMRC to disclose information to one another. Hansard shows almost no debate on this provision. Parliament's attention was instead focussed on the changes to the welfare benefits system being introduced by the Bill, including the creation of universal credit: Hansard (HC), 19 May 2011, col 1048 to 1058. See http://www.publications.parliament.uk/pa/cm201011/cmpublic/welfare/110519/pm/110519s01.htm (last visited 1 July 2014).

[12] Section 1 of the Localism Act 2011 provides a general power of competence for local authorites: "A local authority has power to do anything that individuals generally may do."

[13] *A-G v De Keyser's Royal Hotel Ltd* [1920] AC 508; *R v Secretary of State for the Home Department, ex parte Northumbria Police Authority* [1989] QB 26.

intuitively, more restrictive in practice as public bodies can lack the confidence to make disclosures based on implied powers or fear that a broad power will, on construction by the courts, be revealed to contain implied limits of which they were unaware.

4.22 Thirdly, there is a plethora of express statutory information disclosure powers, numerous statutory powers and functions from which a power to disclose could be implied, and statutory conditions, controls and limits on information disclosure. Statutory gateways are more accurately thought of not as powers to disclose but bundles of statutory provisions regulating disclosure in particular contexts. The gateways are not necessarily contained in a single statute for a single body. Powers, conditions, limits and controls for a particular type of information disclosure can be scattered across different statutes and various delegated instruments. It is a serious undertaking to map all of the applicable statutory material. This unnecessarily increases the cost of legal advice and research to establish a gateway and can lead to a failure to share appropriately until a public body realises it in fact has the necessary power.

4.23 Fourthly, in some areas unauthorised disclosure is also a criminal offence. There are numerous disclosure offences on the statute book and many other misuses of information gathered in an official capacity can result in fines or imprisonment. A wrongful disclosure offence often carries a maximum sentence of two years' imprisonment. It is not clear how often these offences are actually prosecuted. They do, however, appear to have a real effect on risk aversion within institutional cultures. In some contexts this could be beneficial, for example, by encouraging officials to seek departmental legal advice before making a disclosure. However, where there are inadequate legal resources or uncertainty in the application of statute, criminal offences can result in overcautious decisions. There is also a disproportionate fear of monetary penalty notices issued by the Information Commissioner's Office, with an impact on institutional culture, as discussed above.

4.24 These problems cannot be truly separated from issues relating to the legal resources available to public bodies. A County Council, for example, will have access to in-house lawyers, who have expertise in local government law, but are not necessarily information law experts, and a small team of information governance or data protection officers. Information lawyers are uncommon. This is not a problem experienced in the same way by large departments, such as HMRC, which have access to larger and more specialised legal teams. A robust and confident lawyer, with specialism in the relevant law, will be able to interpret and understand the law better and so find practical solutions to facilitate information disclosure.

LACK OF POWER TO SHARE

4.25 A public body must be able to identify a power to share information. Public body consultees often found that they could not identify the necessary power to share information for the purpose requested.

4.26 Birmingham City Council reported that local authorities considered that some of the principal obstacles to effective data sharing relate to their use and potential re-use of data disclosed by the Department for Work and Pensions or Her Majesty's Revenue and Customs. Legislative gateways for the Department for

Work and Pensions and Her Mastery's Revenue and Customs placed significant restrictions on the purposes for which information may be used or re-used. [14]

Birmingham City Council case study: utilities

4.27 Birmingham City Council gave an example which arose out of the Government's policy of tackling fuel poverty.[15]

> A utility company approached the Council to identify which of their customers were in receipt of benefits, so that the utility company could approach them to advise them of their entitlement to a cold weather grant. A number of the criteria used to determine who might be eligible for a grant related to the Department for Work and Pensions benefits and that information is held by the Council only because it was processed by the Council on behalf of the Department. The Council had agreed that if it was able to use the Department data to identify potentially eligible individuals, it would send out letters with the offer details to the residents identified, which would allow the resident to contact the service provider directly. In other words, the utility company would not be given information as to the benefits status of the customer without the consent of the customer.
>
> However, due to the restrictions imposed on the Department for Work and Pensions, in respect of benefit data, the Council was unable to determine any legal basis to permit the use of the data to perform the data matching exercise or to share the data, either under a statutory provision or under the Data Protection Act. When subsequently consulting with the Department, we were advised that they were unable to permit the sharing, or even processing of their information for this purpose.

Birmingham City Council case study: tax and debt

4.28 Public bodies often hold information which they have no power to disclose for a purpose other than that for which the information was provided to them, preventing even disclosure subject to strict limitations. As explained above, the disclosing body might choose to use the most restrictive gateway to ensure the greatest protection against onward disclosure or secondary use. Birmingham City Council gave the example of information held by Her Mastery's Revenue and Customs which it would like to use to make attachment of earnings orders.

> Attachment of earnings orders may be sought against individuals who owe Council Tax and against whom liability orders has been made, but in many cases local authorities will not have their employment details.

[14] Consultation response no. 69 – Birmingham City Council.

[15] For information on this Coalition Government policy, see: https://www.gov.uk/government/policies/helping-households-to-cut-their-energy-bills (last visited 1 July 2014).

> Were a gateway to be established through which [Her Mastery's Revenue and Customs] were permitted to provide this information, it would enable authorities to enforce such debts much more rapidly and easily, and make it much less likely that they would need to use civil enforcement agents (bailiffs) or make further use of the Courts by applying for a bankruptcy order, charging order or a warrant of committal to prison – all of which result in significant additional costs to the individuals concerned.

4.29 The disclosure of information provided for another purpose to a body wishing to use it to recover debt is, of course, a controversial area. Water companies have been keen to obtain information from local authorities as to who lives at particular premises so as to enforce water debt. Unlike other utilities, water companies cannot stop providing water to a property in order to enforce debt payment. Often, a water company will not even know whether water is being used at a property, and only where a water meter is fitted do they know how much water is being used. In consultation, we were told that attempts to persuade the Department for Work and Pensions or local authorities to provide the names and addresses of inhabitants of properties not paying for water had been unsuccessful. The problem here may be the lack of an express gateway, but there are clearly also questions about whether this is an appropriate purpose for data disclosure and whether the public interest is better served by assisting these utility companies in reclaiming the cost of the services provided, or in protecting the privacy of the individuals concerned.

Sharing information for fire prevention purposes

4.30 Fire and Rescue Services expressed a particular concern over their powers to share information for the purposes of fire prevention, which was becoming a more significant part of their public function. London Fire Brigade responded to us that it would like to be able to share personal data gained in the course of the performance of statutory duties, without the subject's consent, where the information is shared for the purpose of "preserving and maintaining human welfare". In its view the current exemption for data shared "in the vital interest of the data subject" sets too high a bar. London Fire Brigade preferred a test based on the "best interests" of the data subject.

4.31 Cheshire Fire and Rescue explained that there is some legislation that provides implicit powers for the Fire and Rescue Service applicable to data sharing. In its experience it is often more difficult to find an obligation for the supplier to share data to support preventive work, such as in the way the Crime and Disorder Act requires data to be provided to the police. Merseyside Fire and Rescue Service mentioned that fire and rescue services were not included in the list of recipient bodies in the Welfare Reform Act 2012 even though including them is recognised as necessary by most local authorities and by those involved in reviewing the 2012 Act. Shropshire Fire and Rescue Service reported some confusion over the powers available to other organisations to share information with fire services, including GP surgeries and clinical commissioning groups.

A LACK OF OBLIGATIONS TO SHARE

4.32 Permissive gateways and broad discretions as to whether to share can lead to a policy not to share. Sometimes a statutory power, or permissive gateway, is

insufficient to encourage appropriate and useful information sharing. This can occur in two different though related ways. First, the distribution of information and the structure of permissive powers can produce a dominant party in negotiations over an information disclosure or an information disclosure system. A would-be recipient public body cannot compel a public body to make a disclosure where there is merely a permissive gateway. This can create a power imbalance which results in any subsequent information sharing agreements reflecting the bargaining inequality of the parties rather than the arrangements that would best serve appropriate sharing. Different bodies have different incentives and disincentives to share and this can influence the exercise of their discretion to use permissive gateways.

4.33 Second, bodies that might be happy to make a limited disclosure, or disclosure with conditions attached, can be reluctant to use a permissive gateway that does not enable them to attach conditions on use or onward disclosure. Although any public body could seek contractual obligations to ensure this, contractual remedies might not be thought sufficient. For example, Her Mastery's Revenue and Customs prefers to disclose information under gateways which prohibit onward disclosure without permission, enforced by means of a criminal wrongful disclosure offence, in order to maintain control over the information that could not be achieved if Her Mastery's Revenue and Customs used its broad ancillary powers as a basis for sharing. This raises the question of the need for mandatory disclosure gateways in certain contexts and the need to give some bodies the ability to impose controls on onward disclosure with strong sanctions attached.

4.34 The Association of Chief Police Officers told us that one of the key issues with data sharing is not so much a lack of potential legislative powers to share but a lack of obligation to share or a lack of common understanding of those powers between different agencies. One consultee believed that there were organisations that had the power to share but often had a policy of not disclosing without consent, instancing the NHS and the Department for Work and Pensions.

4.35 The Veterinary Medicines Directorate reported difficulties in obtaining medical data from health bodies required in order to allow the Directorate to investigate adverse reactions to medicines suffered by humans and to monitor suspected adverse reaction reports to veterinary medicines in animals, humans and the environment.[16]

4.36 The Social Landlords Crime and Nuisance Group responded that many of its members, particularly housing associations, are not able to obtain useful information from the police or local authorities, although it appears that they do share similar information effectively with each other. Such problems are also found in relation to health and social care providers.[17]

4.37 Hertfordshire County Council explained that although the Crime and Disorder Act 1998 gives power to disclose information to local authorities, the Health and Social Care Act 2012 does not include such provisions. This can impede sharing information concerning vulnerable people both internally and externally, for

[16] Consultation response no. 7 – Veterinary Medicines Directorate. Restrictions here also relate to the duty of confidentiality, discussed in ch 5 below.

[17] Consultation response no. 29 – Social Landlords Crime and Nuisance Group.

instance between the NHS and a local authority.

4.38 The West Cheshire Clinical Commissioning Group saw the problem as being not that organisations do not have sufficient power, but that they may not always perceive the significance of the need to share information. Specific guidelines purely pertaining to the sharing of information between health and social care organisations would, they thought, be valuable especially in times of resource constraints where improved sharing of information may also enhance efficiency and safety.

4.39 Humberside Fire and Rescue Service responded that the law allowed sufficient leeway to make appropriate data sharing decisions, but this flexibility could be misused to allow organisations to hide behind the law. Some organisations, they said, are risk-averse and use the law to prevent sharing. Derbyshire Fire and Rescue Service also explained that there is too much flexibility to use the law in a negative way, such as by allowing organisations to hide behind the law. They had found some organisations to be risk-averse, using the law to prevent sharing. Wakefield District Council responded that it seemed in some instances to be easier and quicker to respond that information could not be shared without consent. It was unclear whether this was linked to a conscious policy or merely the understanding of applicable law and policy by the professionals concerned.

4.40 On the other hand, flexibility could be used to stretch the boundaries of acceptable sharing. The Association of Chief Police Officers responded that, although they do have sufficient leeway to exercise judgement, this can be a double edged sword in that it enables data sharing practitioners to perform their functions but can also allow the edges of lawful sharing to be blurred and boundaries pushed.

RESTRICTIVE CONDITIONS ON SHARING

4.41 Some consultees also expressed a concern over the restrictive conditions that could accompany data sharing and limit the use to which information could be put.

Birmingham City Council case study: medical data and public health

4.42 Birmingham City Council explained that Government departments, such as the Department for Work and Pensions, Her Mastery's Revenue and Customs and the Driver and Vehicle Licensing Agency, provide certain amounts of data to public authorities, but do so under restrictive conditions which impact upon the local authority's ability to use the data in further ways in order to support service user needs. There are issues, either in respect of having the powers, or the will to use their powers to permit the sharing of personal data. Birmingham City Council gave the following example:

> The transfer of Public Health functions from the NHS to Local Authorities on 1/4/2013 has indicated the difference in approach between the NHS and Local Authorities.

> Despite the transfer having been planned over 2 years prior to the transfer date, there are still discussions ongoing nationally to determine whether officers handling the Public Health function in Local Authorities are allowed access to NHS 'personal identifiable data', i.e. can the NHS share personal identifiable data with the local authority for the purposes of managing public health functions.
>
> This delay in providing this information has severe implications in respect of local authorities being able to effectively use the information provided to it.
>
> For example, we have recently obtained our latest NHS download for [Secondary Uses Service] Inpatients/Outpatients/A&E data for the current financial year. Due to the current decisions nationally this dataset now does not contain 'personal identifiable fields' (e.g. NHS Number) which the officers had access to when the public health function was performed by the NHS. As a result, this missing data means that the Council is unable to link it to other datasets it holds, e.g. social care datasets, which diminishes its usefulness, and is a considerable hindrance in the Council seeking to work collectively and use the data it has in a joined up manner.
>
> Likewise, for the same reasons, the public health staff, undertaking the same work, under the same statutory obligations, now do not have access to individual population list data for GP practices, which again limits the Council's ability to join up this data with other datasets to support commissioning care groups.

4.43 However, in consultation meetings with Her Majesty's Revenue and Customs, it was explained to us that restrictive conditions, even those which impose a criminal sanction for wrongful disclosure, can help to facilitate sharing where they give HMRC the confidence to share information it would otherwise refuse to share at all. The ability to impose conditions and enforce them effectively promotes rather than discourages sharing by Her Majesty's Revenue and Customs. The importance of taxpayer confidentiality and HMRC's reluctance to share without strong safeguards are closely linked.

LIMITATIONS EXPERIENCED BY BODIES WITHOUT COMMON LAW POWERS

4.44 The Welsh Government's response explained that one of the main barriers to data sharing that the Welsh Government faces is the fact that it derives all of its powers from statute and is therefore unable to rely upon the common law to share data in the way that a UK Government Department headed by a Minister of the Crown is able to do.[18] The Scottish Government response maintained that HMRC, being limited by their statutory functions, is unable to share data with Scottish Government or National Records of Scotland for research and statistics purposes. A number of consultees pointed to difficulties with sharing involving Her Majesty's Revenue and Customs, a statutory department without the

[18] Common law powers are described briefly in ch 1 above and discussed more fully in ch 5 below.

common law powers of ministerial departments.[19]

4.45 Wolverhampton City Council expressed the view that the voluntary sector, which has important links with local authorities in relation to service provision and delivery, has insufficient powers to share information. This can at times result in operational barriers to sharing data. A voluntary organisation is not in fact required to point to a power to act in the same way as a public body; however, in the absence of a statutory function, it is more difficult to find a clear basis for sharing that satisfies the data protection principles. This means that voluntary organisations are more likely to rely on consent and might appear to lack the "power" to disclose information.

4.46 Cheshire West and Chester Council also observed that some organisations outside the public sector, but who work in partnership with it, do not appear to have the same legal mandate to use particular gateways in the areas of crime and disorder, criminal justice, or safeguarding.

THE BENEFITS OF A STATUTORY REGIME

4.47 In the Consultation Paper, we listed a number of advantages of statute when compared with common law:

(1) Statutory provisions are more transparent; they create a simpler legal landscape making clear how the different categories of rules interact and allow the public to have a clear view of how information may be processed and by whom.

(2) Statutory provisions may specify the mechanism by which disclosure is required (for instance, notice in writing), which ensures consistency and transparency for the persons holding the information concerned.

(3) Statutes allow safeguards to be made so that the disclosure is limited to what is necessary.

(4) Statutory provisions may also offer extra guarantees of accountability before Parliament.

(5) Sanctions help enforce obligations of disclosure.

(6) Statutory provisions can give other public bodies data sharing powers which Ministers of the Crown have under the common law.[20]

4.48 These should be borne in mind in developing any new framework for deciding how and when to disclose information.

CONCLUSIONS

4.49 Each decision on whether to disclose information and the terms on which to do so has to be made on its own merits in response to the particular circumstances

[19] For example, consultation meeting no. 21 – National Association of Data Protection Officers Conference attendees.

[20] Consultation Paper, para 4.57.

at that time. A decision-maker needs to have the right knowledge and sufficient discretion to carry out a balancing exercise, weighing up the public interest in disclosure and the public interest in the protection of privacy. Flexibility is an important element in this, but so is clarity. There will be circumstances where an express obligation to disclose information, or a duty to cooperate, impliedly requiring information disclosure, are necessary to counteract the disincentives preventing the use of a permissive gateway. There will also be circumstances where it is important to leave the decision-making power entirely in the hands of the disclosing body, to use a more or less restrictive gateway as they see fit. Further work will be needed to design a framework which takes both of these needs into account.

4.50 The first step will be to map the statutory gateways carefully in order to gain an accurate picture of the current law. Questions can then be asked about the appropriate principles to apply in making data sharing decisions, in order to design a framework which balances disclosure needs with safeguards.

4.51 The vast majority of statutory gateways are permissive. An express statutory permissive gateway can provide clarity and create confidence in the disclosure of information under that gateway. A permissive gateway can also allow the data discloser to control the use of information by the recipient, by choosing to disclose via a highly restrictive gateway with a criminal penalty for wrongful onward disclosure or use.

4.52 The benefits and drawbacks of alternative types of gateway should be considered. This could include:

(1) mandatory gateways, requiring disclosure for the benefit of the statutory purposes of another body, in the public interest, and including an assessment of disadvantages to the disclosing body;

(2) duties to cooperate, setting out the purposes for which cooperation should take place and including specific information-sharing requirements;

(3) model gateways, designed for common types of disclosure, to ensure greater consistency in interpretation;

(4) the relative merits and drawbacks of wide and narrow gateways;

(5) a set of principles and criteria for determining when information can be shared, to replace specific statutory gateways.

(6) appropriate safeguards;

(7) transparency, to increase trust and confidence, both on the part of the individual whose information is subject to disclosure, and on the part of the disclosing body.

4.53 There is therefore a real question of whether the current distribution of powers, conditions and limitations is coherent, justified and as simple as it could be, while also placing adequate controls and safeguards in the right hands.

CHAPTER 5
COMMON LAW

INTRODUCTION

5.1 In addition to powers to share information under statute and restrictions on those powers, Ministerial Departments have common law powers to share information, including Royal Prerogative powers.

THE RAM DOCTRINE

5.2 In Chapter 1, we described the "third source" of government power, derived in part from the "Ram Doctrine". This originated in legal advice drafted for the Government in 1945 by Sir Granville Ram, who was then First Parliamentary Counsel. Ram advised:

> A minister of the Crown is not in the same position as a statutory corporation. A statutory corporation … is entirely a creature of statute and has no powers except those conferred upon it by or under statute, but a minister of the Crown, even though there may have been a statute authorising his appointment, is not a creature of statute and may, as an agent of the Crown, exercise any powers which the Crown has power to exercise, except so far as he is precluded from doing so by statute. In other words, in the case of a government department, one must look at the statutes to see what it may not do.[1]

5.3 Sir Granville Ram's advice was only made public in response to a Parliamentary question in 2003. In the meantime, Professor BV Harris developed the influential concept of a "third source" of power.[2] At its widest, this may be understood as the Crown having all the capacities and powers of a natural person, subject to the ordinary law and limited to the extent that there is express statutory provision.[3] However, the extent and even the existence of a third source of power have come into question more recently. In *R (New London College Limited)* v *Secretary of State for the Home Department*, Lord Sumption said, in a non-binding comment, that the third source might only extend to

> purely managerial acts of a kind that any natural person could do, such as making contracts, acquiring or disposing of property, hiring and firing staff and the like.[4]

1 Hansard (HC), 25 February 2003, col WA12.

2 B V Harris, "The 'third source' of authority for Government action revisited" [2007] *Law Quarterly Review* 225.

3 *Shrewsbury and Atcham Borough Council v Secretary of State for Communities and Local Government* [2008] EWCA Civ 148; [2008] 3 All ER 548; *Entick v Carrington* (1765) 95 ER 807; *A-G v De Keyser's Royal Hotel Ltd* [1920] AC 508; *R v Home Secretary ex parte Fire Brigades Union* [1995] 2 AC 513; though see also *R v Secretary of State for the Home Department, ex parte Northumbria Police Authority* [1989] QB 26.

4 *R (New London College Limited) v Secretary of State for the Home Department* [2013] UKSC 51, [2013] 1 WLR 2358 at [28] and [34].

5.4 Lord Carnwath went further, questioning the concept of a third source of power. In any event the third source could not be relied upon to override any other legal hurdle to information disclosure.

5.5 The House of Lords Constitution Committee considered the Ram Doctrine in 2013, concluding

> It is clear that the description of the scope of Government power denoted by the term "Ram doctrine" is unhelpful and inaccurate: it does not reflect important restrictions on ministerial powers under the common law, and creates an impression that ministers possess greater legal authority than is the case. It also fails to recognise that, whereas lawful expenditure incurred by a private person involves his or her own money, expenditure by the Government does not: it is public money.[5]

CONSULTATION

5.6 Consultees, including the Office of National Statistics and information lawyers, expressed concerns that there was a lack of clarity as the extent of common law powers and a lack of confidence in relying on common law powers to share data. Successive statutory gateways have operated both to reduce the scope of the common law and also to give the impression that where a statutory gateway does not exist, there is no power to share information.

Codification of the common law

5.7 Some consultees asked for codification of the common law insofar as it relates to data sharing.

5.8 It is not at all clear that there is a general common law power to share data without consent. Each set of circumstances would have to be examined individually in order to determine whether a common law power existed.[6] Any such power would be subject to the Data Protection Act 1998 test that sharing is necessary for a public function. However, consultation responses suggested that some believed that such a power exists. The common law powers have been eroded by legislation, but it is not entirely clear how far and what powers remain. The differing views expressed by the courts, often in non-binding statements, add to the uncertainty. Some Ministerial Departments, such as the Home Office rely heavily on their common law powers. There is a need for clarity and certainty as to the extent and effect of the common law.

[5] House of Lords, Constitution Committee, *Thirteenth report: The Pre-emption of Parliament* (24 April 2013). It may be found at: http://www.publications.parliament.uk/pa/ld201213/ldselect/ldconst/165/16502.htm (last visited 1 July 2014).

[6] For example, in *Child Poverty Action Group v Secretary of State for Work and Pensions* [2010] UKSC 54. Child Poverty Action Group challenged the Department for Work and Pension's practice of asserting that the Department had a common law right to recover overpaid benefit from claimants in circumstances where the overpayment was not recoverable under the statutory machinery contained in section 71 of the Social Security Administration Act 1992. The Supreme Court held that section 71 comprised an exhaustive statutory code and that the asserted power had never existed at common law. The practice was therefore unlawful.

Conclusion

5.9 It is beyond the scope of a project on information sharing to embark on a general review of the Ram Doctrine or the possible "third source" of government power. However, a thorough review of the law and clarification of its application to data sharing would be helpful.

PRIVATE LAW RIGHTS

5.10 Private law rights include confidentiality, intellectual property rights and contractual employment rights.

5.11 In the Consultation Paper, we asked:

> Public bodies' use of data can also be subject to private law rights, such as contractual, employment or intellectual property rights.
>
> Question 12: What obstacles to data sharing, if any, does the existence of private law rights create, and are those obstacles appropriate? If possible please give examples.
>
> Question 13: What benefits, if any, to data collection and sharing do these rights afford? If possible please give examples.
>
> Question 14: Do you use strategies to manage the effect, if any, of private law rights on data sharing? If possible, please give examples.

5.12 Few consultees demonstrated awareness of private law rights or their effects on data sharing. A small number noted that intellectual property, especially licensing agreements with private information providers, had created difficulties.

CONFIDENTIALITY

5.13 A public body may be unable to share information where disclosure would be in breach of a duty of confidence. Prior to the coming into force of the Human Rights Act 1998, the key elements of an actionable breach of confidence were that the information was of a private and confidential nature and there was a duty to maintain the confidentiality of the information because a relationship existed such as between doctor and patient, employer and employee or social worker and client. In recent years, breach of confidentiality has developed to take into account the effects of the right to privacy under article 8 of the European Convention on Human Rights, centring on the private nature of the information itself. The House of Lords explained these developments in *Campbell v MGN Limited*, which has been followed and developed in subsequent judgments.[7]

5.14 Confidentiality may be waived by consent, or may be overridden by a countervailing public interest where the law requires disclosure.[8]

[7] *Campbell v MGN Limited* [2004] UKHL 22, [2004] 2 AC 457. See eg *McKennitt v Ash* [2006] EWCA Civ 1714, [2008] QB 73 at [11]. But see Lord Phillips of Worth Matravers in *Douglas v Hello* (No 3) [2005] EWCA Civ, [2006] QB 125 at [53].

[8] The defence of "compulsion of law" is discussed in Consultation Paper, ch 4. We discuss the duty of confidence briefly in ch 1 above and in more detail in the Consultation Paper, paras 3.65 to 3.100.

Consultation

5.15 The Welsh Government noted that it is not always straightforward to determine when a duty of confidentiality arises. A group of academic researchers said that the common law duty of confidentiality placed obligations on public bodies, although there was an appropriate public interest defence, and they considered that its definition in *Re A Company's Application* was too restrictive and should be overturned.[9]

5.16 We have referred to the legally actionable breach of confidentiality in Chapter 1 above, as developed by article 8 of the European Convention on Human Rights. Confidentiality is a much broader principle particularly as between health professionals and patients. It is of great importance in relation to medical professionals, beyond the risk of common law litigation, because it plays such an important role in professional ethics and discipline, to an extent not required by any strict legal obligation.

5.17 The British Medical Association wrote:

> Confidentiality plays a fundamental role in the relationship between health professionals and their patients. The requirement for confidentiality allows patients to divulge sensitive information to their doctor without concern that it will be disclosed to others without their consent, except in very limited and exceptional circumstances. The BMA would have serious concerns if the intention was to pass legislation similar to that originally proposed in the 2009 Coroners and Justice Bill which as drafted permitted an unprecedented level of sharing of confidential health data between government departments.
>
> Whilst there may be benefits in increased sharing between some government departments to streamline processes this would not be appropriate for sensitive healthcare information. This level of sharing would seriously threaten the confidential nature of healthcare information held by the health service and has implications for both the care of patients and the achievement of key public health aims. If patients withhold information from their doctor due to fears about confidentiality then this will also have a negative impact on the quality and usefulness of the data.

5.18 Consultees saw the law relating to confidentiality as lacking clarity and expressed particular concerns over the validity of the concept of implied consent used as a basis for sharing health data, as well as over the clarity and certainty of its application.

5.19 Some consultees observed that although there is a reliance on implied consent to use confidential patient data, this concept has not been tested in the courts and

[9] Consultation response no. 35 – Ashley Savage, Dr Richard Hyde, Mr Jamie Grace, Ms Bansi Desai; in *Re A Company's Application* [1989] Ch 477 the High Court refused to grant an injunction preventing a former employee of a financial services company from disclosing confidential information about the company to a regulatory authority as it would be contrary to the public interest to prevent such disclosures, even if motivated by malice.

some legal opinion considers it to be unsound.[10]

5.20 The Information Commissioner's Office observed that the strict duty of confidentiality that applied to it by virtue of section 59 of the Data Protection Act 1998 created a tension between its duty of confidentiality and its desire to publicise its work for reasons of public accountability and deterrence.

Discussion

5.21 There are complaints of problems arising from confidentiality in the health sector, although these arise from the rules followed by, and understanding of confidentiality in, the health professions, which arguably take a stricter approach than the common law. Patient confidentiality is probably better understood as an aspect of additional professional or sector-specific duties and obligations arising from rules or codes adopted by professional, disciplinary or regulatory bodies.[11] Local authorities expressed concerns that the effect of the duty of confidentiality was interpreted differently by health service professionals from social care professionals.[12]

5.22 The law of confidentiality may however create burdens in particular areas, either due to interpretative confusion or because its requirements have not kept up with developments in administrative requirements and the nature of the delivery of services in the UK.

5.23 The concept of confidentiality has not kept pace with changing societal attitudes and the nature of service provision. For example, a case file on an individual has ceased to be a memory aide for an individual professional, such as a doctor, and has become part of integrated record management for a range of health and social care professionals and public officials, with different interests in the information it contains. The concept of implied consent has been used to manage the resulting tension between confidentiality and the desirability of wider access to an individual's health information in the context of integrated health and social care management.[13]

5.24 The application of the law on confidentiality in practice in professional-client relationships would benefit from review. For example, in medicine, implied consent is widely used as the basis for information to be disclosed from one part of a hospital to another. While both the patient and public interest might be well-

[10] For example, consultation meeting no. 20 – Health and Social Care Forum attendees.

[11] Enforceable guidance on confidentiality for doctors is provided in General Medical Council, Good Medical Practice (2013) para 50 makes reference to General Medical Council, Guidance on Confidentiality (2009), provide the standards by which doctors are assessed for the revalidation process of their licence to practise. Serious or persistent failure may put that registration at risk under Regulation 4(3)(a) of The General Medical Council (License to Practice and Revalidation) Regulations 2012, SI 2012 No 2685.

[12] This distinction was mentioned by many consultees, including consultation meeting no. 24 – Northumbria University and consultation response no. 49 – DAC Beachcroft Solicitors seminar.

[13] The draft EU Regulation on Data Protection includes increased requirements for express consent. The draft as approved by the European Parliament on 12 March 2014 may be found at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last visited 1 July 2014). See, for example, the explanation of explicit consent in the explanatory notes.

served by the disclosure, it is not at all clear that implied consent is interpreted consistently, nor that such consent has been implicitly given in every case.

5.25 There is in our view scope for clarification of the law of implied consent. One option would be codification. The law of implied consent could be modernised to put instances where implied consent is currently relied on into statute as legal bases for disclosure in their own right, obviating the need for reliance on an uncertain common law concept. On the other hand, codification could create more problems than it solves, leading to a requirement for express consent in situations not clearly covered by the new rules. Alternative ways of providing a more consistent approach to confidentiality under the current law could also be considered.

5.26 Health service consultees reported widespread public opinion in favour of the sharing of information directly related to individual patient care. National Voices, for example, reported in consultation that patients tend to believe that there is wide data sharing across the National Health Service and are frequently surprised that one part of the NHS does not have information which they have provided to another part. If a patient attends an urgent care centre provided by, for example, Virgin Health, situated in the grounds of their local hospital, the urgent health centre will take the patient's information and record it on its computer system. If the patient is referred from the urgent care centre into the accident and emergency department of that hospital, the patient will have to give the information afresh to the hospital. In most cases, the urgent care centre and the hospital accident and emergency department will not have access to each other's computer systems.

5.27 Confidentiality lies at the heart of professional relationships such as that between doctors and patients. Any review of the law of information sharing has to recognise that and to consider the interrelationship between the professional duties of confidentiality and the private law duty of confidence on the one hand and the practicalities of efficient patient care on the other.[14]

INTELLECTUAL PROPERTY

5.28 Two consultees responded that they have experienced problems with data sharing due to licensing agreements with external providers, such as the Experian MOSAIC service.[15]

5.29 Northumbria University explained that in the context of university research there are sometimes intellectual property rights that preclude or delay the publication of results. In the research field, organisations may place constraints on the publication of research data (and even findings) on grounds of commercial confidentiality. This, they said, can be appropriate, depending on who funds the research and the level of public interest in the topic of the research. However, this constraint might sometimes be applied if the findings are unfavourable from the organisation's point of view, for example by hiding bad news. When seeking to obtain patents, or to commercialise research, publication has to be embargoed

[14] General Medical Council, *Guidance on Confidentiality* (2009).

[15] Consultation response no. 76 – Northumbria University and consultation meeting no. 50 - Department for the Environment, Food and Rural Affairs, and the Environment Agency.

for a period. Disputes over intellectual property rights could also potentially affect the publication of data.

5.30 The Environment Agency explained that it had many publications, such as flood plans, which rely on intellectual property owned by third parties. Such products are routinely shared with others, including other public sector organisations, utility companies and local communities. Some terms and conditions placed on intellectual property can make it difficult to share with others.

OTHER PRIVATE LAW RIGHTS

Relating to employment

5.31 The Nottingham and Nottinghamshire Local Resilience Forum was not persuaded that private law rights had a significant effect on information sharing, although many employment contracts contain clauses to deal with intellectual property. Somerset County Council was unaware of any obstacles created by private law rights other than a need to have suitable employee screening. The London Borough of Camden reported that *Clift v Slough Borough Council* presents some challenges for the council in respect of warning frontline staff about people who are a threat to health and safety.[16]

"Ownership" of data

5.32 Misplaced ideas about information "ownership" can also be problematic. Wakefield District Council explained that the notion that people "own" data, either individually or as an organisation, confuses people. The focus needs to be on appropriate uses of data, which may be in the interests of the service user, recipient or the wider public interest. Concepts of "ownership" of personal information were raised by many consultees, without a clear understanding of whether the "owner" was the data controller, the data subject or another.

THE IMPORTANCE OF PRIVATE LAW RIGHTS

5.33 A number of consultees considered that private law rights were important to provide for individual assurance, control and redress; to encourage transparency; or to allow for commercialisation, for example in relation to intellectual property.

5.34 Wakefield District Council expressed the view that the private law and public law frameworks operating around data can be helpful in providing for a more explicit discussion of what is to be done with data and how it is to be protected. For example, if a contract or other agreement is being used to provide for data to be shared and processed, this enables clear recording of the basis on which these activities will take place and what limitations and protections are in place. The

[16] In *Clift v Slough Borough Council* [2010] EWCA Civ 1484; [2011] 1 WLR 1774, the Court of Appeal considered the effect of a local authority's obligations under article 8 of the European Convention on Human Rights on the defence of qualified privilege to a defamation claim. The court accepted that the protection of council employees from a potentially violent individual was a legitimate aim, justifying interference with the claimant's article 8 rights. However, communications made in the absence of a duty to publish to those persons and publication to the council's partner organisations (including environmental and refuse collectors, estate maintenance, NHS Primary Care Trust and Community Safety Partnership) were not proportionate to the legitimate aim and the defence of qualified privilege was not available.

process of setting up agreements can be very hard work if there is not a clear shared understanding of the legal frameworks and how these issues will be dealt with in practice. Wolverhampton City Council expressed the view that private rights can provide some clarity when sharing information that is subject to these laws. The Scottish Government response said that if individuals are properly informed in fair processing or privacy notices then it can assist in data sharing as long as the notice makes clear to the data subjects what information will be shared and for what purpose.

5.35 Northumbria University maintained that some degree of commercial confidentiality is necessary to obtain agreement for certain research to be conducted. However, if the research is publicly funded this should not result in complete lack of publication, but in publication with no possibility of the organisation being identified. Embargos to protect patent applications or commercialisation are necessary, but should only be temporary until the patent is awarded or refused or the company has a good head start in commercialisation.

MANAGING PRIVATE LAW RIGHTS

5.36 Consultees felt that individual rights could be accommodated adequately through compliance with the data protection principles and implementing proper policies and guidance. For example, the Welsh Government explained that it had issued guidance for all staff who need to assess privacy impacts in the context of policy development or project management processes. The guidance provides information on how privacy impacts should be assessed, including the arrangements for applying a formal Privacy Impact Assessment ("PIA"). PIA screening is mandatory for certain policies and projects. A PIA screening tool has been developed to identify those aspects of a proposal which are likely to have an impact on privacy or which could result in non-compliance with the Data Protection Act 1998. In addition to the Act it would be relevant to take into account other laws which confer private rights on individuals, such as contract law, the tort of negligence and the law of confidence.

5.37 Northumbria University explained that although disputes over intellectual property do occur in research, they could be dealt with by appropriate legal agreements being set up at the start of a project.

5.38 Some consultees were of the view that private rights were sometimes used as an excuse not to share. Sue Richardson saw a need for steps to be taken to ensure that private law rights are not used as an excuse to prevent sharing.[17]

CONCLUSIONS

5.39 With the exception of confidentiality, private law rights do not appear to place significant inappropriate hurdles in the way of effective data sharing. This is an area where awareness of appropriate available guidance might be improved as well as training. The relevant borderlines could be clarified between data protection and intellectual property law, where, for example, commercial licences prevent data sharing. A review of intellectual property law is beyond the scope of this project.

[17] Consultation response no. 41 – Sue Richardson, University of Bradford.

CHAPTER 6
ANONYMOUS INFORMATION

DEFINITIONS

6.1 One of the complexities surrounding anonymous data is the variety of terms applied to data that have undergone some process designed to anonymise those data. A large number of technical terms can confuse discussions of the law in this area. The purpose of this section is to define commonly used terms and relate them to the legal definitions found in the Data Protection Act 1998.

6.2 The Preamble to the Data Protection Directive recites:

> Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;[1]

6.3 When determining whether data constitute personal data subject to the Directive, one should include consideration of steps reasonably likely to be taken to identify a person from the data, including advances in technology available to the potential data controllers.

6.4 Article 2(a) of the Directive defines “personal data”:

> 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[2]

6.5 “Personal data” is defined by section 1(1) of the Data Protection Act 1998 as

> data which relate to a living individual who can be identified from those data or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller including expression of opinion or intention.

6.6 It is the duty of the data controller to comply with the data protection principles in

[1] Data Protection Directive 95/46/EC, para 26.

[2] Data Protection Directive 95/46/EC, art 2(a).

relation to all personal data with respect to which he or she is the data controller.[3] No obligations in the Data Protection Act 1998 apply to non-personal data**,** such as information about businesses (other than sole traders) or information relating to deceased persons.

6.7 Non-personal data are frequently referred to as "anonymous data". Definition of anonymous data is not found in the 1998 Act but is derived from the definition of personal data in the 1998 Act. We suggest that non-personal data is a broader category than anonymous data, as it could include data that do not relate to an individual at all, whereas anonymous data is used to refer to, and implies, data which do relate to an individual, but one who cannot be identified from those and other data.

6.8 It is important to note that the same data can be personal data in relation to one data controller and anonymous data to another data controller simultaneously. The definition depends on whether identification is possible given the information held or likely to come into possession of the particular data controller.

6.9 It also follows that data which are anonymous in relation to a data controller at one point in time could become personal data if that controller receives additional information (which was previously unlikely to come into his or her possession) which allows the identification of the data subjects.

6.10 Anonymous data can be collected from the start as anonymous information (for example through an appropriate anonymous survey) or can result from the processing designed to render the data anonymous (an anonymisation process).

6.11 Personal data that have been through an anonymisation process may or may not be successfully rendered anonymous, depending on the success of the techniques employed. Data might be successfully anonymised in relation to some potential data controllers but not others, where different controllers possess different additional information. When discussing anonymised data it is important to remember that the anonymisation process itself will be an act of processing personal data which must comply with the data protection principles in the Data Protection Act 1998. It is only to the extent that data are no longer personal data, following a successful anonymisation process, that anonymous data fall outside the scope of the Act.

6.12 A variety of terms are used to describe data that have been subject to various anonymisation techniques.

(1) **De-identified data** is used to describe personal data that have been processed to remove personal identifiers, such as name, gender and postcode.

(2) **Re-identifiable data** is sometimes used to described data that have been de-identified but could be re-identified by a third party, making the data personal to that extent.

[3] Data Protection Act 1998, s 4(4).

(3) **Pseudonymous data** is used to describe personal data which have had the names of data subjects altered to obscure their identity.

(4) **Key-coded data** is used to describe personal data which have been pseudonymised using an electronic key algorithm. This replaces the names of data subjects with a unique identification number, such as 24601, generated automatically by the code. Whether key-coded data is anonymous is dependent not only on whether this pseudonymisation is sufficient but also on whether the key is retained or destroyed by the data controller and who else might have access to the key or be able to recreate it.

ANONYMOUS DATA AND DATA PROTECTION

6.13 If information is no longer personal data within the meaning of the Data Protection Act 1998, the data protection principles do not apply to it. Truly anonymous data is outside the scope of the Data Protection Act 1998 but it is very difficult to achieve anonymisation that takes data relating to individuals outside the definition of personal data.

6.14 Technological advances have made re-identification easier, so that the risk of re-identification of an individual from anonymised or pseudonymised data continues to increase.

6.15 "Big Data" techniques and analytics using large datasets and vast amounts of metadata generated by electronic communications enable the re-identification of far more personal data than ever before.[4] The rapid development and sophistication of these technologies present real challenges for anonymisation techniques and the increasingly outdated legal landscape.

6.16 The Information Commissioner's Office has published guidance on anonymisation, recognising that anonymous information is not an absolute category, but that there is a sliding scale of risk of re-identification.[5]

6.17 The UK Anonymisation Network has been working with the Information Commissioner's Office, universities, private companies and others to provide both technological and legal support in safely anonymising data. The Network commented that the definition in the Consultation Paper is too limited;[6] they proposed three different types of anonymisation when thinking about anonymous data:

(1) Formal anonymisation where unique identifiers such as postcodes are removed from a record.

[4] Metadata is data automatically generated by the use of technology. For example, a mobile telecommunications company will have a record of where a mobile phone was at the time when a call was made, what number was called and how long the call lasted. For examples of the uses of metadata and the controversy surrounding them, see the series of articles by The Guardian newspaper on its investigations of surveillance carried out by the the United States National Security Agency: http://www.theguardian.com/world/the-nsa-files (last visited 1 July 2014).

[5] See http://ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation (last visited 1 July 2014).

(2) Statistical anonymisation where there is some statistically quantifiable risk of re-identification, however small.

(3) Absolute anonymisation where there is absolutely no risk of re-identification, which is only realistically achieved when the data are not made public at all.

6.18 The Network insisted that there is no such thing as truly anonymous data. The aim should be to produce data which are anonymous enough in proportion to their sensitivity.[7] They also explained that the classification of data as anonymised should be considered in context. This includes:

(1) the security infrastructure for holding the data;

(2) who will have access to the data;

(3) the sort of analysis the will data be subjected to;

(4) what other data might co-exist which could be combined with the "anonymous" data, including other co-located data or publicly available data.

6.19 The Network added that the Data Protection Act 1998 does not provide enough detail for people to understand what they need to do in order to make data anonymous. There is no adequate test or definition of "anonymous". We note that the Information Commissioner has published a Code on Anonymisation, which provides helpful guidance. However, many data controllers do not possess the technical expertise to evaluate their attempts at anonymisation effectively.

6.20 There is a lack of clarity in technical and policy discussions of anonymisation about whether anonymisation is being discussed in order to determine whether data is within the scope of the Data Protection Act 1998, to establish that adequate security measures are being taken in relation to de-identified data that remains to some extent personal data, or to apply best practice beyond strict legal requirements. This is an area we would seek to clarify in a full project.

POWERS TO PRODUCE AND RELEASE ANONYMISED DATA

6.21 The Information Commissioner identified as a problem the inability of certain public authorities to use personal data in their possession to produce even anonymised data if the resultant data are not to be used for the authority's own statutory purposes. The Commissioner's view is that, provided the information is anonymised to a satisfactory standard, public authorities should be allowed to share and publish anonymised information derived from the personal data they hold. Public bodies currently lack a clear legal basis to produce and release

[6] Consultation Paper, para 1.16.

[7] Consultation meeting no. 41 – UK Anonymisation Network, University of Manchester. We note that the legal definition of non-personal data is unaffected by the sensitivity of the underlying data. The sensitivity of the data may be of relevance where anonymisation techniques are used as a security measure on personal data to meet the requirements of the 7th data protection principle, to determine what level of security is reasonable.

anonymised datasets.[8]

PRESSURES TO USE IDENTIFIABLE DATA

6.22 The Independent Information Governance Oversight Panel responded that there are many good reasons why organisations in health and social care need good quality data. Patients are at risk if clinicians base their decisions on inadequate data. Dangers multiply if there is poor handover of information between care teams or conflicting advice to patients from professionals. The issue is particularly relevant to this review because poor data are cited by managers in health and social care as a reason why they need access to information about individuals. If they cannot trust the accuracy and relevance of anonymised data, they may think the only way to discover the truth is to look at a selection of real cases involving real people. For this reason, poor data quality may be used as an excuse for ignoring the principles of sound information governance. The Review Panel found the excuse unsatisfactory. They saw the correct solution to these problems as being to improve the quality of data and not to compensate for poor data by adopting poor information governance.

> Commissioners [of National Health Services] told the Review Panel that because the quality of local demographic or administrative data is sometimes poor, they often require three identifiers to ensure they are distinguishing the correct individual. This means that instead of using de-identified data for limited disclosure or limited access, for which Commissioning Support Units could have a legal basis, commissioners are reliant on personal confidential data for which they may have no legal basis.[9]
>
> All providers need to ensure that their patients are correctly identified… to improve data quality and hence remove the requirement for commissioners to have personal confidential data.
>
> During the evidence gathering the Review Panel heard frequent complaints that local data sets are too poor to enable data linkage without multiple direct identifiers which therefore creates a dependence on personal confidential data being used.
>
> For example, research has shown that when planning services it is possible to link data and match individuals using de-identified data for limited disclosure or access and the NHS number as an identifier in up to 99.8% of cases. However, this still leaves a minority of cases, such as Cancer Registries looking for individuals suffering from rare forms of cancer, where this approach will be insufficient, and individuals have to be matched using personal confidential data.

[8] Consultation meeting no. 10 – Information Commissioner's Office.

[9] The Department of Health published The Information Governance Review: To Share or Not to Share (Caldicott 2) in March 2013. Dame Caldicott chaired that review panel and subsequently accepted the Secretary of State's invitation to chair The Independent Information Governance Oversight Panel.

> The quality concerns cannot simply be addressed by an improvement in data quality. The organisation receiving the data must also be able to rely upon the data as being of an appropriate quality (i.e. fit for purpose). It is not enough that an organisation is receiving data that is good enough. They must have a way of knowing that it is good enough. This may be difficult for the sender organisation to demonstrate in a straightforward way (because they may not know exactly what the receiving organisation intends to do with the data). This is a problem that must be grappled with in the Open Data initiative more generally and it would be helpful for the law to develop cognisant of this need.

6.23 Supporting adequate anonymisation is therefore an important way of reducing reliance on personal data, with the increased risks it brings for privacy.

DATA SHARING FOR RESEARCH AND STATISTICAL PURPOSES

6.24 The sliding scale of risk posed by various levels of anonymised data is one of the problems identified by those sharing data for research and statistical purposes. The data might be processed as personal data but then anonymised and analysed.

6.25 Several consultees thought that the right balance was not struck in the case of data sharing for statistical purposes. The Scottish Government, for example, said that the "current patchwork of legal powers to share data for research and statistical purposes" creates disproportionate burden to public bodies who want to share data for legitimate research and statistical purposes and does not provide clarity and transparency to data subjects.

6.26 The Office of National Statistics (ONS) raised questions about the lack of an obligation upon others to disclose information to it. It argued that the ONS is in a unique position because data sharing for statistical purposes, if carried out correctly, has no direct impact on an individual.

> ONS considers sharing information for statistical purposes to be fair. A principle existing in law would be welcomed. In particular, ONS would want statistical purposes to get similar recognition to some other special purposes (for example, journalism) do in the Act. The Act does not distinguish statistics produced by government departments from statistics and research performed by non-public sector organisations. There is a public interest consideration for Official and National Statistics which in the opinion of ONS should be reflected in the Act. Therefore ONS contends that the processing of personal information for statistical purposes is always 'fair' under the first Principle, as long as the necessary conditions for statistics are met absolutely (further use for statistical purposes only, and a guarantee of confidentiality in any published products).[10]

6.27 ONS considered sharing information for statistical purposes to be fair and said that a statement of principle to that effect in the law would be welcome. The Data

[10] Consultation response no. 55 – Office for National Statistics.

Protection Act 1998 does not distinguish statistics produced by government departments from statistics and research performed by non-public sector organisations. ONS argued that there is a public interest in official and national statistics which should be reflected in the Act. It contended that the processing of personal information for statistical purposes is always 'fair' under the first principle, as long as the necessary conditions for statistics are met, such as further use for statistical purposes only and a guarantee of confidentiality if the information is made publicly available.

6.28 It is not current practice to obtain consent from users of public services for disclosure of their information to the ONS. ONS must rely upon other departments either having a statutory gateway or rely upon them concluding that the data access is in the public interest. The Office for National Statistics argued that good quality national statistics are fundamental to the effective government of the country and the delivery of public services and that disclosure to the Office was therefore in the public interest.

6.29 ONS found it rare for any statute to specify disclosure of data to it for the production of statistics. In practice, they have found that the key has been convincing ministers and officials of the value of including a data sharing clause in each Bill. ONS told us that ministers and officials are reluctant to agree to the inclusion of data sharing clauses in Bills due to the complexities and uncertainties associated with these clauses, which can threaten to lengthen the time it takes for the Bill to be passed. ONS argued that provisions for sharing data for the purpose of national statistics should be included in all relevant new legislation in terms approved by the Chief Statistician. ONS currently relies on implied or common law powers, which many bodies are reluctant to use.[11]

6.30 The Scottish Government also saw the lack of explicit powers to share data for statistical and research purposes as a greater obstacle to gathering statistics than statutory barriers. Bill teams "shy away" from including explicit statutory powers to share for research and statistical purposes, the Scottish Government told us, out of a fear that these will make passage of the legislation through Parliament more difficult. Recent understandings with Bill teams that data sharing needs to be explicit when drafting legislation have, we were told, assisted in progressing data sharing in Scotland. The lack of explicit powers makes sharing more difficult. Health research frequently involves sharing data between health boards and/or between the NHS and researchers in universities or commercial organisations. Data controllers in health boards can adopt differing views on a particular use of data, or even disagree about who should be taking the decision. The delay, and resulting costs, associated with such disagreements are a significant obstacle to research involving shared data.[12]

CONCLUSIONS

6.31 Technology has developed apace since the 1995 Data Protection Directive and its transposition in the United Kingdom in the Data Protection Act 1998. Information can no longer be truly anonymous if it is shared. The law on anonymisation needs to be reviewed so as reflect a sliding scale of risk with

[11] Consultation response no. 55 – Office for National Statistics.

[12] Consultation response no. 74 – Scottish Government.

regard to anonymous data. Thought should be given to whether similar balancing tests should be applied to anonymised or pseudonymised data as to personal data, and what other considerations should be applied where information is to be used for purposes not directly related to the individual concerned. Although much of this depends on legislation at the level of the European Union, a full law reform project could explore the scope for a more risk-based approach in dealing with data that are de-identified but may nevertheless remain within the definition of personal data.

CHAPTER 7
PROBLEMS OTHER THAN THE LAW

INTRODUCTION

7.1 In this part, we consider other reasons why organisations and those working within them do not disclose information, irrespective of whether they have the power to do so in law. These reasons have a significant effect on whether information is shared and cannot be dismissed as matters to be resolved with better training and guidance. We also consider the incentives and disincentives which affect decision-making. Any system of effective information disclosure must be developed with these individual and organisational concerns and behaviours in mind.

7.2 Although the barriers we identify in this Chapter are not legal barriers, or primarily caused by the legal regime, a full law reform project may be able to suggest reforms that mitigate the effect of some of these barriers. Any effective law reform process must also recognise the non-legal pressures, incentives and disincentives at play and be aware of the organisational culture around data sharing. It would not be possible to proceed without the valuable understanding and insights we gained through consultation.

INDIVIDUAL RELUCTANCE AND PUBLIC TRUST

Public awareness of data sharing

7.3 Consultees noted that the public had become more informed and had greater awareness of data sharing. We think this is a positive development. The London Borough of Camden responded that individuals are becoming more aware of their rights and are becoming more vocal in challenging the way in which the authority is using their data.[1] Cheshire Fire and Rescue responded similarly but noted its experience that where sharing is for the individual's benefit, and not for profit or marketing purposes, individuals are supportive.[2] Another consultee responded that this greater awareness was a positive development, as it encouraged organisations to strike an appropriate balance between the privacy rights of individuals and the public good.[3] A number of consultees attributed this to high profile cases reported in the media, which had made the public more aware of privacy and data protection issues. We recognise the increased public awareness of data sharing issues.

7.4 A number of fire and rescue services cautioned however that some individuals are inherently suspicious of the public sector and its uses of personal data.[4] There can be a false assumption that public bodies generally share data, making individuals reluctant to supply information in the first place to forestall any sharing. One consultee added that this is particularly the case in relation to

1 Consultation response no. 37 – London Borough of Camden.

2 Consultation response no. 26 – Cheshire Fire and Rescue Service.

3 Consultation meeting no. 7 – Amberhawk Conference attendees..

4 Consultation response no. 10 – West Midlands Fire and Rescue Service; consultation response no. 72 – Manchester Fire and Rescue Service.

information requested in support of the duties under the equalities legislation, which is either not completed or struck through by individuals.

Individual reluctance

7.5 Problems are caused by individual reluctance. A group of academic researchers told us in relation to whistle blowing that anonymous reporting of concerns, fuelled by concern that the whistleblower will be identified, caused problems because anonymous complaints might be rejected by regulators or because anonymity made it difficult to secure consent for further sharing or onward disclosure.[5] Shropshire Fire and Rescue Service responded that mistrust by individuals puts pressure on public bodies not to share information.[6] There is a fear or concern that sharing will lead to intervention by other agencies. A number of consultees noted that individual reluctance could result in incomplete or inaccurate data which harmed the quality and usefulness of the data collected.[7]

Public perceptions

7.6 Consultees reported widely that the public claim high expectations that public bodies will protect their data but also express frustration where they feel bodies should "talk to each other" but fail to do so. It is entirely appropriate for the public to hold high expectations of public bodies. The law should facilitate high standards and appropriate sharing.[8]

7.7 For example, the Social Landlords Crime and Nuisance Group reported that, although it recognised a growing concern over the potential for personal data to be misused, there was also a real sense that the public expect public agencies to talk to each other. They told us that the public are equally frustrated by the obstacles presented by inconsistent and inaccurate application of data protection principles. This is especially the case where an individual must repeat the same information to a number of related services.[9] The London Borough of Camden told us that some individuals see the council as "one organisation" and others do not. They saw a need for a balanced approach so that proportionate sharing can take place and individuals do not have to repeat information when engaging with different parts of the council.[10]

7.8 Several consultees considered that identity fraud was a significant concern for individuals. They had high expectations that public bodies will keep information secure and will not share it inappropriately.

7.9 Sue Richardson of Bradford University perceived an increasing lack of public

5 Consultation response no. 35 – Regulation and Enforcement Group of Researchers.

6 Consultation response no. 6 – Shropshire Fire and Rescue.

7 Consultation meeting no. 7 – Amberhawk Conference attendees.

8 Resarch on public attitudes to data protection suggests that the public opinion varies enormously, as do public attitudes and behaviours when asked to share their own personal data. See for example, Ian Brown, "Privacy attitudes, incentives and behaviours" (2011) at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1866299 (last visited 1 July 2014) and Demos, *Private Lives: a People's Inquiry into Personal Information* (2010) p 21. These issues are discussed in ch 2 above at paras 2.6 to 2.15.

9 Consultation response no. 29 – Social Landlords Crime and Nuisance Group.

trust. Acknowledging that the public have a poor understanding generally of data sharing, she expressed the view that it would be worrying if the public did not question data sharing at all. Data protection practitioners on the ground reported to her that many members of the public assume that public bodies already share most if not all the data they hold with other public bodies, leading to frustration when they are asked to 'tell their story' numerous times to different bodies and annoyance when communication between public bodies is not good because information has not been shared.[11]

7.10 Northumbria University cautioned that attitudes towards the sharing of information vary significantly between different groups of people.[12] They noted a marked difference in attitudes between different age groups and referred us to the research of Briggs, Coventry and Little, *Who Knows About Me.*[13]

7.11 It is important not to rest on an oversimplified impression of the range of public attitudes to data sharing. Any reform should be carefully considered, with full consultation.

BARRIERS TO EFFECTIVE AND APPROPRIATE DATA SHARING

The structure of public services

7.12 Some barriers to effective data sharing are caused by the structure of public administration and the way services are delivered. Particular difficulties arise in the commissioning and the contracting out of public services and in large sectors where the service is fragmented between numerous public bodies, for example in the NHS. The public-private divide is increasingly blurred in the provision of public services. This can create problems for private or third sector providers or partners. It can be extremely difficult simply to map all the relevant public bodies involved in, for example health or child safeguarding, and to know where information is held and by whom. Some consultees in the health sector reported confusion over who the data controller was in relation to particular information in the National Health Service.

7.13 Practices can vary enormously. As Richard Carthew of the Health and Social Care Information Centre explained:

> I think the NHS is so big and, in particular, so unbelievably fragmented, that people outside the NHS find it difficult to realise how many relationships they have to build. You have to build relations in each organisation, and each professional group, ie acute hospitals, community services, mental health services, GPs, social care departments; and then doctors, nurses, therapists, managers …

[10] Consultation response no. 37 – London Borough of Camden.

[11] Consultation response no. 41 – Sue Richardson, University of Bradford. The public perception that public bodies share more data than they do in fact was widely reported to us in consultation meetings.

[12] Consultation response no. 76 – Northumbria University.

[13] Briggs, Coventry and Little, *Who Knows About Me – an analysis of age-related disclosure preferences, in British Computer Society, Proceedings of the 25th British Computer Society Conference on Human-Computer Interaction* (2011).

> There's no single point of access for a public servant – nor, of course is there for a patient nor the public … The "NHS" isn't an entity.

7.14 Some consultees explained that public trust decreases where services are outsourced to the private sector. Nottinghamshire Local Resilience Forum reported that public concern focussed on the physical security of data and the transfer of data to private third parties. UK Anti-Doping maintained that public concern related to control. The public are content to share even sensitive personal data as long as they remain in control of the sharing of those data. However, once the responsibility for sharing the data falls to a third party, no matter how trustworthy they are, the attitude of individuals becomes very risk-averse.[14] The reluctance of an organisation to share personal data may be affected by the relationship it has with the individuals it deals with. Northumbria University reported anecdotal evidence that the outsourcing of public services to private organisations alters the trust the public has in these services. People trust private organisations less as they feel their data will be used for other commercial activities.[15]

7.15 Mind also pointed out to us that the NHS is a multiplicity of bodies and that in the care sector services are commissioned from a wide range of organisations. Privately run organisations commissioned to provide services provide diverse information about their data protection policies, which can cause confusion for consumers. They may also subcontract to other private service providers. Mind gave an example of a caller to its Legal Advice Line who complained that a private agency had been given her name and address to conduct a feedback survey of her use of a psychiatric service. The result of increased privatisation and segmentation of health and social care is that it is more likely that sensitive health information will be shared with a range of different organisations, increasing the potential risk for unlawful disclosures.[16]

7.16 In the recent controversy over proposals to add personal information collected by general practitioners to a database of personal information collected by hospitals, managed by the Health and Social Care Information Centre, the media reported widespread concerns that information would be provided to private medical research bodies, including pharmaceutical companies who, it was feared, would use information for making decisions about matters such as medical insurance.[17]

[14] Consultation response no. 9 – Nottingham and Nottinghamshire Local Resilience Forum; consultation response no. 60 – UK Anti-Doping.

[15] Consultation response no. 76 – Northumbria University.

[16] Consultation response no. 71 – Mind.

[17] See for example, Nick Triggle, Health Correspondent for the BBC: http://www.bbc.co.uk/news/health-26259101 (last visited 1 July 2014); Sophie Borland in the Daily Mail http://www.dailymail.co.uk/news/article-2562296/Controversial-plan-share-medical-records-NHS-hold-six-months.html (last visited 1 July 2014)and Ben Goldacre in The Guardian http://www.theguardian.com/commentisfree/2014/feb/28/care-data-is-in-chaos (last visited 1 July 2014).

Guidance and administrative rules

7.17 There are also issues concerning guidance and administrative rules and requirements. For example, the perceived lack of clarity and specificity of Information Commissioner's Office guidance and the administrative rules and requirements for access to NHS computer systems can create barriers to data sharing. Consultees often complain that guidance is insufficiently concrete and prescriptive to answer particular concerns. There is reluctance in a risk-averse field to take responsibility for decision making based on broad principles or abstract or high-level guidance.

INCENTIVES AND DISINCENTIVES TO SHARE

7.18 In consultation, we found that many of the problems encountered in data sharing were due to disincentives to share and a lack of incentives to share. A significant problem with the current framework of statutory gateways is its lack of appreciation of and responsiveness to the economics of data sharing relationships between different public bodies.[18]

7.19 Consultees considered that, given the resource implications of sharing and the different remits and priorities of public bodies, it was essential to achieve commitment and support at all levels for data sharing projects and to quantify the benefit of that sharing. Difficulties in achieving this could operate as a barrier to sharing.

7.20 It is seen as essential to gain commitment and support for data sharing from the supplying body at all levels. For example, Cheshire Fire and Rescue told us of its experience that, without clear definition of the benefits expected from data sharing, there was no incentive for the supplying body to allocate resources to provide data or to accept the risks relating to discretionary data sharing.[19] Some other fire and rescue services regarded this as a recognised barrier to sharing, where organisations failed to recognise the wider community benefits. Patient data from the NHS were given as an example.[20]

7.21 Differing priorities or policy remits can also cause problems for data sharing. The Association of Chief Police Officers pointed to a lack of motivation where organisations with differing remits wished to obtain data from one another, caused by a lack of understanding of the needs of the requesting agency and of the public interest benefits in a particular case. Local partnerships were helping to address these sorts of issues. Historically public bodies put their resources into areas likely to be subject to public inspection. There appeared to be little investment in effective information sharing.[21]

7.22 Differing business models can also create hurdles to effective information sharing. The Department for the Environment, Food and Rural Affairs told us of a number of occasions where a body had been unable to obtain necessary data from another government body whose business model enabled or required data

[18] Resources and economic issues are discussed below at paras 7.39 to 7.53.

[19] Consultation response no. 26 – Cheshire Fire and Rescue Service.

[20] Consultation response no. 72 – Manchester Fire and Rescue Service.

[21] Consultation response no. 45 – Association of Chief Police Officers.

supplies to be charged for, or delivered with some receipt in return. The lack of resources to pay or equivalent data to 'trade' resulted in the data not being provided.[22]

7.23 A lack of incentives can contribute to failure to share data appropriately. For example, NHS Protect encourages health bodies to participate in the Audit Commission's annual National Fraud Initiative (NFI) data-matching exercise. The NFI requires significant input from health bodies but does not usually produce a large return for them, as most matches identify benefit or tax credit-related frauds, rather than frauds against the NHS. This discourages health bodies from giving this work priority.[23]

7.24 The Department of Health noted that although there is no need to incentivise NHS and social care organisations to share information, there is anecdotal evidence that some smaller health and social care providers are concerned that the resources required to support information sharing may impact on their ability to provide frontline services. It may therefore be necessary for information sharing projects to consider whether additional resources should be made available to help organisations meet the additional costs of providing data.[24]

7.25 Unavailability of feedback on the outcome of data sharing can leave organisations unaware of its impact. Shropshire Fire and Rescue Service saw the lack of feedback as fuelling a reluctance to use resources to provide information whose supply did not further the supplying organisation's aims and objectives.[25]

RISK AVERSION

7.26 Many consultees pointed to the risk aversion shown by public bodies or individuals within them and gave further examples.

7.27 Shropshire Fire and Rescue Service found GP surgeries very reluctant to provide either anonymised data for strategic planning and safety strategies or information relating to high risk and vulnerable people, even where legislation permitted it, preventing early intervention or delaying action for those most at risk.[26] West Midlands Fire and Rescue similarly perceived obstacles to receiving information from the health sector.[27]

7.28 Gaist Solutions regarded most such obstacles as cultural and practical rather than legal. Public bodies are very protective of the data they hold and there has been duplication of data protection measures.[28] The Office of National Statistics also described having to duplicate work where data were already held by other Government departments, because of a reluctance to share.[29]

7.29 The Welsh Government identified the difficulties of balancing competing interests and a fear of making the wrong decision which could result in a breach of the Data Protection Act 1998 and a possible Information Commissioner's Office fine as obstacles to data sharing, pointing out that media stories often focus on cases

[22] Consultation response no. 62 – DEFRA.

[23] Consultation response no. 58 – NHS Protect.

[24] Consultation response no. 77 – Department of Health.

[25] Consultation response no. 6 – Shropshire Fire and Rescue.

where personal data have been incorrectly shared and that this will resonate with the decision maker.[30]

7.30 Sheffield City Council similarly saw staff uncertainty and a risk-based approach as leaving data not shared when they ought to be.[31]

The culture of anxiety

7.31 Some identified a culture of anxiety surrounding data sharing and leading to risk aversion and to the use of flexibility to adopt restrictive interpretations and practices. For example, Marion Oswald described a crisis of confidence in data sharing, as well as "professional silos" which do not communicate.[32]

7.32 In a number of our consultation meetings fears were expressed over the scope of personal and criminal liability for wrongful disclosure. [33]

7.33 Northumbria University saw examples of a consequent highly risk averse approach to information sharing in a range of Inquiries emerging over the last few decades in the field of child protection, where a failure to share information had been a common feature.[34] However, consultees working for local authorities reported widely that confidence in sharing information for the purposes of safeguarding children had increased significantly.[35]

7.34 The Independent Information Governance Oversight Panel likewise described a culture of anxiety about data sharing as permeating many health and social care organisations from the boardroom to front line staff. In its report, the Review Panel traced this anxiety to instructions issued by managers in an attempt to protect their organisations from fines for breaching data protection laws.[36] They saw the resulting 'risk-averse' approach to information sharing as preventing professional staff at the front line from co-operating as they would like and using their clinical judgement.[37]

7.35 Several consultees, both at consultation events and meetings, referred to

[26] Consultation response no. 6 – Shropshire Fire and Rescue.

[27] Consultation response no. 10 – West Midlands Fire and Rescue Service.

[28] Consultation response no. 16 – Gaist Solutions, Stephen Berry.

[29] Consultation response no. 55 – Office for National Statistics.

[30] Consultation response no. 43 – Welsh Government.

[31] Consultation response no. 80 – Sheffield City Council.

[32] Consultation response no. 18 – Marion Oswald, University of Winchester.

[33] We discussed fears relating to monetary penalties above in ch 3 at paras 3.30 to 3.50.

[34] Consultation response no. 76 – Northumbria University.

[35] For example, consultation meeting no. 24 – seminar at Northumbria University Information Law Centre; consultation meeting no. 18 – Leicestershire County Council.

[36] The Department of Health published The Information Governance Review: To Share or Not to Share (Caldicott 2) in March 2013. Dame Caldicott chaired that review panel and subsequently accepted the Secretary of State's invitation to chair The Independent Information Governance Oversight Panel.

[37] Consultation response no. 65 – Independent Information Governance Oversight Panel.

personal responsibility for unauthorised disclosure as promoting a level of anxiety which hampers the use of flexible powers. Reference was made to criminal liability, professional discipline, other sanctions, and the impact on an individual's employment, including dismissal, delayed professional advancement, damage to professional reputation and even unfair treatment and harassment by colleagues.

7.36 We found evidence in the public sector of an over-cautious culture of adopting the safer option. The Office for National Statistics told us of problems it had experienced on a number of occasions because of narrow or overly cautious interpretations of the law, technological issues, or simply a poor understanding of the benefits to be gained from data sharing. This was particularly true when the Office had tried to obtain information from public bodies set up by statute, such as Her Majesty's Revenue and Customs, though the Office for National Statistics had also observed a shift from a culture of trust to a risk adverse culture in relation to data sharing in Ministerial Departments.[38]

7.37 We have found confusion and consultees reported a lack of authoritative guidance for public bodies. The seminars organised by DAC Beachcroft also called for more clarity in relation to the powers to impose sanctions for inappropriate sharing, which would be assisted by publishing the Information Commissioner's decisions on individual complaints.[39] The Beachcroft seminars recommended that staff making decisions should be protected from action against them personally where their employing organisation had endorsed a decision to share, suggesting also that we should consider the benefits of a "good faith" defence in relation to criminal sanctions, where a decision in good faith had followed a consideration of the relevant legal concepts and principles.[40]

Fear of enforcement

7.38 As discussed in Chapter 3, the fear of enforcement action, often misplaced, is a barrier to sharing information effectively and appropriately.[41]

RESOURCES

Economic implications of sharing

7.39 Problems also relate to the cost and resource implications of sharing. Any genuine and effective attempt to improve data sharing cannot afford to ignore the administrative and economic burden of data sharing. Any reform of data sharing law must be conscious of this aspect of the problem.

7.40 Sue Richardson referred to the resources required to amend or edit data records and datasets to facilitate lawful sharing, especially as the data held by many public bodies were of poor quality. Public bodies did not invest enough in ensuring data quality and accuracy, creating a reluctance to share because bodies cannot trust the quality of data they then receive. The cost of sharing data securely is also a barrier, particularly for the numerous small third sector

[38] Consultation response no. 55 – Office for National Statistics.

[39] Consultation response no. 49 – DAC Beachcroft Solicitors seminar.

[40] Good faith defences already exist in a large proportion of wrongful disclosure offences.

[41] Paras 3.30 to 3.50 above.

organisations delivering services under contract to public bodies. The cost of employing someone with knowledge and skills of the law and other information governance aspects as well as knowledge of the ICT needed are part of the problem. The other part is the actual cost of providing secure networks and encryption. [42]

7.41 The Association of Independent Healthcare Organisations pointed to an example given by the Private Healthcare Information Network, which wanted to link data on hospital episodes from private acute hospitals to any National Health Service hospitals episodes in order to identify re-admissions within a specified timeframe. This was only possible with an application under section 251 of the NHS Act 2006,[43] which delayed the project extensively due to the number of challenges experienced in getting the application approved. The upshot was a decision to ask all patients for specific consent to the linkage being carried out without further applications under section 251 being required.[44]

7.42 Birmingham City Council described the edited electoral roll as an example of information produced for the purposes of publication, where the costs may outweigh the benefits.

> The local authority is seeing an increased demand for various types of organisation as well as individuals seeking to use the electoral register for a variety of purposes. This is an interesting example of the costs of creating an accurate database for the purposes of data sharing, which the local authority perceive as outweighing any public benefit …The Council's view is that the costs of creating and updating an edited register, in terms of not just the resourcing, but also the potential discouragement to potential electors, outweigh the benefits, both in terms of the income, and the benefits to the electorate, and would rather the obligation to create and maintain the public register, and make it available for commercial exploitation, was abolished

The costs of data sharing

7.43 There are limited resources available for data sharing, a scarcity of legal resources and a lack of skills and training.

7.44 London Fire Brigade found turning the Information Commissioner's Office guidance into actual data sharing agreements unnecessarily onerous. They told us that there is no agreed template for a data sharing agreement and when templates are used they are amended to reflect local legal and information governance advice. There is a wide variation in the standard of quality and different levels of "red tape" in such documents, which run to tens of pages. London Fire Brigade thought that these documents could be reduced in length and made public, perceiving a clear need to review the way in which data sharing agreements have been implemented and improvements made. They also found transfer from one data controller to another data controller unnecessarily

[42] Consultation response no. 41 – Sue Richardson, University of Bradford.

[43] Section 251 creates a statutory mechanism by which the duty of confidence may be disapplied.

[44] Consultation meeting no. 22 – Sally Taber, Independent Healthcare Advisory Services.

onerous.[45]

7.45 The London Borough of Camden saw limited resources and capacity as a potential barrier to data sharing, with limited time to think or learn about data sharing. Councils are continuously required to "do more with less" and restructure to meet tightened budgets. However, this slows the process down.[46]

7.46 Transport for London explained that it was simply unable to resource the processing of all public body requests to share data. In the financial year 2012, the Surface Transport Enforcement and On-Street Operations Department received over 8,000 requests for data under section 29 of the Data Protection Act 1998.[47]

7.47 The Office of the Senior Traffic Commissioner told us that a data sharing agreement between the Driver and Vehicle Standards Agency, which is a Department for Transport enforcement agency, and the Traffic Commissioners had taken more than two years to draft, redraft, amend and agree. The resources for the task were non-existent. Temporary measures had to be put in place to enable data to be exchanged lawfully in the interim. The Office expects to arrange another five agreements in the next year with the Department of the Environment for Northern Ireland, Transport for London, the highways agency, the Association of Chief Police Officers (possibly requiring further agreements for each police force), and the Bus Service Operators Grant Section of the Department for Transport. This work is additional to an existing heavy work load and the small team lacks the skills and resources to take on the work alone. This means there is a reliance on the goodwill of staff within Department for Transport and Driver and Vehicle Standards Agency to assist. All support staff, traffic commissioners and deputies will have to achieve refresher training on data protection and data handling. The requirement to have multiple data sharing agreements does not easily aid or support these objectives.[48]

Further reductions in public spending

7.48 Consultees considered that cost would become a greater problem as a consequence of further reductions in public spending. For example, Shropshire Fire and Rescue Service saw resources as a particular issue in an austerity climate, possibly resulting in requests for information being considered low priority or declined without full consideration of their importance. Humberside Fire and Rescue Service responded that although a lack of resources usually hinders rather than prevents sharing, by causing delay, it could be a larger problem in the future with further reductions in public sector resources.[49] Betsi Cadwaladr University Local Health Board responded that the continuing reduction in public sector meant that improving systems, equipment and resources to manage

[45] Consultation response no. 37 – London Borough of Camden.

[46] Consultation response no. 36 – London Fire Brigade.

[47] Consultation response no. 61 – Transport for London.

[48] Consultation response no. 23 – Senior Traffic Commissioner. Examples of powers to charge fees and related economic issues are discussed in ch 9 in relation to the Department for Work and Pensions at para 9.37 and following.

[49] Consultation response no. 20 – Humberside Fire and Rescue Service.

processes was a constant battle.[50]

Data sharing as a low priority

7.49 Data sharing is often a low priority, as it is seen as a peripheral rather than core activity. Data sharing does not tend to be integrated into project design and planning, so that data sharing issues are raised at the end of the process, when insufficient time and resources are available to resolve possibly complex data sharing issues. The Social Landlords Crime and Nuisance Group explained that reduced resources have made data sharing a lower priority for the police. Similarly, landlords rely on housing benefit data to inform their income management whilst at the same time housing benefit departments are stretched trying to implement the changes, with data sharing relegated down the order of priorities.[51]

7.50 Data sharing must be balanced against other priorities. The Land Registry, Nottingham Office, explained that the Land Registry is a founder member of the Public Data Group, alongside Ordnance Survey, Companies House and the Meteorological Office who together play a valuable role in providing public information and improving access to data to support economic growth. However, the Land Registry had to balance this commitment with ensuring that its delivery of statutory services is not allowed to suffer as a result of voluntary data sharing activities. It therefore endeavours to balance the amount of time and resource (both human and mechanical) spent on sharing data with the primary purpose of its statutory services.[52]

7.51 A number of fire and rescue services identified lack of resources as a potential barrier for some organisations because they focus their resources on core business whereas data sharing is perceived to be peripheral. Resourcing may also create perverse incentives not to share, for example where the organisation's funding is threatened by sharing data.

7.52 Sue Richardson of Bradford University regarded the main areas affected by resources as training and data quality, which seem to her to be de-prioritised because they are not sufficiently well specified in the standards that public bodies are moving towards.[53]

7.53 The Association of Chief Police Officers found it not uncommon for the demand for data to outstrip the capacity to deliver data, with the result that some organisations have, in the past, filtered requests for data. Reduced resources are likely to lead to a reduction in sharing as organisations concentrate their resources in 'core' areas of activity.[54]

[50] Consultation response no. 13 – Betsi Cadwaldr University Local Health Board.

[51] Consultation response no. 29 – Social Landlords Crime and Nuisance Group.

[52] Consultation response no. 31 – HM Land Registry.

[53] Consultation response no. 41 – Sue Richardson, University of Bradford.

[54] Consultation response no. 45 – Association of Chief Police Officers.

INCOMPATIBILITY OF COMPUTER SYSTEMS

7.54 Adhering to traditional practices, using disparate and incompatible data and IT systems, and cultural resistance or failure to prioritise sharing all seem to create inappropriate obstacles.

7.55 One consultee explained that some inappropriate barriers to information sharing are technical. For example, the requirements and controls of the public service network local authority email system restrict the ability of local authorities to share with the private, charitable and voluntary sectors, which do not or cannot meet those standards.[55] Another responded that differing security regulations prevented access to other systems. For example, there is compliance with an Information Governance Toolkit for health services in England but not Wales; strict regulations for NHS Networks but less regulation for local government networks; and a level of encryption in England which has not been purchased in Wales.

7.56 We heard that access to IT systems can create inappropriate obstacles, for example, where information is held in many different systems and databases, which create challenges when bodies seek to identify and share information across those systems and databases. We were given an example where, within a single hospital, different medical and surgical departments had their own databases of patient information, so that a doctor in the obstetrics department could not have access to the database containing information about a patient's HIV status.

7.57 The Information and Records Management Society complained that the lack of data management practice in many public bodies, the many unstructured data types, including email, documents and spread sheets, used by public bodies and the use of incompatible systems can be barriers to sharing.[56] One consultee responded that barriers were created by bodies not having good practical arrangements in place for processing personal data. Good practice can avoid such obstacles.

7.58 Nottinghamshire and Nottinghamshire Local Resilience Forum and others reported that incompatible technology and barriers created by different information technology systems prevented sharing. There could be a reluctance to address technology problems due to a lack of expertise. A combination of information technology and data sharing policies make the task difficult. The practical difficulties of providing data in an appropriate format are not insignificant and electronic exchange is difficult without proper IT support.[57]

7.59 Incompatible data systems, combined with a lack of national data sharing standards, policies and agreements or central policy, cause inappropriate obstacles.

7.60 Examples of good practice were also identified. The Humber Data Observatory was given as one example of overcoming some of the obstacles. It is a website,

[55] Consultation response no. 1 – Somerset County Council.

[56] Consultation response no. 30 – Information Records and Management Society.

[57] Consultation response no. 9 – Nottingham and Nottinghamshire Local Resilience Forum.

hosted by the local authority, which provides open access to information and statistics about the region.[58]

A RELUCTANCE TO USE IMPLIED OR ANCILLARY POWERS

7.61 As discussed in Chapter 3, there is sometimes reluctance on the part of public bodies to rely on their implied or ancillary powers, which created an unnecessary obstacle to lawful sharing. The Office for National Statistics found those holding data sought by the Office to be over-reliant on express legislation and not to make sufficient use of implied and common-law powers derived from other sources of law. This was particularly true when the Office had tried to obtain information from public bodies that have been set up by statute, such as Her Majesty's Revenue and Customs. The Office also pointed to the reduced use of common law powers by Government departments.[59]

DATA SECURITY

7.62 Consultees described security standards as generally high, although there have been notable data losses widely reported in the media.

Over-caution and ownership

7.63 A number of consultees expressed the view that security concerns promote caution and risk aversion. For example, Fire and Rescue Services responded that concern about security breaches, especially in light of high profile losses, meant that public bodies exhibit caution when sharing data. A group of academic researchers saw security concerns as feeding into a sense of ownership and detected a need to recognise those concerns.[60] David Stone, Kaleidoscope Consultants, found the response to security concerns often disproportionate to the real risks, for example observing an unhelpful focus on technical security, such as email which has a miniscule risk of interception in transit, as opposed to focussing on the risk presented by human error, for example, the possibility of inaccurate email addressing resulting in a data breach.[61]

The burden of security arrangements

7.64 A number of consultees pointed to the significant burden of putting appropriate security arrangements in place.

7.65 For example, Somerset County Council described security as a significant barrier to local authority data sharing. The administrative burden and expense of complying with the controls imposed by the local authority Public Service Network (PSN) email system could exclude local authorities from accessing networks with

[58] Consultation response no. 20 – Humberside Fire and Rescue Service. The Humber Data Observatory website may be found at: http://www.humberdataobservatory.org.uk (last visited 1 July 2014).

[59] Consultation response no. 55 – Office for National Statistics.

[60] Consultation response no. 35 – Dr Ashley Savage, Dr Richard Hyde, Mr Jamie Grace and Ms Bansi Desai.

[61] Consultation response no. 70 – Kaleidoscope Consultants, David Stone.

other partners.[62]

7.66 London Fire Brigade regarded secure systems as appropriate but they could make it difficult to transfer personal data securely from one organisation to another as the IT infrastructures of public authorities are different with no common standard. The Public Services Network could alleviate these problems but with significant costs.[63]

7.67 The Insolvency Service Intelligence Team responded that in relation to security a "form over substance" attitude can hinder sharing. Organisations that adhere to the National Intelligence Model (NIM) security requirements view security in an overly narrow way. Insolvency Service security requirements do not differ greatly from NIM security measures but organisations refuse to share because they cannot say they are NIM compliant. NIM compliance has in effect become a requirement for certain organisations before they will share certain types of data.[64]

7.68 The Social Landlords Crime and Nuisance Group noted that many landlords were outside the secure government email system, which could cause public bodies concern about the security of emails. An increasing number now have access to Criminal Justice Secure (CJS) email accounts, approved for use by a limited number of agencies, including the police and probation services. The Group saw evidence that addressing concerns over security had little positive impact on speed and efficiency.[65]

7.69 The Office for National Statistics added that security, although necessary, imposed an extra layer of cost upon data sharing. Data sharing becomes more difficult to negotiate and anonymisation can hamper or damages the reusability of the data. The Office for National Statistics found inconsistency across Government departments on how data are classified and the level of protection required on certain data, which needed to be harmonised across all departments to ensure consistency.[66]

7.70 The Association of Independent Healthcare Organisations responded with a useful case study illustrating the administrative burden of accessing data. Any non-NHS organisation that requires Smart Cards for access to certain systems must have them issued through an appropriate NHS organisation. A pilot project is planned to allow a range of non-NHS organisations to test and finalise an application process to allow non-NHS organisations to have their own Registration Authority, if strict criteria are met.[67]

7.71 The Association provided us with proposed criteria in the form of several pages of tables, illustrating a high level of complexity and administrative burden.

[62] Consultation response no. 1 – Somerset County Council.

[63] Consultation response no. 36 – London Fire Brigade.

[64] Consultation response no. 19 – The Insolvency Service.

[65] Consultation response no. 29 – Social Landlords Crime and Nuisance Group.

[66] Consultation response no. 55 – Office for National Statistics.

[67] Consultation meeting no. 22 – Sally Taber, Independent Healthcare Advisory Services.

Trust between public bodies

7.72 A lack of trust between partner organisations can also present a barrier to effective data sharing.

7.73 For example, Leeds City Council detected distrust between different organisations about how they handle and store third party data, telling us that, if data processing arrangements were more consistently used and effective auditing carried out, confidence would grow about how organisations treat third party data. A lack of this knowledge had led to a risk averse attitude to sharing data.[68]

7.74 Shropshire Fire and Rescue Service also saw security as an important issue, capable of acting as a barrier as public bodies were usually unaware of the security arrangements of other organisations and public bodies and therefore feared data security breaches. They saw some organisations as more concerned about the legal requirements and any sanctions than the security of their systems.[69]

7.75 Welwyn Hatfield Borough Council noted, however, a contrary tendency to assume that the requesting body has measures in place to hold information securely.[70]

Security not a priority

7.76 Some consultees noted that improvements in security meant that security was no longer the dominant factor it used to be.

7.77 Cheshire West and Chester Council said that security played a minor role. Most public bodies now have the appropriate technical methods in place to transfer information securely.[71]

DATA QUALITY

7.78 Consultees explained that although the quality of data does not usually influence whether data are disclosed, it does have an impact on the usefulness of sharing, which can contribute to reluctance to support sharing. Data quality is generally quite poor and there are significant resource implications for maintaining the quality of datasets. Some consultees noted that poor data quality increased the pressure to use identifiable data for research purposes to improve the quality.

7.79 Sue Richardson of Bradford University maintained that quality was the real issue. The quality of data is generally quite poor and the knowledge that this is the case undermines the confidence needed to share safely. It can also lead to organisations not wanting to accept data offered.[72]

[68] Consultation response no. 17 – Leeds City Council.

[69] Consultation response no. 6 – Shropshire Fire and Rescue Service.

[70] Consultation response no. 2 – Welwyn Hatfield Borough Council.

[71] Consultation response no. 63 – Cheshire West, Cheshire Council and West Cheshire Clinical Commissioning Group (Joint Response).

[72] Consultation response no. 41 – Sue Richardson, University of Bradford.

7.80 The Association of Chief Police Officers saw data quality as a significant though largely unrecognised factor, observing a lack of focus on data quality across public bodies, with some exceptions. The Association noted that while specialist staff historically entered data entry, now it was done by staff who do not have the same level of dedication. Poor quality data led to an inability to access all relevant information that could be considered for sharing.[73]

7.81 On the other hand, Birmingham City Council did not consider that quality played a part in public bodies' ability to share data. Acknowledging that there is always a risk that some information will either be out of date or be subject to errors, they saw this as a risk affecting all data controllers. They told us that their practice was that "when sharing data, we require that where individuals advise the partner organisation that information is incorrect, they let us know so we can investigate, and where appropriate, correct the error".[74]

7.82 Delegates of the Society for Computers and Law's Privacy Data Protection Group saw the potential inaccuracy of data as a huge concern where a public body collected the data in one context and another public body with whom the information has been shared sought to use it in a different context, regarding it as essential to question the context from which the data comes.[75]

7.83 A number of consultees observed that poor data quality could have adverse effects on appropriate and desirable data sharing.

7.84 For example, Leeds City Council responded that although organisations should be looking to provide reliable, trustworthy and authentic information, data quality was not thought about over and above security and personal data issues.[76]

7.85 The Social Landlords Crime and Nuisance Group also responded that if poor data are captured then poor data are shared, which can have direct implications on how the data are then used. The Group believed that more thought needed to be given to why the data were being collected and who might need access. They said "we believe there is a significant issue around data competence and whether the skill sets within public bodies set up to cope with and analyse ever evolving and more complex data sets are suitably developed and resourced".[77]

7.86 The Information and Records Management Society said that "if you do not trust your own data which have been accumulated over many years by various groups you are unlikely to want to share it with others".[78] Nottinghamshire and Nottinghamshire Local Resilience Forum gave quality concerns as a significant barrier to sharing, saying that "many bodies argue that it is pointless to share data because it will be out of date as soon as it is shared".[79]

[73] Consultation response no. 45 – Association of Chief Police Officers.

[74] Consultation response no. 69 – Birmingham City Council.

[75] Consultation response no. 73 – Society for Computers and Law.

[76] Consultation response no. 17 – Leeds City Council.

[77] Consultation response no. 29 – Social Landlords Crime and Nuisance Group.

[78] Consultation response no. 30 – Information Records and Management Society.

[79] Consultation response no. 9 – Nottingham and Nottinghamshire Local Resilience Forum.

7.87 We received other evidence that poor quality of data can have a significant impact on data sharing. A group of academic researchers saw complete information as vitally important for regulators and enforcement bodies.[80] Shropshire Fire and Rescue Service feared that data quality could be overlooked, echoing the view that quality concerns, such as over data considered unreliable or unverified, might result in a reluctance to share.[81]

7.88 West Midlands Fire and Rescue, however, regarded poor quality data as a better indicator of vulnerability or deprivation than no data at all.[82] Similarly, Humberside Fire and Rescue Service took the view that poor quality did not necessarily prevent sharing but rather reduced the reliability and usefulness of the data shared.[83] Some missing data on individuals' lifestyles would greatly enhance the intelligence held by the fire service on individual risk profiles, such as hoarding behaviours which present an increased fire risk.

7.89 The Public and Commercial Services Union Land Registry Group responded that the Land Registry had good quality data but incomplete registration meant that the data could not be used as widely as possible.[84]

7.90 The Insolvency Service Intelligence Team responded that perfect record keeping was unlikely to be achieved in practice by any organisation. Although it was difficult to provide specific examples or quantify the degree of concern it raised, it was certainly an issue that influenced decisions to share data.[85]

CONCLUSIONS

7.91 The issues outlined above are not strictly problems with the law, but they are matters which need to be borne in mind in carrying out a review of the legal framework for data sharing. Ever since public bodies started holding data and communicating electronically, attempts have been made to improve data sharing between them, but without overarching success. Any law reform project must recognise and evaluate the incentives and disincentives discussed in this chapter and develop a framework which, so far as possible, addresses the disincentives and which works with, rather than against, the organisational cultures.

[80] Consultation response no. 35 – Dr Ashley Savage, Dr Richard Hyde, Mr Jamie Grace and Ms Bansi Desai.

[81] Consultation response no. 6 – Shropshire Fire and Rescue.

[82] Consultation response no. 10 – West Midlands Fire and Rescue Service.

[83] Consultation response no. 20 – Humberside Fire and Rescue Service.

[84] Consultation response no. 8 – Public and Commercial Services Union Land Registry Group.

[85] Consultation response no. 19 – The Insolvency Service.

PART 3
DATA SHARING IN PRACTICE

INTRODUCTION

In this and the next two Chapters, the statutory and common law powers of two government departments are examined in order to illustrate data sharing issues for government departments. In addition, a brief description is provided of a cross-government project, requiring extensive data sharing: the Troubled Families Programme.

CHAPTER 8
HER MAJESTY'S REVENUE AND CUSTOMS

INTRODUCTION

8.1 The first case study is of Her Majesty's Revenue and Customs (HMRC), which has been selected for a number of reasons. First, many consultees expressed concern about legal difficulties in obtaining information held by HMRC. Secondly, HMRC is a statutory department and therefore does not have the benefit of relying on the common law powers of Crown Departments or the Ram Doctrine. It is therefore illustrative of some of the problems encountered by such bodies. Thirdly, HMRC holds an enormous amount of sensitive data about individuals and has a long history of protecting taxpayer confidentiality. The statutory framework therefore illustrates very well some of the tensions and difficulties around confidentiality, wrongful disclosure and controls on onward disclosure. Finally, it provides a valuable example of a complex statutory scheme.

HER MAJESTY'S REVENUE AND CUSTOMS

Commissioners for Revenue and Customs Act 2005

8.2 HMRC is a statutory department created by the Commissioners for Revenue and Customs Act 2005 through the merger of Her Majesty's Commissioners of Customs and Excise and Inland Revenue. HMRC has extensive statutory powers. A large and complex body of statute applies to HMRC and controls the disclosure of information both internally and externally.[1]

The importance of taxpayer confidentiality

8.3 The importance of taxpayer confidentiality was emphasised repeatedly in debates during the passage of the 2005 Act. It remains an important part of HMRC's institutional culture and practices.

8.4 During the passage of the Commissioners for Revenue and Customs Bill, a debate developed over the method by which officers of HMRC would be required to recognise their statutory duty of confidentiality. The Government proposed that a declaration be made by an official. Opposition parties argued strongly for the

[1] We are particularly grateful to HMRC for providing us with information about HMRC's legal gateways.

retention of an oath. Although it might be thought that little turns on the distinction between a solemn declaration and an oath, the debate demonstrates the strength of feeling in Parliament at the time over the importance of maintaining taxpayer confidentiality.

8.5 Taxpayer confidentiality was then and is now considered to be a fundamental operating principle in HMRC. It is understood to be very important to maintaining the tax base and to efforts to close the tax gap: the gap between tax received and the sum HMRC believes is payable nationally.[2] The strong emphasis on taxpayer confidentiality was also seen as an important principle respected in the United Kingdom to a greater extent than in other European systems, making comparisons with other jurisdictions inapt,[3] although all tax authorities do recognise "a basic right to confidentiality and secrecy".[4] The topic was also politically sensitive at the time of the passage of the 2005 Act because there was perceived to be a need to ensure that Treasury officials, Ministers or special advisers could not seek to see individual tax records for political reasons.[5]

8.6 There was strong cross-party recognition of the importance of taxpayer confidentiality in the House of Commons. On 26 January 2005, the Paymaster General, Dawn Primarolo MP, said

> On Second Reading and in Committee, I made it clear that the new department, Her Majesty's Revenue and Customs, would take taxpayer confidentiality every bit as seriously as its predecessors. The new clauses underline our commitment to taxpayer confidentiality, and I hope that as such they will be uncontroversial.
>
> Let me remind Members briefly of our high standards of confidentiality. The issue is taken seriously by everyone: staff, Members in all parts of the House and, indeed, taxpayers. The Bill contains provisions for safeguarding taxpayer confidentiality that strengthen those previously available. That includes, in clause 17,[6] a civil sanction for unauthorised disclosure of any information held by Her Majesty's Revenue and Customs which is binding on appointment, and in clause 18,[7] in relation to customer confidential information, the additional safeguard of a criminal sanction. That too applies to all functions of Her Majesty's Revenue and Customs.[8]

8.7 She also emphasised that "taxpayer confidentiality remains of paramount

[2] See for example, The *O'Donnell Review of Revenue Departments* (2004). The Review was a major review of the organisations responsible for tax policy and administration which proposed the merger of Inland Revenue and Customs and Excise. See also *Hansard* (HC), 11 January 2005, cols 57 to 58, Standing Committee E, 2nd Sitting.

[3] *Hansard* (HC), 11 January 2005, cols 60 to 61, Standing Committee E, 2nd Sitting

[4] OECD Practice Note GAO002: *Taxpayers' Rights and Obligations*.

[5] Hansard (HC), 11 January 2005, cols 56 to 57, Standing Committee E, 2nd Sitting

[6] This provision became s 18 of the 2005 Act.

[7] This provision became s 19 of the 2005 Act.

[8] *Hansard* (HC), 26 January 2005, vol 430, col 394.

importance in the new department".[9]

8.8 Andrew Tyrie MP (Conservative) agreed that:

> The Paymaster General is right to say that there should be all-party support for the retention of confidentiality. I back her in that, as it is at the heart of safeguarding the Revenue and crucial to safeguarding people's right to privacy and, therefore, to their trust in the Revenue service.[10]

8.9 John Burnett MP (Liberal Democrat) added that confidentiality was

> important because the successful collection of tax depends on many factors, not least the perception of fairness and confidence by the public that their affairs will be kept confidential. It is vital that taxpayers are assured of the Inland Revenue's ability to keep their affairs secret, which is the principal way in which the tax base is preserved.[11]

8.10 HMRC takes its duty of taxpayer confidentiality very seriously.[12] Some consultees perceived that this has made HMRC reluctant to exercise its powers to disclose information where it is within its power to do so and would bring about a public benefit. The remainder of this Chapter examines the legal position of HMRC in the light of these tensions.

8.11 The perception that HMRC is reluctant to disclose should be contrasted with the large amount of data that the department can and does share legally through existing legal gateways. HMRC does in fact share a large amount of information within the existing statutory framework. There are wide statutory gateways between HMRC and the Department for Work and Pensions, Border Force, UK Immigration Enforcement, and the National Crime Agency. HMRC shares data with other law enforcement bodies where it supports HMRC's functions. The introduction to HMRC's data sharing consultation response document sets out HMRC's current position on data sharing:

> Her Majesty's Revenue and Customs' (HMRC) relationship with businesses and individuals is unique. This is reflected in the scope and depth of the information HMRC collects, creates and protects on behalf of taxpayers in carrying out its departmental functions. HMRC recognises that it is important for the department to play a full part in the Government's Open Data agenda, using its information to

[9] *Hansard* (HC), 26 January 2005, vol 430, col 395.

[10] *Hansard* (HC), 26 January 2005, vol 430, col 396.

[11] *Hansard* (HC), 26 January 2005, vol 430, col 396 to 397.

[12] Anthony Inglese, General Counsel at HMRC, was involved in a controversial exchange before the Public Accounts Committee on 7 November 2011 regarding the effect of his statutory duty of confidentiality on his ability to answer questions put by the Committee. This view was also expressed by many consultees during the Law Commission scoping consultation. Officials at HMRC noted that it was protective of taxpayer information for good reason and added that the position had improved since 2005, with HMRC pursuing a number of projects to improve its practice and there being a greater willingness to disclose information where appropriate and lawful to do so.

> improve transparency and promote economic growth. It also wishes to improve data sharing with other public sector bodies to deliver better services across the public sector.
>
> HMRC was created by the Commissioners for Revenue and Customs Act 2005 (CRCA). This legislation provides strong protection for the information that HMRC holds. HMRC officials are prohibited from sharing information except in the limited circumstances set out in the CRCA. This legislation enshrines the core principle of what is often described as 'taxpayer confidentiality'**.** HMRC is committed to maintaining this important principle, which is essential to the effective operation of the tax system because it supports compliance and willing cooperation. It is therefore paramount that any data release has appropriate safeguards.[13]

8.12 In some respects HMRC is relatively open in sharing taxpayer identifying information. The Permanent Secretary for Tax disclosed information in relation to HMRC's work on tax avoidance schemes in "off the record" background briefings to journalists, including identifying data about firms and individuals who were promoters of film investment schemes. Such briefings were intended to inform journalists to avoid inaccuracy on the understanding that nothing said would be published. This understanding was breached by the journalists who published comments from the meeting. In proceedings brought by one of the subjects of the information, the court held that there was a "rational connection between the function of HMRC to collect tax in an efficient and cost-effective way and the disclosures made by [the Permanent Secretary for Tax] in the course of the briefing".[14] Such a judgement fell within the lawful parameters of section 18(2)(b) of the Commissioners for Revenue and Customs Act 2005, as the disclosures were intended to maintain good relations with the press, to encourage journalists to share information with HMRC and to encourage journalists to convey HMRC's negative attitude towards film investment schemes, promoting public awareness.[15] The court also rejected arguments that the disclosures were a breach of article 8 or article 1 of Protocol No. 1 of the European Convention on Human Rights, a breach of legitimate expectation or an abuse of power. The disclosure was held to be lawful and proportionate. The case is a good example of how wide HMRC's existing power to share for the purpose of its functions already is.

[13] *Sharing and Publishing Data for Public Benefit: Summary of Responses and Outcomes* (10 December 2013) paras 1.3 to 1.4, https://www.gov.uk/government/consultations/sharing-and-publishing-data-for-public-benefit (last visited 1 July 2014).

[14] *McKenna v HMRC* [2013] EWHC 3258 (Admin), [2014] STC 673, para 39. This case is pending appeal in the Court of Appeal.

[15] See para 8.25 below.

LEGAL POWERS OF HMRC

Declaration of confidentiality

8.13 All Revenue and Customs Commissioners and officers appointed under the 2005 Act make a declaration acknowledging their duty of confidentiality under section 18 of the Act, as soon as is reasonably practicable following their appointment.[16]

Broad ancillary powers

8.14 Section 9(1) of the 2005 Act provides

> (1) The Commissioners may do anything which they think—
>
> (a) necessary or expedient in connection with the exercise of their functions, or
>
> (b) incidental or conducive to the exercise of their functions.[17]

8.15 HMRC is responsible for a large number of functions:

(1) the collection and management of revenue for which the Commissioners of Inland Revenue were responsible before the commencement of the 2005 Act;

(2) the collection and management of revenue for which the Commissioners of Customs and Excise were responsible before the commencement of the 2005 Act; and

(3) the payment of tax credits for which the Commissioners of Inland Revenue were responsible before the commencement of the 2005 Act.[18]

8.16 The Commissioners are also responsible for all the other functions which vested in the Commissioners of Inland Revenue or the Commissioners of Customs and Excise before the commencement of the 2005 Act.[19]

8.17 HMRC has broad and extensive ancillary power to share data where this is necessary or expedient in connection with, or incidental or conductive to, the exercise of a function. This means that potentially a great deal of sharing is possible under section 9.

8.18 This is especially so if one accepts the suggestion we heard from some legal practitioners in this field that implied powers can be the legal basis for mutually beneficial exchanges of information between public bodies. If a transfer of some of A's information is made in order to obtain B's information for the purpose of A's function, then that exchange might be seen as incidental or consequential to the carrying out of A's function itself.[20] This could include information exchanges,

[16] Commissioners for Revenue and Customs Act 2005, s 3.

[17] Commissioners for Revenue and Customs Act 2005, s 9.

[18] Commissioners for Revenue and Customs Act 2005, s 5(1).

[19] Commissioners for Revenue and Customs Act 2005, s 5(2).

[20] *AG v Great Eastern Railway* (1880) 5 App Cas 473.

where one disclosure in the overall exchange is wholly for another body's statutory function, although such exchanges would still be subject to the control of the Data Protection Act 1998 and Human Rights Act 1998. There is considerable uncertainty over whether such an approach is proper or would be effective in a particular case, which may go some way towards explaining the proliferation of powers permitting disclosure to assist another body in the exercise of statutory functions. Even where a more restrictive approach is taken by the courts, an implied power will exist where the action is necessary in order to make the statutory power effective to achieve its purpose.[21]

8.19 HMRC's powers to share data were the subject of advice from the First Treasury Counsel to HMRC, which was revealed by the Public Accounts Committee in November 2011 during a controversial argument over the evidence of Anthony Inglese, General Counsel of HMRC, to the Committee. The Chair of the Public Accounts Committee quoted advice from the First Treasury Counsel to HMRC in 2009 that stated "as [the Public Accounts Committee] are a parliamentary body with an oversight role over HMRC it follows that HMRC's functions would extend to assist the Public Accounts Committee (PAC) with that oversight role. So there is no absolute bar on disclosure".[22] Anthony Inglese observed that there was more recent advice in 2011 which stated that HMRC could not provide taxpayer identifiable data to Parliament, but refused to be drawn on whether First Treasury Counsel's advice was correct. Although it is not clear from this admittedly limited quotation, which could have been taken out of context, it does appear to suggest lines of argument that HMRC functions include assisting other bodies and it may therefore disclose information for such purposes. The effect of this would be to make the ancillary power very broad indeed and render many other explicit powers less obviously necessary. We do not comment on the correctness of the conclusion quoted in 2011, especially without benefit of seeing the advice in full, but merely note the existence of such arguments, which were made in high profile circumstances.

8.20 We note that HMRC's recent written evidence to PAC, Forty-First Report Gift Aid and other tax reliefs on charitable donations,[23] states:

> HMRC discloses non-identifying information to PAC on the basis that it supports the Department's function of being held to account by PAC. This includes information about its administration of the tax system which PAC needs to assure itself that HMRC is applying resources and processes appropriately. HMRC does not disclose details of the settlement of tax liabilities with specific taxpayers as it judges that disclosing such information would be detrimental to its function of collecting tax."

8.21 Many consultees felt that HMRC is often reluctant to use its ancillary power to disclose information where it is not accompanied by the controls on further or onward disclosure found in many other statutory gateways, including the benefit

[21] *Ward v Metropolitan Police Commissioner* [2005] UKHL 32, [2006] 1 AC 23, para 24.

[22] Transcript of Oral Evidence to the Public Accounts Committee, 7 November 2011, HC 1531-II, question 253.

[23] (2014) HC 835.

of criminal sanctions for onward disclosure without the permission of the Commissioners. Part of the proliferation of statutory gateways reflects HMRC's unwillingness to share without additional control over the future uses of the information. Paradoxically, therefore, the greater restrictive controls in other gateways, sometimes including wrongful onward disclosure provisions, can act to facilitate more sharing than would be the case under broad and generous ancillary powers, because the permissive nature of the ancillary power means that HMRC will not in fact use it as extensively as it could. HMRC does not consider that its power to disclose information for its functions is as broad and generous as we have set out.

Internal use of information

8.22 HMRC has extensive power to use information internally. Information acquired by HMRC in connection with one of its functions may be used in connection with any other function, subject to any provisions restricting or prohibiting the use of information contained in the Act, any other enactment or an international or other agreement to which the United Kingdom or Her Majesty's Government is a party.[24] HMRC is therefore bound by the Data Protection Act 1998 and the Human Rights Act 1998, for example, and the priority between these provisions is clear. The 2005 Act makes clear that nothing in sections 17 to 21, on use and disclosure of information, authorises the making of a disclosure which either contravenes the Data Protection Act 1998 or is prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000.[25]

Strict confidentiality protections

8.23 The Commissioners for Revenue and Customs Act 2005 contains a strict confidentiality provision in relation to external sharing of HMRC data.[26] Section 18(1) provides that officials may not disclose information which is held by the Revenue and Customs in connection with a function of the Revenue and Customs, unless one of a number of exceptions in section 18(2) apply.

8.24 Section 18(2) provides that subsection (1) does not apply to a disclosure:

> (a) which—
>
> (i) is made for the purposes of a function of the Revenue and Customs, and
>
> (ii) does not contravene any restriction imposed by the Commissioners,
>
> (b) which is made in accordance with section 20 or 21,
>
> (c) which is made for the purposes of civil proceedings (whether or not within the United Kingdom) relating to a matter in respect of which the Revenue and Customs have functions,

[24] Commissioners for Revenue and Customs Act 2005, s 17.

[25] Commissioners for Revenue and Customs Act 2005, s 22.

[26] Sometimes it is referred to as a secrecy provision and is compared to provisions in legislation concerning official secrets.

(d) which is made for the purposes of a criminal investigation or criminal proceedings (whether or not within the United Kingdom) relating to a matter in respect of which the Revenue and Customs have functions,

(e) which is made in pursuance of an order of a court,

(f) which is made to Her Majesty's Inspectors of Constabulary, the Scottish inspectors or the Northern Ireland inspectors for the purpose of an inspection by virtue of section 27,

(g) which is made to the Independent Police Complaints Commission, or a person acting on its behalf, for the purpose of the exercise of a function by virtue of section 28,

(h) which is made with the consent of each person to whom the information relates, or

(i) which is made to the Scottish Ministers in connection with the collection and management of a devolved tax within the meaning of the Scotland Act 1998.

8.25 In relation to section 18(2)(a)(i), section 51 of the 2005 Act defines a "function" as "any power or duty (including a power or duty that is ancillary to another power or duty)." Section 18 as a whole defines the scope of the prohibition on disclosure. It does not, in itself, provide HMRC with the underlying legal power to disclose information because if HMRC is not prohibited from disclosure it nevertheless remains a creature of statute and must therefore identify a legal power to disclose.[27]

8.26 Where disclosure of revenue and customs information relating to a person is prohibited by section 18(1), the information is exempt from the Freedom of Information Act 2000 by virtue of section 44(1)(a) of that Act if its disclosure would specify the identity of the person to whom the information relates or would enable the identity of such a person to be deduced.[28]

Other confidentiality provisions in the 2005 Act

8.27 Additionally, information disclosed in reliance on subsection (2)(i), which permits disclosures made to the Scottish Ministers in connection with the collection and management of a devolved tax within the meaning of the Scotland Act 1998, may not be further disclosed without the general or specific consent of the Commissioners.[29] Information disclosed in the public interest under section 20 may not be further disclosed without the consent of the Commissioners, which may be general or specific and is deemed where the Commissioners have disclosed under section 20(7) for the purpose of enabling information to be

[27] There might be an argument that the section 18(2) grounds assume that the disclosure named is in fact within the power of HMRC, which might be a reason for holding that HMRC in fact has that power. However, we think the proper approach is to identify the power independently of section 18(2).

[28] Commissioners for Revenue and Customs Act 2005, s 23.

[29] Commissioners for Revenue and Customs Act 2005, s 18(2A).

entered into a computerised database.[30]

8.28 There is also a separate prohibition on further disclosure on information disclosed under section 21 (disclosure to a prosecuting authority), except for a purpose connected with the exercise of the prosecuting authority's functions or with the consent of the Commissioners.[31]

Wrongful disclosure

8.29 It is an offence to contravene the above confidentiality provisions by disclosing revenue and customs information relating to a person whose identity is specified in the disclosure or can be deduced from it.[32] Revenue and customs information means information about, acquired as a result of, or held in connection with the exercise of a function of the Revenue and Customs but, for these purposes, does not include information about the internal administrative arrangements of HMRC.[33]

8.30 The offence is punishable by up to two years' imprisonment, a fine or both.[34] A prosecution may only be instituted by the Director of Revenue and Customs Prosecutions or with the consent of the Director of Public Prosecutions, in England and Wales; or by the Commissioners or with the consent of the Director of Public Prosecutions for Northern Ireland, in Northern Ireland.[35]

8.31 There is a defence of reasonable belief that the disclosure was lawful or that the information had already and lawfully been made available to the public.[36]

8.32 Contravention of the prohibition on further disclosure under section 21(3) is also an offence with a maximum sentence of two years' imprisonment, a fine or both.[37] A prosecution may only be instituted by the Director of Revenue and Customs Prosecutions or with the consent of the Director of Public Prosecutions, in England and Wales; or by the Commissioners or with the consent of the Director of Public Prosecutions for Northern Ireland, in Northern Ireland.[38] There is also a defence of reasonable belief that the disclosure was lawful or that the information had already and lawfully been made available to the public.[39]

8.33 In addition to the wrongful disclosure offence contributing to a cautious attitude on the part of HMRC officials, some consultees seemed to suggest that the wrongful disclosure offence also acted to inhibit the onward disclosure of

[30] Commissioners for Revenue and Customs Act 2005, s 20(9).

[31] Commissioners for Revenue and Customs Act 2005, s 21(3).

[32] Commissioners for Revenue and Customs Act 2005, s 19(1).

[33] Commissioners for Revenue and Customs Act 2005, s 19(2).

[34] Commissioners for Revenue and Customs Act 2005, s 19(4).

[35] Commissioners for Revenue and Customs Act 2005, s 19(5) to (6).

[36] Commissioners for Revenue and Customs Act 2005, s 19(3).

[37] Commissioners for Revenue and Customs Act 2005, s 21(4) and (6).

[38] Commissioners for Revenue and Customs Act 2005, s 21(7) to (8).

[39] Commissioners for Revenue and Customs Act 2005, s 21(5).

information received from HMRC.[40] A similar offence was cited in relation to Department of Work and Pensions data.[41] It should be noted that there are in fact numerous wrongful disclosure offences in addition to section 19, applying in many cases to onward disclosure. However, as section 18(1) can only be contravened by a Revenue and Customs official and section 18(2A) and 20(9) only apply to certain cases of onward disclosure, it is not obvious why, for example, local government officials should express a fear of committing the offence in relation to the onward disclosure of information received from HMRC under its powers in the 2005 Act, other than section 18(2)(i) or section 20. We have some suspicion that this might be in part due to confusion between section 18(2)(a)(i) and section 18(2)(i), as only the latter is subject to the prohibition on onward disclosure in section 18(2A).

8.34 Part of the answer might lie in fears of secondary liability for the criminal act of another.[42] Individuals can be held criminally liable either as principals or secondary parties to an offence. Where an offence is committed by a principal, a secondary party can be held liable for the same offence where they "aid and abet, counsel or procure" that offence.[43] The words are given their ordinary meaning.[44] For example, aiding and abetting could be done by intentionally encouraging a wrongful disclosure[45] and counselling or procuring could be done by advising or soliciting a wrongful disclosure.[46] There might also be a question of an offence of intentionally encouraging or assisting an offence under section 44 Serious Crime Act 2007. It should be stressed that this is highly theoretical. We are unaware of any such argument being made or any prosecution being brought on this basis. These doctrines in any event cannot render unlawful an onward disclosure where the initial disclosure is lawful. It can only extend liability for the unlawful act of a Revenue and Customs official in the initial disclosure. We think the fears expressed by some consultees are based on a misconception but such perceptions have a real impact on data sharing.

8.35 Another potential explanation is based on section 55 of the Data Protection Act 1998. The offence under section 55 is unrelated to the wrongful disclosure provisions in the Commissioners for Revenue and Customs Act 2005 but could apply in relation to questions of onward disclosure. Section 55 provides that a person is guilty of an offence if he or she knowingly or recklessly obtains or discloses personal data or the information contained in personal data, or procures the disclosure to another person of the information contained in personal data, without the consent of the data controller. There are exceptions where a person shows that:

(1) The obtaining, disclosing or procuring was necessary for the purpose of preventing or detecting crime or was required or authorised under any

[40] Consultation meeting no. 7 – Amberhawk Conference.

[41] See ch 9 on the Department for Work and Pensions.

[42] See generally Archbold, *Criminal Pleading, Evidence and Practice* (2014).

[43] Accessories and Abettors Act 1861, s 8; Magistrates' Courts Act 1980, s 44.

[44] *Attorney General's Reference (No. 1 of 1975)* [1975] QB 773.

[45] *R v Clarkson* [1971] 1 WLR 1402.

[46] *R v Calhaem* [1985] QB 808.

enactment, by any rule of law or by the order of a court.

(2) He or she acted in the reasonable belief that he or she had in law the right to obtain or disclose the data or information, or to procure the disclosure of the information to the other person.

(3) He or she acted in the reasonable belief that he or she would have had the consent of the data controller if the data controller had known of the obtaining, disclosing or procuring and the circumstances of it.

(4) In the particular circumstances the obtaining, disclosing to procuring was justified as being in the public interest.

8.36 Therefore, if a person holding information, in relation to which HMRC is the data controller, knowingly or recklessly discloses that information onwards without HMRC's consent, in circumstances that do not fall under the exceptions above, an offence would be committed by the disclosing person. This could occur, for example, where HMRC discloses information pursuant to its functions to a data processor for a particular purpose and the data processor discloses onwards without consent. It may be difficult to know whether HMRC is the data controller of information or whether it has disclosed the information to another who holds it as controller in their own right. However, in such circumstances a reasonable if mistaken belief that the person was the data controller himself or herself and therefore had in law the right to obtain or disclose the data or information would amount to a defence.

8.37 We are unaware of any prosecution brought on such a basis, although clearly the threat or fear can have some effect on officials asked to make data sharing decisions. Although the penalty for a section 55 offence is only a fine, any conviction is highly damaging for public officials.[47] There is a power exercisable by the Secretary of State to provide by order to amend the Data Protection Act 1998 to make an offence under section 55 an imprisonable offence.[48] Although the provision itself came into force on 8 May 2008, no such order has been made to date.[49]

8.38 In the absence of wrongful disclosure provisions in the 2005 Act, HMRC would therefore retain some control over onward disclosure if it discloses on a basis which means it retains its status as data controller. However, HMRC told us that it does not generally view the department as the data controller for information shared through legislative gateways. The requirement for HMRC's consent to onward disclosure is usually set out in legislation, rather than occurring because it remains the data controller. It is a requirement laid on the receiving body by the relevant legislation. There may be some confusion over the existence, use and effect of these provisions, but there are also numerous wrongful disclosure offences linked to particular statutory gateways outside the 2005 Act. A strong argument can be made for reviewing the use of wrongful disclosure offences in relation to information disclosure. Consultees consistently expressed greater

[47] Such conduct could also be the subject of internal disciplinary proceedings.

[48] Criminal Justice and Immigration Act 2008, s 77.

[49] See Rosemary Jay, *Data Protection Law and Practice* (4th ed) p 721 for a discussion of the history of calls for the use of this power.

fears of criminal liability than we felt were justified. The fragmentary and inconsistent existence of wrongful disclosure offences may be part of the cause of this and this may benefit from rationalisation and simplification.

Express powers to share information in the Commissioners for Revenue and Customs Act 2005

8.39 Under section 20 of the 2005 Act, HMRC has a power to disclose information in the public interest.

8.40 Disclosure is permitted where it is made on the general or specific instructions of the Commissioners; the Commissioners are satisfied that it is in the public interest; and one of the following applies:

(1) The disclosure is made to a person exercising public functions for the purposes of the prevention or detection of crime in order to comply with an obligation of the United Kingdom, or Her Majesty's Government, under an international or other agreement relating to the movement of persons, goods or services.

(2) The disclosure is made to a body which has responsibility for the regulation of a profession and relates to misconduct on the part of a member of the profession, where that misconduct occurs in relation to a function of the Revenue and Customs.

(3) The disclosure is made to a constable exercising functions which relate to the movement of persons or goods into or out of the United Kingdom or is made for the purposes of the prevention or detection of crime.

(4) The disclosure is made to the National Criminal Intelligence Service and for a purpose connected with its functions under section 2(2) of the Police Act 1997.[50]

(5) The disclosure is made to a person exercising public functions in relation to public safety or public health and for the purposes of those functions.

(6) The disclosure is made to the Secretary of State for the purpose of enabling information to be entered into a computerised database and the information relates to a person suspected of an offence, a person arrested for an offence, the results of an investigation and anything seized.[51]

8.41 The Treasury may also specify in regulations kinds of information to which public interest disclosure applies, if the Treasury is satisfied that it relates to national security, public safety, public health or the prevention or detection of crime.[52] Such regulations may make provision limiting or restricting the disclosures that may be made in reliance on the regulations.[53] Regulations must be made by

[50] This provision deals with criminal intelligence.

[51] Commissioners for Revenue and Customs Act 2005, s 20(1) to (7).

[52] Commissioners for Revenue and Customs Act 2005, s 20(1)(b)(ii) and (8)(a).

[53] Commissioners for Revenue and Customs Act 2005, s 20(8)(b).

statutory instrument under the affirmative resolution procedure.[54] No regulations have been made to date. HMRC has also informed us that no requests have been made for regulations to be made under this power, perhaps because the relevant circumstances are so narrow.

8.42 HMRC also has a power to disclose information to a prosecuting authority, including for the purpose of enabling the authority to consider whether to institute criminal proceedings in respect of a matter considered in the course of an investigation conducted by or on behalf of Her Majesty's Revenue and Customs and to give advice in connection with a criminal investigation or criminal proceedings.[55]

THE PLETHORA OF GATEWAYS

8.43 Section 18(1) is also subject to any other enactment permitting disclosure.[56] According to HMRC, there are 273 such provisions in legislation.[57] These function to permit sharing outside the powers discussed above.

8.44 In the remainder of this Chapter, we survey the variety of statutory provisions that enable HMRC to share data. Those powers range from very wide to very narrow permissive gateways and include permissive gateways for the disclosure of information to assist another body in the performance of that body's statutory functions and permissive gateways to establish exchanges of information. There are provisions providing for the compilation or maintenance of registers. There are also a variety of mandatory gateways: powers held by other bodies to obtain information from HMRC. Such powers take the form of powers to request or require information, duties to disclose information triggered by requests, powers to require attendance or information by notice, powers to inspect, copy or remove documents, powers of access to computers and other rights of access to systems, powers to require disclosure or evidence by order, duties promptly to inform a body in defined circumstances, and powers to authorise disclosure by regulation. Powers also exist which place limits on the use of a gateway by type or source of information, place restrictions on the way in which information can be held or used, or limit recipients by reference to statutory lists.

8.45 It was also suggested to us in consultation that some of these powers are relied upon on occasion because they offer better control of the conditions for onward disclosure and more effective sanctions for wrongful disclosure. This was

[54] Commissioners for Revenue and Customs Act 2005, s 20(8)(c) to (d).

[55] Commissioners for Revenue and Customs Act 2005, s 21; see Public Bodies (Merger of the Director of Public Prosecutions and the Director of Revenue and Customs Prosecutions Order) 2014, SI 2014 No 834, s 9.

[56] Commissioners for Revenue and Customs Act 2005, s 18(3).

[57] Consultation meeting no.11 – HMRC. HMRC shared a spreadsheet detailing its powers with us. It is important to note that, as warned by HMRC, even this spreadsheet is not up to date. In the brief survey of the different types of power conducted below, we found seven gateways that have been repealed or revoked and replaced with similar provisions in other Acts or statutory instruments. We find this indicative of the problems that arise when a proliferation of statutory gateways for highly specific purposes are scattered across so many diverse statutes. It is clearly difficult to keep such arrangements under review.

considered necessary to give HMRC the confidence to share.[58]

8.46 Many of the powers are certainly more elaborate than the gateways in the 2005 Act. Many contain detailed provisions on:

(1) the identity of discloser and recipients;

(2) tests to be applied, such as reasonableness, and considerations to be taken into account when exercising a discretion to share;

(3) the purposes for which information can be disclosed, from broad to narrow purposes;

(4) conditions that must be fulfilled for a power or duty to share to arise;

(5) the identity of the individual who makes the decision as to whether the discloser discloses information to the recipient, which can be the discloser (for permissive powers), the recipient (for mandatory powers) or even sometimes a third party (where that party determines whether A should disclose to B);[59]

(6) the procedure that must be followed, including notices, orders, directions, mechanisms for challenge and appeal;

(7) prohibitions on and conditions for onwards disclosure, enforced by wrongful disclosure offences, with different statutory defences; references to compliance with codes;

(8) explicit proportionality provisions; limits on the type of information that can be disclosed;

(9) limits on the way information can be held or presented;

(10) provision for the format in which information may or must be shared; the disapplication of confidentiality or other statutory requirements;

(11) the relationship between the powers and the Data Protection Act 1998, Freedom of Information Act 2000 and Regulation of Investigatory Powers Act 2000; and

(12) the effect of other powers on the power concerned.

8.47 There is a spectrum of provisions, from a broad permission to share to duties to disclose. There are duties to inform promptly; duties to pass on information routinely; duties to pass on information if required, ordered, or given notice; permissive gateways triggered by a request or notice; and discretionary permissive gateways varying from extremely narrow to very broad permissions. Some of the statutory provisions applicable to HMRC disclosure do not concern

[58] Consultation meeting no. 11 – HMRC.

[59] For example, the Secretary of State for Education has the power to require HMRC to pass information to local authority databases under a regulation making power under s 12 of the Children Act 2004, although the power is not in use for that, or any, purpose currently.

HMRC exclusively but are also applicable to other public bodies.

8.48 Not all of the provisions to share data or establish data sharing mechanisms are currently in use. Some appear to have been established for particular projects, which no longer exist.[60] Some provide for the compilation or establishment of registers or databases rather than disclosure.

8.49 A survey of some of the statutory gateways applicable to HMRC highlights some important themes when considering the drafting and structure of such powers. The powers show a significant diversity of approach. They cannot be easily taken out of context as controls and conditions on the use of the power are often found in the surrounding legislation. Gateways are drafted in a detailed and highly specific manner and are sometimes idiosyncratic. A full law reform project would require a mapping exercise of powers to share information.

8.50 It is not always clear why different approaches are taken. We believe this reflects the ad hoc and disjointed way in which HMRC's powers have evolved over time. We also believe that this is true more broadly of the legislative framework relating to data sharing. Analysis of HMRC's statutory gateways points towards an important set of considerations for any reform project that would seek to rationalise and simplify information disclosure with appropriate and robust safeguards and appropriate mechanisms. The question is whether the disjointed, inconsistent and scattered powers of bodies to share information can be consolidated, simplified and made more easily accessible and understandable without losing important distinctions and safeguards that reflect the particular needs of very different sharing arrangements. We feel that such an analysis would be an important exercise, which would need to consider all the aspects of information disclosure arrangements explained above and described in detail below. HMRC has told us that it agrees with the key point of this section, that it would be helpful to rationalise existing gateways.

8.51 HMRC added, in correspondence with us, that gateways are often created by other departments for their own purposes, sometimes with little, or indeed, no, consultation with HMRC about the form of the gateway or the policies to be applied. Another factor is that historically there was relatively little consistency across the many gateways created to enable HM Customs and Excise and Inland Revenue to share information, some of which date back to the 1960s and 1970s. Since the merger of the departments to create HMRC in 2005, HMRC has sought to apply a set of consistent "policy principles" to its statutory information gateways. These include the preference for the gateway to be permissive to provide flexibility for HMRC and to ensure that the information flow remains within HMRC's capacity to provide; restrictions on onward disclosure; and the requirement for a criminal sanction for wrongful disclosure of identifying information.

EXAMPLES OF HMRC'S GATEWAYS

Powers to disclose for a general purpose (permissive gateways)

8.52 Some powers grant HMRC very wide powers to disclose information for broad and general purposes.

Serious Crime Act 2007, section 68

8.53 For example, section 68 of the Serious Crime Act 2007 provides that a public authority may, for the purposes of preventing fraud or a particular kind of fraud, disclose information, of any kind, as a member of a specific anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation, to specified anti-fraud organisations,[61] members of such organisations and any other people to whom disclosure is permitted under the arrangements concerned.[62] Section 68(3) provides that disclosure under the section does not breach any obligation of confidence or any other restriction on the disclosure of information, however imposed,[63] although it provides that nothing in the section authorises any disclosure of information which contravenes the Data Protection Act 1998 or is prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000.[64] The provision also provides that nothing in the section authorises a public authority which has functions exercisable within devolved competence, as defined by section 54 of the Scotland Act 1998, to disclose information whose subject-matter is a matter about which provision would be within the legislative competence of the Scottish Parliament if it were included in an Act of that Parliament.[65] The section also clarifies that it does not limit the circumstances in which information may be disclosed apart from the section.[66]

8.54 Revenue and customs information disclosed by HMRC under section 68 of the 2007 Act which reveals the identity of the person to whom it relates is protected by a wrongful onward disclosure offence. It is an offence for a person, who has received such information from HMRC or come into possession of it as a result of such a disclosure by HMRC to another person, to disclose the information, where the persons knows, suspects or has reasonable grounds to suspect the information is information of that kind.[67]

8.55 There are exceptions where the disclosure is made by a person acting on behalf of a person to whom the information was disclosed and the disclosure is to another person acing on behalf of that person, whether as an employee or otherwise; where the disclosure is for the purposes of the detection, investigation or prosecution of an offence in the UK; where the disclosure is with the consent of HMRC; or where it is a disclosure made in pursuance of a European Union

[60] For example, Children Act 2004, s 12.

[61] Such organisations were specified in Serious Crime Act 2007 (Specified Anti-Fraud Organisations) Order 2008, SI 2008 No 2353. They are CIFAS, Experian Limited, Insurance Fraud Investigators Group, N Hunter Limited, The Insurance Fraud Bureau, and The Telecommunications United Kingdom Fraud Forum Limited.

[62] Serious Crime Act 2007, s 68(1) to (2).

[63] Serious Crime Act 2007, s 68(3).

[64] Serious Crime Act 2007, s 68(4).

[65] Serious Crime Act 2007, s 68(5) to (6). Note that these provisions are pending repeal at a date to be appointed: Criminal Justice and Licensing (Scotland) Act 2010, s 98.

[66] Serious Crime Act 2007, s 68(7).

[67] Serious Crime Act 2007, s 69.

obligation or duty imposed by an enactment.[68] There is a defence of reasonable belief that the disclosure was lawful or that the information has already and lawfully been made available to the public.[69] The offence is subject to a maximum penalty of two years imprisonment and a fine or both and prosecution can only be brought by the Director of Revenue and Customs Prosecutions or with the consent of the Director of Public Prosecutions, in England and Wales.[70]

8.56 It is useful to note, in relation to this offence, that in the Public Bill Committee in the House of Commons the Parliamentary Under-Secretary of State for the Home Department, Vernon Coaker MP, explained:

> Clauses 64 and 65 were included in the Bill in recognition of the fact that a specific additional safeguard is needed to protect against improper onward disclosure of Her Majesty's Revenue and Customs information. That is to conform with the safeguards attached to HMRC information in other circumstances. Clause 64 allows for the same additional safeguards to be applied by order to public authorities' information. I hope that it is evident that the penalty in clause 65 applies in a very narrow set of circumstances relating to wrongful onward disclosure of information shared by public authorities through a specified anti-fraud organisation. Currently, that applies only to HMRC information.
>
> The maximum penalty of two years' imprisonment is consistent with the maximum penalty for all other comparable data-sharing offences — for example, under section 19 of the Commissioners for Revenue and Customs Act 2005 and section 10 of the Official Secrets Act 1989. In addition, the Government have proposed an amendment to the Data Protection Act 1998 to include a maximum custodial penalty of two years for the offence of unlawfully obtaining personal data under section 55 of that Act; the measure is in the recently published Criminal Justice and Immigration Bill. The Government do not accept the case for doubling the penalty in the limited circumstances of clause 64.[71]

8.57 There is also provision for a code of practice for disclosure of information to prevent fraud, although this is not yet in force.[72]

Anti-terrorism, Crime and Security Act 2001, section 19

8.58 The effect of section 19 of the Anti-Terrorism, Crime and Security Act 2001 is,

[68] Serious Crime Act 2007, s 69(2). There is also an exception regarding information relating to provision within the competence of the Scottish Parliament, which is pending repeal.

[69] Serious Crime Act 2007, s 69(4)

[70] Serious Crime Act 2007, s 70.

[71] *Hansard* (HC), 5 July 2007, col 251, Public Bill Committee, 8th Sitting. On the proposed amendment to the Data Protection Act 1998, which became the Criminal Justice and Immigration Act 2008, s 77, see above at para 8.37 and Rosemary Jay, *Data Protection Law and Practice* (4th ed) p 721 for a discussion of the history of calls for the use of this power.

[72] Serious Crime Act 2007, s 71.

according to HMRC, to give HMRC a very broad power to disclose information held by or on behalf of HMRC for the purposes of any criminal investigation whatsoever which is being or may be carried out, whether in the United Kingdom or elsewhere; for the purposes of any criminal proceedings whatever which have been or may be initiated, whether in the United Kingdom or elsewhere; for the purposes of the initiation or bringing to an end of any such investigation to proceedings; or for the purpose of facilitating a determination or whether any such investigation or proceedings should be initiated or bought to an end.[73] Such a disclosure must be proportionate to what is sought to be achieved by it and can be made by the Commissioners for Revenue and Customs, or with their authority. [74] By section 13 of the 2005 Act, an officer of HMRC may exercise any function of the Commissioners apart from some limited non delegable functions set out in that section, so HMRC officers may make such a disclosure.

8.59 Nothing in section 19 authorises disclosures prohibited by any provision of the Data Protection Act 1998[75] and nothing shall be taken to prejudice any power to disclose information which exists apart from the section.[76]

8.60 Information obtained by means of a disclosure authorised by section 19 of the 2001 Act cannot be further disclosed except for a purpose mentioned in section 19(2) and with the consent of the Commissioners.[77] Nothing in section 19 creates an offence of wrongful disclosure, so the prohibition can only be enforced by injunction or ex post facto internal disciplinary action; the same as applies to HMRC information outside the scope of section 19 of the Commissioners for Revenue and Customs Act 2005.

CAN A STATUTORY PROVISION TO THE EFFECT THAT "NO OBLIGATIONS OF SECRECY PREVENT DISCLOSURE" CREATE A POWER TO DISCLOSE?

8.61 However, the section is not without difficulties.[78] It provides that no obligation of secrecy imposed by statute or otherwise prevents the disclosure of information to which the section applies.[79] It is not clear that mere removal of an obligation of secrecy is sufficient to create a power to share the information. Even if HMRC is not bound by obligations of secrecy it must, as a statutory department, point to a positive power to disclose. Disclosure under the 2001 Act is however far broader in scope than public interest disclosure under section 20 of the Commissioners for Revenue and Customs Act 2005.

8.62 This appears to be an example of a wider problem: many statutory powers on disclosure of information are drafted merely in terms of providing that no obligation of secrecy however imposed prevents disclosure.

8.63 The effect of this has not been considered by the courts. The section has been

[73] Anti-terrorism, Crime and Security Act 2001, s 19.

[74] Anti-terrorism, Crime and Security Act 2001, s 19(3).

[75] Anti-terrorism, Crime and Security Act 2001, s 19(7).

[76] Anti-terrorism, Crime and Security Act 2001, s 19(10).

[77] Anti-terrorism, Crime and Security Act 2001, s 19(5).

[78] The 2001 Act has been criticised for a number of flaws.

[79] Anti-terrorism, Crime and Security Act 2001, s 19(2).

treated as creating a power and has not been challenged but it remains the case that on the face of it the section only disapplies a statutory duty of confidentiality. It is not at all clear that this confers a power to share. A purposive interpretation of the legislation could support an argument that the intention is to allow disclosure, therefore creating the necessary power. It is clearly arguable that the section assumes or implies that the necessary power does exist underlying the removal of the prohibition. Nevertheless, we find this form of drafting puzzling.

Permissive gateways for the disclosure of information for the purposes of another body's functions

8.64 Many gateways provide for information disclosure for the purposes of another body. This is necessary as disclosure purely for the functions of another body will not fall under the power of HMRC to disclose for the purposes of its functions.[80] The existence of such powers may also be necessary to facilitate sharing because it enables HMRC to rely upon the condition in schedule 2(5) or 3(7) of the Data Protection Act 1998 – that the processing of personal data or sensitive personal data respectively is necessary for the exercise of any function conferred by or under an enactment – when demonstrating that the processing in question is fair, especially where exemptions such as national security do not apply to the processing in question. [81]

Counter Terrorism Act 2008, sections 19 and 20

8.65 HMRC[82] may disclose information to any of the intelligence services for the purposes of the exercise by that service of any of its functions, subject to the Data Protection Act 1998 and Part 1 of the Regulation of Investigatory Powers Act 2000.[83] This power is clearly broader than the public interest power under section 20 of the Commissioners for Revenue and Customs Act 2005.

Transport (Scotland) Act 2001, section 63

8.66 A narrower permissive gateway exists in section 63 of the Transport (Scotland) Act 2001, which provides that information obtained by, among other things, a government department may be disclosed to a charging authority in relation to road user charging schemes in Scotland for or in connection with the exercise of any of the charging authority's functions with respect to a charging scheme.[84] It contains provision for onward disclosure, providing that any information which has been or could be disclosed under section 63(1) for or in connection with the exercise of the charging authority's functions may be disclosed to any person with whom the authority has entered into arrangements under section 61(b) of the

[80] Although it is possible that sharing for another's purposes as part of a broader exchange which assisted HMRC to carry out its own functions could fall within the scope of s 9 of the Commissioners for Revenue and Customs Act 2005. We certainly heard a similar argument being made in relation to implied powers from a small number of consultees during the consultation period. See para 8.19 above.

[81] Data Protection Act 1998, s 28.

[82] Indeed any person.

[83] Counter Terrorism Act 2008, ss 19 and 20.

[84] Transport (Scotland) Act 2001, s 63(1). A charging scheme is a scheme for imposing charges in respect of the use or keeping of motor vehicles on roads and a charging authority is the local traffic authority which made or proposes the scheme: s 49(5).

Act,[85] and information disclosed in that way may be disclosed to any other person in connection with the charging scheme but not used otherwise than in connection with the charging scheme.

Corporation Tax Act 2010, section 261

8.67 Section 261(b) of the Corporation Tax Act 2010 is regarded by HMRC as a statutory gateway. It provides that no obligation as to secrecy or other restriction on the disclosure of information imposed by statute or otherwise prevents the disclosure of information to the Secretary of State for the purpose of assisting the Secretary of State to discharge his or her functions in connection with that part of the Act. Information obtained by such disclosure is not permitted to be further disclosed, except for the purposes of legal proceedings arising out of the functions to which it refers.[86]

Corporation Tax Act 2009, section 1206

8.68 Section 1206 of the Corporation Tax Act 2009 provides that section 18(1) of the Commissioners for Revenue and Customs Act 2005 does not prevent disclosure to the Secretary of State for the purposes of the Secretary of State's functions under listed provisions concerning the certification of relevant programmes as British, the certification of video games as British, and the certification of films as British.[87]

8.69 Section 1206(2) provides that information so disclosed may be disclosed to the British Film Institute. Section 1206(3) provides that a person to whom information is disclosed may not otherwise disclose it except for the purposes of the Secretary of State's listed functions; if the disclosure is authorised by an enactment; if the disclosure is in pursuance of a court order; for the purposes of a criminal investigation or legal proceedings (whether criminal or civil) connected with the operation of Parts 15 to 15B of the Corporation Tax Act 2009 or schedule 1 to the Films Act 1985; or with the consent of either HMRC or each person to whom the information relates.

Finance Act 1994, schedule 7 paragraphs 28 to 28B

8.70 Schedule 7 paragraph 28 to the Finance Act 1994 provides that notwithstanding any obligation not to disclose information that would otherwise apply, HMRC may disclose information to the Secretary of State, or an officer authorised by the Secretary of State, whose name must be notified to HMRC in writing, for the purpose of assisting the Secretary of State in the performance of his duties under the Act. Information that has been disclosed to a person by virtue of this cannot be disclosed by him except to another person to whom the disclosure could have been made instead of him or for the purpose of any proceedings connected with the operation of any provision of, or made under, any enactment in relation to insurance or to tax. Paragraph 28A makes identical provision in respect of the Treasury. Paragraph 28B provides that HMRC may disclose information to the Financial Conduct Authority or the Prudential Regulation Authority for the

[85] Transport (Scotland) Act 2001, s 63(3)(a).

[86] Corporation Tax Act 2010, s 261(2).

[87] Corporation Tax Act 2009, s 1206(1) to (1A).

purpose of assisting those regulators in the performance of their functions. Such information cannot be further disclosed except for the purpose of any proceedings connected with the operation of any provision or, or made under, any enactment in relation to insurance or to tax. [88]

Financial Services and Markets Act 2000, section 350

8.71 Section 350 of the Financial Services and Markets Act 2000 provides that no obligation as to secrecy imposed by statute or otherwise prevents the disclosure of revenue information to the Financial Conduct Authority or Prudential Regulation Authority, if the disclosure is made for the purpose of assisting or enabling those regulators to discharge functions under the Act or any other Act, or to the Secretary of State, for the purpose of assisting in the investigation of a matter under section 168 of the Act or with a view to the appointment of a section 168 investigator. Disclosures to the Financial Conduct Authority and Prudential Regulation Authority may only be made by or under the authority of the Commissioners of Inland Revenue.[89] Information so obtained may not be used except: for the purpose of deciding whether to appoint a section 168 investigator; in the conduct of a section 168 investigation; in criminal proceedings brought against a person under the Financial Services and Markets Act 2000 or the Criminal Justice Act 1993 as a result of a section 168 investigation; for the purpose of taking action under the Act against a person as a result of a section 168 investigation; or in proceedings before a Tribunal as a result of such action taken.[90] Such information obtained from HMRC may not be disclosed except by or under the authority of the Commissioners of Inland Revenue or in the proceedings mentioned above or with a view to their institution, unless the person to whom it is disclosed is a person to whom it could have been disclosed under section 350(1).[91]

8.72 Section 350(5), prohibiting onward disclosure, is accompanied by a wrongful disclosure offence subject to a maximum penalty of two years' imprisonment, a fine or both.[92] It is also an offence, subject to a penalty of up to three months imprisonment or a level 5 fine, to use information for a purpose other than those listed in section 350(4).[93] There is a defence where a person did not know and had no reason to suspect that information was confidential information or that it had been disclosed in accordance with section 350 and took all reasonable precautions and exercised all due diligence to avoid committing the offence.[94]

[88] Finance Act 1993, s 37 is drafted in identical terms regarding disclosure to the Secretary of State, the Gambling Commission, or their authorised officers, for the purposes of assisting them in the performance of duties imposed by or under any enactment in relation to lotteries. Finance Act 1994, sch 7, para 28B(2)

[89] Financial Services and Markets Act 2000, s 350(2). The consent could now be given by the Commissioners for Revenue and Customs: Commissioners for Revenue and Customs Act 2005, s 5(2)(a).

[90] Financial Services and Markets Act 2000, s 350(4).

[91] Financial Services and Markets Act 2000, s 350(5) to (6).

[92] Financial Services and Markets Act 2000, s 352(1) to (2).

[93] Financial Services and Markets Act 2000, s 352(4) to (5).

[94] Financial Services and Markets Act 2000, s 352(6).

Construction Products Regulations 2013, regulation 13

8.73 Regulation 13 of the Regulations gives the Secretary of State a power, where he or she considers that information is required which another person is likely to be able to provide, for the purpose of deciding whether to serve, vary or revoke a prohibition notice or to serve to revoke a notice to warn, to serve a notice requiring that person to provide specified information within a specified period and to produce specified records as a specified time and place and to permit a person appointed by the Secretary of State to take copies of the records at that time and place.[95] It is an offence punishable by fines to fail, without reasonable cause, to comply with such a notice or to provide information, knowingly or recklessly, which is false in a material particular.[96]

Charities Act 2011, section 54

8.74 Section 54 provides that HMRC may disclose information to the Charity Commission if the disclosure is made for the purpose of enabling or assisting the Commission to discharge any of its functions, where the information relates to an institution, undertaking or body that is a charity; an institution established for charitable, benevolent or philanthropic purposes, an institution by or in respect of which a claim for tax exemption has at any time been made, or a subsidiary undertaking of a charity or a body entered in the Scottish Charity register which is managed or controlled wholly or mainly in or from England and Wales.[97] Sections 56 and 57 control the further disclosure of HMRC information by the Commission.

8.75 Section 57 provides that Revenue and Customs information disclosed under section 54(1) may not be further disclosed without the consent of HMRC.[98] Such disclosure is an offence punishable by up to two years imprisonment, a fine or both.[99] There is a defence of reasonable belief in the lawfulness of the disclosure or that the information had already and lawfully been made available to the public.

Permission to exchange

Trade in Animals and Related Products (Wales) Regulations 2011, regulation 37

8.76 Regulation 37 provides that HMRC, general customs officials and any enforcement authority may exchange information for the purposes of the Regulations and may divulge information to the enforcement authorities in England, Scotland and Northern Ireland for the purposes of the Part or the equivalent legislation in those jurisdictions. No person may disclose information so received if the information relates to a person whose identity is specified in the disclosure or can be deduced from the disclosure, the disclosure is for a purpose other than the purposes specified in the paragraph and the Commissioners have

[95] Construction Products Regulations 2013, SI 2013 No 1387, reg 13(1) to (2).

[96] Construction Products Regulations 2013, SI 2013 No 1387, reg 13(3) to (4).

[97] Charities Act 2011, s 55.

[98] Charities Act 2011, s 57(2).

[99] Charities Act 2011, s 57(3) to (4).

not given their prior consent.[100]

8.77 Breach of regulation 37(3) is an offence, punishable by up to two years' imprisonment, a fine or both.[101]

Firearms Act (Amendment) Regulations 1992, regulation 10(1)(b)

8.78 Regulation 10(1)(b) provides that no obligation as to secrecy or other restriction upon the disclosure of information imposed by statute or otherwise shall preclude disclosure to the Secretary of State or any officer of his by any government department of any information required by the Secretary of State for the purpose of facilitating the communication or exchange of information in pursuance of the 1991 Directive on control of the acquisition and possession of weapons.

Tests of reasonable requirement

Housing Scotland Act 1987, section 195(5)

8.79 HMRC may disclose to the Secretary of State such particulars as he or she may reasonably require for determining whether a grant should be made under the section or whether a grant so made should be repaid or the amount of such a grant or repayment.[102]

Examples of mandatory gateways

8.80 Various forms of mandatory information disclosure apply to HMRC.

Banking Act 2009, section 218

8.81 For example, section 218(3) of the Banking Act 2009 provides that HMRC shall transfer to the Bank of England any information acquired or held in connection with functions in respect of the issue of banknotes in Scotland or Northern Ireland.

Requesting or requiring

8.82 It is not always clear whether a power to request creates a permissive gateway for HMRC, if it agrees to the request, or a mandatory gateway, in which case it is hard to distinguish requests from requirements.

Merchant Shipping Act 1995, section 206

8.83 A general lighthouse authority may, for the purposes of determining whether any and, if so, what general light dues are payable in respect of any ship, require HMRC to furnish to the general lighthouse authority such information in its possession or control relating to the arrival or departure of the ship at or from any port within their area as they may reasonably require for the purpose or

[100] Trade in Animals and Related Products (Wales) Regulations 2011, SI 2011 No 2379, reg 37(3).

[101] Trade in Animals and Related Products (Wales) Regulations 2011, SI 2011 No 2379, regs 39 and 42.

[102] Housing Scotland Act 1987, s 195(5).

information relating to the movements of ships of any class or description.[103] It is the duty of HMRC to furnish the information as soon as reasonably practicable.[104]

Criminal Appeal Act 1995, section 17

8.84 Section 17 of the Criminal Appeal Act 1995 gives the Criminal Cases Review Commission power, where it believes that a person serving in a public body has possession or control of a document or other material which may assist the Commission in the exercise of any of its functions, and where it is reasonable to do so, to require the person who is the appropriate person in relation to the public body to produce the document or other material or give the Commission access to it and allow the Commission to take away the document or other material or make and take away a copy of it in such form as they think appropriate; may direct that person that the document or other material must not be destroyed, damaged or altered before the direction is withdrawn by the Commission. The section provides that the duty to comply is not affected by any obligation of secrecy or other limitation on disclosure which would otherwise prevent the production of the document or other material to the Commission or the giving of access to it to the Commission.[105]

Parliamentary Commissioner Act 1967, section 8

8.85 Section 8 of the Parliamentary Commissioner Act 1967 provides that for the purpose of an investigation under section 5(1) of the Act the Commissioner may require any Minister, officer or member of the department or authority concerned or any other person who is in his opinion able to furnish information or produce documents relevant to the investigation to furnish such information or produce any such document. No obligation to maintain secrecy or other restriction upon the disclosure of information obtained by or furnished to persons in Her Majesty's service, whether imposed by enactment or by any rule of law, applies to the disclosure of information for the purposes of an investigation under the Act.[106]

Mandatory sharing triggered by requests

Taxation (International and Other Provisions) Act 2010, section 128

8.86 Section 128 provides that no obligation as to secrecy imposed by enactment prevents HMRC from disclosing information required to be disclosed under the Arbitration Convention in pursuance of a request made by an advisory commission set up under the Convention.

Police Act 1997, section 113B (as amended by Serious Organised Crime and Police Act 2005)

8.87 Under section 113B of the Police Act 1997, which makes provision for the Disclosure and Barring Service to issue enhanced criminal record certificates, the Disclosure and Barring Service must, before issuing an enhanced criminal record certificate, request any relevant chief officer to provide any information which the

[103] Merchant Shipping Act 1995, s 206(1) to (2).

[104] Merchant Shipping Act 1995, s 206(4).

[105] Criminal Appeal Act 1995, s 17(4).

[106] Parliamentary Commissioner Act 1967, s 8(3).

officer reasonably believes to be relevant for the purpose described in the statement and in the officer's opinion ought to be included in the certificate.[107] For these purposes the Commissioners for HMRC are treated as if they were a police force.[108]

Revenue and Customs (Complaints and Misconduct) Regulations 2010, regulation 53

8.88 Regulation 53 of the Revenue and Customs (Complaints and Misconduct) Regulations 2010 provide that the Commissioners for Revenue and Customs are under a duty at all times to provide the Independent Police Complaints Commission with all such information and documents as may be specified or described in the 2010 Regulations.[109] It is also the duty of the Commissioners to provide the Independent Police Complaints Commission with all such other information and documents specified or described in a notification given by the Independent Police Complaints Commission to the Commissioners, and to produce or deliver up to the Independent Police Complaints Commission all such evidence and other things so specified or described, as appear to the Independent Police Complaints Commission to be required by it for the purposes of the carrying out of any of its functions.[110] The form, manner and period of providing, producing or delivering such information must be as specified in the notification imposing the requirement or in any subsequent notification given by the Independent Police Complaints Commission to the Commissioners for the purposes of the regulation.[111] A requirement imposed may authorise or require information or documents to be provided electronically.[112] Nothing requires the Commissioners to provide the Independent Police Complaints Commission with any information or document, or to produce or deliver up any other thing, before the earliest time at which it is practicable for the Commissioners to do so or to provide, produce, or deliver anything at all in a case in which it never becomes practicable to do so.[113]

Notices to require attendance/information

Freedom of Information Act 2000, section 51

8.89 The Information Commissioner may serve an authority with an information notice if he has received an application under section 50 of the Freedom of Information Act 2000 and reasonably requires any information, including unrecorded

[107] Police Act 1997, s 113B(4).

[108] Police Act 1997, s 113B(11).

[109] A similar provision, albeit with considerably less detail, can be found in the UK Border Agency (Complaints and Misconduct) Regulations 2010, SI 2010 No 782, reg 48. Revenue and Customs (Complaints and Misconduct) Regulations 2010, SI 2010 No 1813, reg 53(1).

[110] Revenue and Customs (Complaints and Misconduct) Regulations 2010, SI 2010 No 1813, reg 53(2).

[111] Revenue and Customs (Complaints and Misconduct) Regulations 2010, SI 2010 No 1813, reg 53(3).

[112] Revenue and Customs (Complaints and Misconduct) Regulations 2010, SI 2010 No 1813, reg 53(5).

[113] Revenue and Customs (Complaints and Misconduct) Regulations 2010, SI 2010 No 1813, reg 53(4).

information, [114] for the purposes of determining whether a public authority has complied or is complying with any of the requirements of Part 1 or for the purpose of determining whether a public authority in relation to the exercise of its functions under the 2000 Act conforms with that proposed in the codes of practice under section 45 and 46.[115] An information notice may require an authority, within such time as is specified in the notice, to furnish the Commissioner, in such a form as specified, with such information relating to the application, to comply with Part 1, or to conform with the code of practice as so specified.

8.90 An information notice must contain a statement of the purpose for which the information is sought and the Information Commissioner's reasons for regarding the information sought as relevant for the given purpose and particulars of the right of appeal conferred by section 57 of the Act.[116] The time specified in an information notice must not expire before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the information need not be furnished pending the determination or withdrawal of the appeal.[117] An authority is not required to furnish information in respect of legally privileged materials.[118]

Powers of inspection, copy and removal

Audit Commission Act 1998, section 6

8.91 Section 6 of the Audit Commission Act 1998 provides that an auditor has a right of access at all reasonable times to every document relating to a body subject to audit which appears to him necessary for the purposes of his functions under to Act.[119] The right includes a power to inspect, copy or take away the document.[120] An auditor may also require a person holding or accountable for any such document to give him such information and explanation as he thinks necessary for the purposes of his functions under the Act and, if he thinks it necessary, to require the person to attend before him in person to give the information or explanation or produce the document.[121]

8.92 The section also makes provision for documents kept in electronic form, which the auditor may require a person to produce in a form in which it is legible and can be taken away.[122] In connection with inspecting such a document, an auditor may obtain access to, and inspect and check the operation of, any computer and associated apparatus or material which he considers is or has been used in connection with the document and require individuals to afford him such

[114] For an example of extremely detailed legislative provision for powers to require information see the Criminal Justice Act 1987, ss 2 to 3. Freedom of Information Act 2000, s 51(7).

[115] Freedom of Information Act 2000, s 51(1).

[116] Freedom of Information Act 2000, s 51.

[117] Freedom of Information Act 2000, s 51(4).

[118] Freedom of Information Act 2000, s 51(5).

[119] Audit Commission Act 1998, s 6(1).

[120] Audit Commission Act 1998, s 6(1A).

[121] Audit Commission Act 1998, s 6(2).

[122] Audit Commission Act 1998, s 6(4A).

reasonable assistance as he may require for that purpose.[123] It is an offence punishable by fines to fail to comply with requirements of an auditor.[124]

Access to computers/rights of access

Budget Responsibility and National Audit Act 2011, section 9

8.93 Section 9 of the Budget Responsibility and National Audit Act 2011 gives the National Audit Office a right of access at reasonable times to all Government information which it might reasonably require for the purpose of the performance of its duty under section 4 of the Act.[125] The Office is entitled to require from any person holding or accountable for any Government information any assistance or explanation which the Office reasonably thinks necessary for that purpose, but the section is subject to any enactment or rule of law which operates to prohibit or restrict the disclosure of information or the giving of any assistance or explanation.[126]

Powers to order disclosure/require giving of evidence

Inquiries Act 2005, section 21

8.94 The Chairman of an inquiry may by notice require a person to attend at a time and place stated in the notice, or in the form of a written statement, to give evidence, to produce any documents in his comments in his custody or under his control that relate to a matter in question at the inquiry, to produce any other thing in his custody or under his control for inspection, examination or testing by or on behalf of the inquiry panel.[127] The Chairman may by notice require a person, within such period as appears to the inquiry panel to be reasonable to provide evidence to the inquiry panel in the form of a written statement.

8.95 The notice must explain the possible consequences of not complying with the notice and indicate what the recipient should do if he wishes to make a claim that he is unable to comply with the notice or it is not reasonable in all the circumstances to require him to comply with the notice.[128] Such claims are determined by the chairman of the inquiry, who may revoke or vary the notice on that ground, having first considered the public interest in the information in question being obtained by the inquiry, having regard to the likely importance of the information.[129]

Proceeds of Crime Act 2002, sections 345 and 350

8.96 A Proceeds of Crime Act production order[130] may be made in relation to material

[123] Audit Commission Act 1998, s 6(4B) to (4C).

[124] Audit Commission Act 1998, s 6(6).

[125] Budget Responsibility and National Audit Act 2011, s 9(1).

[126] Budget Responsibility and National Audit Act 2011, s 9(2) and (4). Contrast National Audit Act 1983, s 6, which is not subject to any such prohibition or restriction.

[127] Inquiries Act 2005, s 21(1) to (2).

[128] Inquiries Act 2005, s 21(3).

[129] Inquiries Act 2005, s 21(4) to (5).

[130] Proceeds of Crime Act 2002, s 345.

in the possession or control of an authorised government department and may require any officer of the department who may be for the time being in possession or control of the material to comply with it.[131]

Powers to authorise disclosures by regulation

Charities Act 2006, section 72

8.97 Section 72 of the Charities Act 1972 provides that the Minister may by regulations authorise relevant public authorities to disclose information to the Northern Ireland regulator for the purpose of enabling or assisting the regulator to discharge its functions.[132] Such regulations must prohibit onward disclosure of HMRC data without the consent of HMRC, enforced by a wrongful disclosure offence carrying a maximum sentence of two years' imprisonment, a fine or both and with a reasonable belief defence.

Limits placed on gateways by type/source of information

Customs and Excise Management Act 1979, section 10

8.98 Some legislation places limits on the type or source of the information to which it relates. For example section 10 applies only to information listed in the section and contained in any document with which the Commissioners have been provided in pursuance of the Customs and Excise Acts 1979 for the purpose of making entry of any goods on their importation.[133]

For the compilation or maintenance of a register

8.99 Some legislation provides power for the compilation or establishment of registers or other records, such as section 12 of the Children Act 2004.[134] Section 91 of the Value Added Tax Act 1994 provides that for the purpose of the compilation or maintenance by the Department for Business, Innovation and Skills of a central register of businesses, or for the purpose of any statistical survey conducted or to be conducted by those bodies, HMRC may disclose to an authorised officer listed particulars obtained or recorded by them in pursuance of the 1994 Act.[135]

Restrictions on manner of holding or using information

8.100 Some legislative provisions place additional restrictions on the way in which information can be held or used by HMRC. For example, regulation 4 of the Stamp Duty Land Tax (Use of Information Contained in Land Transaction Returns) Regulations 2009 provides that relevant information may be available for use by the Department of Finance and Personnel for the purpose of any of its lawful functions but must not be used in any way which would permit any person

[131] Proceeds of Crime Act 2002, s 350.

[132] Charities Act 2006, s 72(2).

[133] Customs and Excise Management Act 1979, s 10(2). The listed information is the description of the goods, including any maker's catalogue number; the quantities of the goods imported in a particular period; the name of the marker of the goods; the country of origin of the goods; the country from which the goods were consigned.

[134] See "Existing powers not currently in use" below.

[135] Value Added Tax Act 1994, s 91(1). Wrongful further disclosure is also protected by a criminal offence punishable by two years' imprisonment or a fine or both.

other than an officer of the Department of Finance and Personnel to identify the vendor or the purchaser.[136] The provision also adds that relevant information made available under the regulation must not be disclosed outside the Department of Finance and Personnel without the consent, general or specific, of HMRC.[137]

Specified lists of recipients

8.101 Some legislative provisions use lengthy lists of permitted recipients of information and purposes for which the information may be disclosed.[138]

Existing powers not currently in use

Children Act 2004, section 12

8.102 Sometimes steps are never taken to use existing powers in statute to facilitate information disclosure. For example, section 12 of the Children Act 2004 provides that the Secretary of State may, for the purpose of arrangements under section 10 and 11 of the Children Act 2004 or under section 175 of the Education Act 2002, by regulations require local authorities in England to establish or operate databases containing information in respect of persons to whom such arrangements relate or himself or herself establish and operate or make arrangements for the operation and establishment of one or more databases containing such information.[139] The section provides that the Secretary of State may make provision in relation to the establishment and operation by regulations of any databases under the section.[140] Those regulations may make provision permitting HMRC to disclose information for inclusion in the database.[141] However, this power has never been exercised with the effect that HMRC do not disclose information to Children Act 2004 Information Databases.[142] There are no regulations under section 12 currently in force.

CONCLUSIONS

8.103 A consideration of the legislative framework that applies to HMRC is valuable because it highlights many of the considerations that apply in drafting a legislative gateway for data sharing. It shows that legislative gateways are often detailed provisions capable of a great deal of variation, proliferating across a range of statutes and statutory instruments. Provisions are complex and lack consistency. However, there are distinct features and considerations that could form the basis

[136] Stamp Duty Land Tax (Use of Information contained in Land Transaction Returns) Regulations 2009, SI 2009 No 2095, reg 4(1).

[137] Stamp Duty Land Tax (Use of Information contained in Land Transaction Returns) Regulations 2009, SI 2009 No 2095, reg 4(2).

[138] Examples include the Serious Crime Act 2007, s 68; Finance Act 2000, sch 6, para 137; Offender Management Act 2007, s 14.

[139] Children Act 2004, s 12(1).

[140] Children Act 2004, s 12(5).

[141] Children Act 2004, s 12(6)(c) and (8)(c).

[142] See Explanatory Note to the Children Act 2004 Information Database (England) (Revocation) Regulations 2012, SI 2012 No 1278. The note explains that the "ContactPoint" database established and operated under this power was closed down on 6th August 2010 and the data it contained destroyed.

for designing a simplified approach to data sharing. These are the balance to be struck between a permissive or mandatory gateway approach in particular circumstances; controls on onward disclosure; restrictions on the type of information, uses of that information, and retention of that information; the procedure by which information can be disclosed, requested, and ordered; and other related provisions, such as permitting the creation of registers or other databases.

CHAPTER 9
THE DEPARTMENT FOR WORK AND PENSIONS

INTRODUCTION

9.1 This Chapter provides the second case study, discussing a detailed web of gateways. We have chosen the Department for Work and Pensions ("the Department"), as it is the largest ministerial department and it holds an enormous amount of personal data. Unlike HMRC, a creature of statute, the Department has both statutory and common law powers. The Department replaced the Department for Social Security as well as other predecessors and has taken on some of their powers. It does use common law powers to disclose information, but it seems to us that these have been eroded by successive statutory interventions. The Department also holds personal information about the vast majority of the population and sensitive data in relation to part of the population, data to which many other public bodies would like to gain access, and guards the information it holds closely.

9.2 The Department has a similar though less extensive proliferation of statutory powers to HMRC, drafted in detailed and diverse ways, reflecting the ad hoc development of the legislation, some of which has been subject to numerous amendments. In this Chapter we consider the powers of the Department in order to improve our understanding of the driving forces behind the proliferation of gateways. We also consider some features of the statutory scheme, where these illustrate general points from the consultation and concerns about the ad hoc nature of gateways in general.

9.3 We found at least 63 statutory gateways empowering the Department to share information with others, together with further provisions allowing other bodies to disclose or use data from the Department. In consultation, we saw a large number of express statutory gateways permitting, for example, local authorities to use or share social security information obtained from the Department in particular ways. Local authorities are creatures of statute and therefore need statutory authority, either express or implied, to act.[1] In addition, the wrongful disclosure offences relating to social security information apply to officials outside the Department itself. This contrasts with section 19 of the Commissioners for Revenue and Customs Act 2005, which applies to HMRC and those who supply services on its behalf. The result is that pressure to draft express gateways to ensure clarity and to reassure officials extend beyond the Department itself, even where there are implied powers that on a proper view could support sharing.[2] This in turn leads to a proliferation of gateways.

9.4 There are not as many wrongful disclosure provisions in relation to data held by the Department as there are in relation to HMRC's data. This seems to be related

[1] Such legality is of course also an important requirement of the Data Protection Act 1998 and Human Rights Act 1998.

[2] This desire to rely on an express statutory power to provide certainty was commented on by a number of local authorities. Consultation meeting no. 24 – Northumbria University Information Law Centre.

to the fact that the principal wrongful disclosure provision under section 18 of the Commissioners for Revenue and Customs Act 2005 only extends to HMRC officials, whereas the principal wrongful disclosure provision in relation to social security information extends to a far wider set of officials.[3] As a result, the legislation relating to HMRC has developed more detailed controls restricting onward disclosure, backed by discrete wrongful onward disclosure offences, whereas the Department has a wider-ranging prohibition on disclosure, tempered by express statutory gateways for its partners. The statutory schemes therefore, although both complex and tending towards the proliferation of gateways, look quite different in terms of the structure of onward disclosure provisions and wrongful disclosure offences. There may be additional reasons for structural differences in the statutory framework, and any full reform project would need to investigate these.

WRONGFUL DISCLOSURE UNDER SECTION 123 OF THE SOCIAL SECURITY ADMINISTRATION ACT 1992

9.5 The main wrongful disclosure offence in relation to social security is found in section 123 of the Social Security Administration Act 1992. This offence, combined with data protection law and the possibility of internal disciplinary action, is an effective deterrent, and no prosecutions have had to be launched under this section since the late 1990s.[4]

9.6 Section 123 makes it an offence for "a person who is or has been employed in social security administration or adjudication" to disclose, without lawful authority, any information acquired in the course of their employment which relates to a particular person.[5] It also makes it an offence for "a person who is or has been employed in the audit of expenditure or the investigation of complaints" to disclose, without lawful authority, any information acquired in the course of their employment, which is, or is derived from, information acquired or held by or for the purposes of any of the government departments or other bodies or persons referred to in Part 1 of schedule 4 to the Act or corresponding legislation in Northern Ireland, and which relates to a particular person.[6] Where a disclosure falls outside the broad scope of this section, statutory powers permitting disclosure can be found with distinct wrongful disclosure provisions. The offences are punishable by imprisonment of up to two years or a fine or both.[7]

9.7 It is not an offence under section 123 to disclose information in the form of a summary or collection, so framed as to prevent information relating to a particular person to be ascertained or to disclose information which has previously been disclosed to the public with lawful authority.[8] It is a defence for a person charged with an offence to prove that at the time of the alleged offence, they believed that they were making the disclosure in question with lawful authority and had no reasonable cause to believe otherwise, or that they believed that the information

3 Social Security Administration Act 1992, s 123.

4 Consultation meeting no. 44 – Department for Work and Pensions.

5 Social Security Administration Act 1992, s 123(1).

6 Social Security Administration Act 1992, s 123(2).

7 Social Security Administration Act 1992, s 123(5).

8 Social Security Administration Act 1992, s 123(3).

in question had previously been disclosed to the public with lawful authority and had no reasonable cause to believe otherwise.[9]

9.8 As with "persons employed in the audit of expenditure or the investigation of complaints", the reference to "persons employed in social security administration or adjudication" is given an extensive meaning. The expression includes persons specified in Part 1 of schedule 4 to the Act and corresponding legislation in Northern Ireland as well as any person who carries out the administrative work of any of the government departments or other bodies specified in that legislation and any person who provides, or is employed in the provision of, services to any of those departments, persons or bodies.[10] The schedule contains a long list of persons and bodies including, in addition to the Department for Work and Pensions, the Ministry of Justice and the Ministry of Defence, local authorities administering housing benefit or council tax benefit and civil servants in or staff of those bodies.[11]

9.9 A disclosure is regarded as made with lawful authority if, and only if, it is made:

(1) by a civil servant or a person employed in the audit of expenditure or the investigation of complaints, in accordance with his or her official duty;[12]

(2) by any other person either for the purposes of the function in the exercise of which he or she holds the information and without contravening any restriction duly imposed by the person responsible or to, or in accordance with an authorisation duly given by the person responsible;[13]

(3) in accordance with any enactment or order of a court;[14]

(4) for the purpose of instituting, or otherwise for the purposes of, any proceedings before a court or before any tribunal or other body or person referred to in Part 1 of schedule 4 to the Act or Part 1 of schedule 4 to the Northern Ireland Administration Act; or

(5) with the consent of the appropriate person.[15]

[9] Social Security Administration Act 1992, s 123(4).

[10] Social Security Administration Act 1992, s 123(6).

[11] Social Security Administration Act 1992, sch 4.

[12] Social Security Administration Act 1992, s 123(9)(a).

[13] Social Security Administration Act 1992, s 123(9)(b). The "person responsible" is the Secretary of State, the Lord Chancellor or any person authorised by either of those persons for the purposes of the subsection, including a reference to the "person responsible" within the meaning of any corresponding enactment having effect in Northern Ireland: Social Security Administration Act 1992, s 123(9).

[14] Social Security Administration Act 1992, s 123(9)(c).

Impact of express powers on common law powers

9.10 The Department makes use of its common law powers to share data, although the proliferation of statutory gateways can erode those powers in some circumstances.[16] The existence of common law powers can provide a lawful basis for processing information so as to ensure compliance with the first Data Protection Principle in the Data Protection Act 1998, and also to ensure that disclosure is "in accordance with the law" for the purposes of article 8 of the European Convention of Human Rights and the Human Rights Act 1998. However, the existence of so many express statutory powers, and concern about the erosion of common law powers, may have encouraged a tendency to create further statutory powers in order to provide a similar level of transparency and Parliamentary scrutiny, rather than relying on common law powers.

9.11 The Department informed us that where an express power exists, if a need is subsequently identified to share similar information in circumstances not covered by the power, it is likely to be necessary to consider legislating to extend the power rather than relying on common law powers.

Impact of express gateways on the statutory framework

9.12 The Department makes use of implied statutory powers to disclose information. In consultation we heard that a focus on express gateways has undermined confidence in the use of implied gateways.[17] However, the proliferation of gateways suggests a pressure to make data sharing powers explicit to avoid the risk of legal challenge as to the scope and terms of any implied gateway.[18] This will also be true where there is sufficient doubt about the scope of an express power to make it unsafe to rely on the statutory defence under section 123(4): belief that the disclosure in question was made with lawful authority, without reasonable cause to believe otherwise. If a reasonable legal uncertainty is

[15] Social Security Administration Act 1992, s 123(9)(e). The "appropriate person" is the person to whom the information in question relates, except that if the affairs of that person are being dealt with under a power of attorney, by a controller appointed under art 101 of the Mental Health (Northern Ireland) Order 1986, by a Scottish mental health custodian (a guardian or other person entitled to act on behalf of the person under the Adults with Incapacity (Scotland) Act 2000), by a mental health appointee (a person directed or authorised as mentioned in r 38(1)(a) of Order 109 of the Rules of the Supreme Court (Northern Ireland) 1980 or a controller ad interim under r 38(1)(a) of the same), where the appropriate person is the attorney, controller, custodian or appointee, or where the affairs of that person are being dealt with under a power of attorney, the person to whom the information relates: Social Security Administration Act 1992, s 123(10). Where the person to whom the information relates lacks capacity, within the meaning of the Mental Capacity Act 2005, to consent to its disclosure, the appropriate person is a donee or an enduring power of attorney or lasting power of attorney, or a deputy appointed for him or her, or any other person authorised, by the Court of Protection, with power in that respect: Social Security Administration Act 1992, s 123(11).

[16] See, generally, Consultation Paper paras 4.34 to 4.59 and in particular para 4.44.

[17] Examples include consultation response no. 55 – Office for National Statistics at paras 5.8 and 5.15 and consultation response no. 79 – Karen Thompson at p 4. Implied powers are, however widely used as evidence by the Department for Work and Pensions and others, as indicated in consultation response no. 83 – Department of Education, which gave section 27 of the Children Act 1989 as an example of a duty to cooperate in the performance of a function being understood to imply a legal basis for data sharing.

[18] This was a common theme raised in consultation meetings, including consultation meetings no. 24 – Northumbria University and no. 27 – Birmingham City Council.

acknowledged by an individual, they would have reasonable cause to believe otherwise and would not be protected by the defence in the event they turned out to be wrong. Express gateways help to avoid the limitations of the defence in the face of uncertainty, by reducing that uncertainty.

9.13 There are a great variety of gateways, from very broad powers to exceedingly narrow ones. The development of the statutory framework also reflects an ad hoc approach.

EXAMPLES OF DEPARTMENT FOR WORK AND PENSIONS' GATEWAYS

Welfare Reform Act 2012, section 127: a broad gateway

9.14 Section 127 of the Welfare Reform Act 2012 provides a very broad information disclosure power for the transfer of information between the Department for Work and Pensions and HMRC.

9.15 The power was not commented on during readings of the Bill in the House of Commons, and the only discussion at Committee stage concerned a proposed amendment to introduce the possibility of using or adapting information sharing systems to inform policy on the living wage.[19] There are several other examples of data sharing powers that have passed through the Parliamentary process with little or no debate.[20] This raises a general point about the practice of providing express gateways in Acts of Parliament on an ad hoc basis. Such powers sometimes struggle to attract attention because the substance of the proposed reform rightly attracts the majority of concern in Parliament.[21] This can mean that information sharing provisions in Bills or subordinate legislation are under-scrutinised. A full project would need to consider the means by which new data sharing arrangements or powers are subjected to scrutiny.

9.16 Section 127 of the Act provides that information held for the purposes of any HMRC functions by HMRC or a person providing services to HMRC may be supplied to the Department or a person providing services to the Department for use for the purposes of functions relating to social security, employment or training, the investigation or prosecution of offences relating to tax credits, or child support.[22] It also provides that information held by the Department, or by a person providing services to the Department, for those purposes may be supplied to HMRC or a person providing services to HMRC for use for the purposes of HMRC functions.[23] HMRC functions are defined as any function for which the Revenue and Customs Commissioners are responsible by virtue of section 5 of

[19] See *Hansard* (HC), 19 May 2011, vol 528, col 1037.

[20] For example, information sharing orders under the Statistics and Registration Service Act 2007.

[21] The Welfare Reform Act 2012 made substantial changes to the social security system which remain the topic of political debate and controversy.

[22] Functions relating to social security include functions relating to statutory payments as defined in s 4C(11) of the Social Security Contributions and Benefits Act 1992, maternity allowance under s 35 of the Social Security Contributions and Benefits Act 1992, statutory payments as defined in s 4C(11) of the Social Security Contributions and Benefits (Northern Ireland) Act 1992, and the maternity allowance under s 35 of the Social Security Contributions and Benefits (Northern Ireland) Act 1992: Welfare Reform Act 2012, s 127(8); Welfare Reform Act 2012, s 127(1), (2) and (7).

[23] Welfare Reform Act 2012, s 127(3), (4) and (7).

the Commissioners for Revenue and Customs Act 2005 or which relates to a matter listed in schedule 1 to that Act.[24]

9.17 Where information supplied under the section has been used for the purposes for which it was supplied, it is lawful for it to be used for any purposes for which information held for those purposes could be used.[25] The section contains a control on onward disclosure. Section 127(5) provides that information supplied under the section must not be supplied by the recipient of the information to any other person or body without the authority of the Commissioners for Her Majesty's Revenue and Customs, in the case of information supplied by HMRC under section 127(2), or the authority of the Secretary of State, in the case of information supplied by the Department under section 127(4).[26]

9.18 Further provisions of the Welfare Reform Act 2012 permit information sharing between the Department and other bodies. Section 128 permits the Department and those providing services to it to disclose information, held for the purposes of the Department's functions relating to social security or child support, to prosecution authorities for purposes connected with criminal proceedings. Onward disclosure of information relating to a particular person, except for statutorily prescribed purposes, is an offence punishable by a fine, up to two years' imprisonment, or both.[27]

9.19 Section 131 permits the Department or a person providing services to it to supply information relating to social security benefits and certain welfare services to a local authority or to a provider to a local authority of services connected with welfare services, housing benefit or council tax. Onward disclosure of information relating to an individual received under section 131 is an offence unless the disclosure is made with lawful authority within the meaning of section 123 of the Social Security Administration Act 1992.

Powers that remain necessary despite the breadth of section 127

9.20 Despite the broad nature of section 127, a number of other powers remain on the statute book to facilitate information sharing between HMRC and the Department where the information disclosure falls outside section 127, either because the particular type of information is not covered by section 127 or because the powers contain mandatory elements not reflected in the permissive section 127. The Welfare Reform Act 2012 repealed some powers that existed before 2012 and which it rendered obsolete.

Social Security Administration Act 1992, section 121F

9.21 Section 121F of the Social Security Administration Act 1992 is still in force and was not repealed by the Welfare Reform Act 2012. It provides that information which is held by the Department, or a person providing services to the Department, for the purposes of functions relating to war pensions, may, and must if an officer of HMRC authorised by HMRC for the purposes of the section

[24] Welfare Reform Act 2012, s 127(7).

[25] Welfare Reform Act 2012, s 127(6).

[26] Welfare Reform Act 2012, s 127(5).

[27] Welfare Reform Act 2012, s 129.

so requires, be supplied to HMRC or a person providing services to HMRC for use for the purposes of functions relating to contributions, health in pregnancy grant, statutory sick pay or statutory maternity pay, or functions under Part 3 of the Pensions Act.

9.22 Information relating to war pensions is not within the scope of sections 127(4) and 127(8). Two significant differences apply to war pension information. First, the power in section 121F only extends to the supply of such information to HMRC for defined purposes, and not for HMRC's functions as a whole. Secondly, the power is an example of a generally permissive gateway that is mandatory when certain conditions are fulfilled. The permissive gateway in section 121F becomes mandatory where an authorised officer requires information, as there is a duty to supply information in those circumstances.

Tax Credits Act 2002, section 59 and schedule 5 paragraph 6

9.23 Section 59 of the Tax Credits Act 2002 gives effect to schedule 5 of the Act. Schedule 5 paragraph 6, which provides that information held for the purposes of functions relating to war pensions, as defined by section 25(4) of the Social Security Act 1989,[28] or for the purposes of employment and training by the Department or a person providing services to the Department, may be supplied to HMRC or a person providing services to HMRC, for use for the purposes of functions relating to tax credits, child benefit or guardian's allowance.[29] HMRC may require the information to be so supplied if the information is held for the purposes of functions relating to child support.[30]

9.24 Similarly, this provision contains a mandatory gateway element in relation to war pension and employment and training information, if held in relation to child support. There is some overlap between this permissive gateway and section 127, as employment and training information can be disclosed to HMRC for all of its functions on a permissive basis. However, this enables employment and training information held for child support purposes to be subject to the mandatory gateway of HMRC for use for the purposes of functions relating to tax credits, child benefit or guardian's allowance.

Child Trust Funds Act 2004, section 17

9.25 Section 17(4) of the Child Trust Funds Act 2004 provides that information held by the Department, or any person providing services, may be supplied to HMRC or a person providing services to HMRC, for use for the purposes of, or for any purposes connected with, the exercise of any function of HMRC relating to child trust funds. The power covers a type of information not included in section 127 of the Welfare Reform Act 2012 and allows it to be shared subject to a more restrictive purpose limitation. The purposes listed serve to limit the scope of the power to share.

[28] Tax Credits Act 2002, sch 5(6)(iv).

[29] Tax Credits Act 2002, sch 5(6)(i) and (ii).

[30] Tax Credits Act 2002, sch 5(6)(iii).

STATUTORY DEBRIS

9.26 Statutory gateways also reflect the ad hoc and contingent nature of their development where powers have not been used, are under-utilised or are sometimes simply never brought into force.

Powers in primary legislation not currently used

Serious Crime Act 2007, section 68

9.27 Section 68 of the Serious Crime Act 2007[31] provides that a public authority may, for the purposes of preventing fraud or a particular kind of fraud, disclose information, of any kind, as a member of a specific anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation, to specified anti-fraud organisations,[32] members of such organisations and any other people to whom disclosure is permitted under the arrangements concerned.[33] Section 68(3) provides that disclosure under the section does not contravene any obligation of confidence or any other restriction on the disclosure of information, however imposed,[34] although it provides that nothing in the section authorises any disclosure of information which contravenes the Data Protection Act 1998 or is prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000.[35] The provision also provides that nothing in the section authorises a public authority which has functions which are exercisable within devolved competence, as defined by section 54 of the Scotland Act 1998, to disclose information whose subject-matter is a matter about which provision would be within the legislative competence of the Scottish Parliament if it were included in an Act of that Parliament.[36] The section also clarifies that it does not limit the circumstances in which information may be disclosed apart from the section.[37]

9.28 However, there are not currently any data sharing arrangements between the Department and anti-fraud organisations in force under this section. This means that although there is a power to share, it is not used in practice.

Education Act 2005, section 108

9.29 Section 108 of the Education Act 2005 is an example of an existing power to disclose data which was created for the purpose of a particular project at a particular time and is noticeably out of date in relation to England. It provides that information held by the Department, or a person providing services to it, for the purposes of functions relating to social security may be supplied to listed

[31] This is also discussed in ch 8 above.

[32] Such organisations are specified in Serious Crime Act 2007 (Specified Anti-Fraud Organisations) Order 2008, SI 2008 No 2353. They are CIFAS, Experian Limited, Insurance Fraud Investigators Group, N Hunter Limited; The Insurance Fraud Bureau, and The Telecommunications United Kingdom Fraud Forum Limited.

[33] This section is also discussed in ch 8 above. Serious Crime Act 2007, s 68(1) to (2).

[34] Serious Crime Act 2007, s 68(3).

[35] Serious Crime Act 2007, s 68(4).

[36] Serious Crime Act 2007, s 68(5) to (6). Note that these provisions are pending repeal at a date to be appointed: Criminal Justice and Licensing (Scotland) Act 2010 (Scottish Act), s 98.

[37] Serious Crime Act 2007, s 68(7).

persons[38] for use for purposes relating to eligibility for education maintenance allowances.

9.30 The power was created to support Educational Maintenance Allowance, which no longer exists in England, although it has been retained by devolved authorities. The continuing existence and application of the power in England does no harm. If there is no eligibility to receive Educational Maintenance Allowance, information cannot be shared relating to that eligibility, save perhaps for address information as geographical location determines eligibility and it may be necessary to establish that an individual is ineligible because they in fact live in England. Importantly, the scope of the section in relation to England is much reduced by the removal of the benefit to which it relates and reflects the limits of an ad hoc legislative approach to data sharing power.

Powers to make subordinate legislation not currently used

Children Act 2004, section 12

9.31 The Secretary of State for Education has powers to make regulations requiring the creation of databases. Like HMRC, the Department also listed section 12 of the Children Act 2004 in discussions with us. This section provides that the Secretary of State may, for the purpose of arrangements under section 10 and 11 of the Children Act 2004 or under section 175 of the Education Act 2002, by regulations require local authorities in England to establish or operate databases containing information in respect of persons to whom such arrangements relate, or himself establish and operate or make arrangements for the operation and establishment of one or more databases containing such information.[39] The section provides that the Secretary of State may make provision in relation to the establishment and operation by regulations of any databases under the section.[40] The power in the Children Act 2004 is not currently being exercised and there are no regulations under it in force. [41]

9.32 The purpose of the section was originally to make provision for the "ContactPoint" database and it remains on the statute book even after the decommissioning and destruction of that database. Section 12 is an example of the statutory debris of past information sharing initiatives which remain in the statute book long after the project that gave rise to them expired. Such powers are available for use in the future, but do not lend themselves to the coherent and principled development of the statutory scheme.[42]

[38] The Secretary of State, the Chief Executive of Skills Funding, the Assembly, a Northern Ireland Department, the Scottish Ministers, and any person providing services to those persons: Education Act 2005, s 108(3).

[39] Children Act 2004, s 12(1).

[40] Children Act 2004, s 12(5).

[41] See Explanatory Note to the Children Act 2004 Information Database (England) (Revocation) Regulations 2012, SI 2012 No 1278. The note explains that the "ContactPoint" database established and operated under this power was closed down on 6th August 2010 and the data it contained destroyed.

[42] See paras 8.53 to 8.56 above.

Not yet in force/never commenced

Tribunals, Courts and Enforcement Act 2007, section 97

9.33 Some powers to share data reach the statute book but are never in fact commenced. For example, section 97 of the Tribunals, Courts and Enforcement Act 2007 provides for information requests by courts for the disclosure of information relating to the full name, address, date of birth, and national insurance number of, and other prescribed information about, a debtor from (as was intended) the Department. However, the provision has never been brought into force and by a Written Ministerial Statement on 17 March 2009 the Government announced, following a reassessment of the Act to ensure that the enforcement provisions remained appropriate, that it would not be bringing the provision into effect and would instead commence a consultation exercise with a view to implementing changes.[43]

Other difficulties with the ad hoc development of the legislative scheme

Future proofing the legislative scheme

PENSIONS ACT 2008, SECTION 142 AND DISCLOSURE OF STATE PENSION CREDIT INFORMATION (WARM HOME DISCOUNT) REGULATIONS

9.34 Section 142 of the Pensions Act 2004 and regulations made under it set up arrangements for information disclosure in relation to the energy rebate scheme.[44] New regulations will be needed for any replacement scheme. It is a good example of the difficulty of future-proofing the statutory framework to control appropriate sharing without repeated changes to that framework. The need for replacement regulations can cause problems when addressing energy poverty.

Acts of Parliament dedicated to information disclosure

9.35 Another feature of the ad hoc development of the statutory scheme for data sharing is that sometimes not merely legislative intervention to create a clear and express statutory gateway is required, but entire Acts of Parliament have been required to facilitate certain sharing arrangements. There is a real question over whether this is an effective use of Parliamentary time, although undoubtedly scrutiny is much improved. Two examples are the Television Licences (Disclosure of Information) Act 2000 and the Digital Switchover (Disclosure of Information) Act 2007. A full reform project may need to consider how to address needs for unforeseen data sharing powers created by changes during policy development.

OTHER FEATURES OF THE DEPARTMENT'S STATUTORY POWERS

9.36 This section contains a discussion of provisions that concern the Department and illustrate the themes and considerations that an analysis of gateways can direct one towards.

The power to charge fees: the micro-economics of statutory gateways

9.37 One general problem we heard about during consultation was that permissive

[43] *Hansard* (HC), 17 March 2009, vol 489, col 46WS.

[44] https://www.gov.uk/the-warm-home-discount-scheme (last visited 1 July 2014).

gateways sometimes fail to reflect the micro-economics of data sharing. For example, the body holding information that it is free to disclose through a permissive gateway may reasonably choose not to use the power. This can happen because the legal risk and the practical and transactions costs would fall on the disclosing body while the benefits of the disclosure would pass entirely to the recipient of the information or an individual in relation to whom the recipient body, rather than the disclosing body, has statutory functions or owes duties. This means that although the public good, or the individual about whom information is held, ultimately stands to benefit from the disclosure, the disclosure does not occur. A full Law Commission project should consider what mechanisms might help to tackle problems that arise from the micro-economics of the data sharing relationship.

9.38 One example of such a mechanism can be found in the Department's statutory framework. Section 122C(4) of the Social Security Administration Act 1992 provides that the Secretary of State may impose conditions on the use of information supplied under section 122C(2) and may charge a reasonable fee in respect of the cost of supplying information under that subsection. This power has the potential to redistribute the transaction costs of data sharing in favour of more efficient outcomes, by requiring the recipient body to bear the cost of supplying the information they wish to receive.

9.39 It should be noted that a power to charge a fee may also necessitate a power (and a budget) to enable recipient bodies to make use of such an arrangement. For example, in consultation Defra observed that the business models of some of its executive agencies do not permit the payment of fees to receive information, which hinders sharing.[45]

Duties to cooperate

9.40 In consultation, the idea of using duties to cooperate to encourage effective data sharing arrangements was well received. In particular, some officials observed that for any gateway to operate effectively there must be cooperation, and that appropriate and effective sharing is more likely where proper cooperative relationships are in place. This reflects a consistent theme from the consultation: the importance of relationships in negotiating information disclosure.[46] In a full project, the Law Commissions should consider the extent to which duties to cooperate could improve data sharing and the disadvantages of using duties to cooperate.

9.41 An example of a duty to cooperate can be found in section 325 of the Criminal Justice Act 2003. Section 325 provides that in establishing arrangements for the purpose of assessing and managing the risks posed in an area by sexual and violent offenders, as defined by section 327 of the Act, and other persons who, by reason of offences committed by them (wherever committed), are considered by the responsible authority to be persons who may cause serious harm to the public, the responsible authority must act in cooperation with listed persons,

[45] This point was made by Defra generally and not in relation to the Department for Work and Pensions. Consultation response no. 62 – Defra.

[46] Consultation meeting no. 7 – Amberhawk Conference; consultation meeting no. 12 – Dr Rob Wilson and Professor Mike Martin.

including the Department,[47] and it is the duty of those persons to co-operate in the establishment of those arrangements, to the extent that such co-operation is compatible with the exercise by those persons of their relevant functions.[48] This co-operation expressly includes the exchange of information.[49] Those persons and the authority are under a duty to draw up a memorandum setting out the ways in which they are to cooperate.[50] The Secretary of State has a power to amend the list by order to add or remove any person or description of persons.[51] The Secretary of State has a power to issue guidance on the discharge of the functions conferred by section 325[52] and the responsible authorities must have regard to any such guidance in discharging their functions under the section.[53]

Limitations on use

Education and Skills Act 2008, section 87

9.42 Section 87 of the Education and Skills Act 2008 provides that information about an individual who has attained the age of 19 which is held by the Secretary of State for the purposes of any functions relating to social security or is held by the Secretary of State or a devolved authority and relates to any training or course of education undertaken by the individual, whether before or after the individual attained the age of 19, may be used in connection with the exercise of an assessment function of the Secretary of State or a devolved authority or disclosed to a person for use in connection with the exercise of an assessment function of the Secretary of State or a devolved authority.[54] An assessment function is a function evaluating the effectiveness of training or education provided for persons who have attained the age of 19, assessing policy in relation to the provision of such training or education, assessing policy in relation to social security or employment as it affects the provision of or participation in such

[47] The list comprises every youth offending team established for an area any part of which falls within the relevant area; the Ministers of the Crown exercising functions in relation to social security, child support, war pensions, employment and training; every local authority acting in the exercise of its relevant functions any part of whose area falls within the relevant area; every local housing authority any part of whose area falls within the relevant area; every local authority (in its capacity as a person exercising functions for the purposes of the health service) any part of whose area falls within the relevant area; every private registered provider of social housing or registered social landlord which provides or manages residential accommodation in the relevant area in which relevant sexual or violent offenders and others reside or may reside; every Health Authority any of whose area falls within the relevant area; every person who is designated by the Secretary of State by order for the purposes of this paragraph as a provider of electronic monitoring services; persons listed in UK Borders Act 2007, s 48(1A)(a) to (e) and any person acting pursuant to arrangements relating to the discharge of a function within s 48(1A) of that Act: Criminal Justice Act 2003, s 325(6).

[48] Criminal Justice Act 2003, s 325(1) to (3).

[49] Criminal Justice Act 2003, s 325(4).

[50] Criminal Justice Act 2003, s 325(5).

[51] Criminal Justice Act 2003, s 325(7).

[52] Criminal Justice Act 2003, s 325(8).

[53] Criminal Justice Act 2003, s 325(9).

[54] Education and Skills Act 2008, ss 87(1) to (3).

training or education.[55]

9.43 Section 89 addresses the use of information disclosed in reliance on section 87(1)(a). It provides that information so disclosed may be used by the person to whom it is disclosed only in connection with the exercise of an assessment function and, so far as is reasonably practicable, the information must not be used in such a way that the identity of the individual is disclosed to, or capable of being disclosed by, a person carrying out an evaluation or assessment of a kind mentioned in section 87(4)(a) to (c) of the Act. The provision therefore places limits on the ways in which information may be used, including a requirement to preserve anonymity, not absolutely, but so far as reasonably practicable.

9.44 Information disclosed in reliance on section 87(1)(a) is also protected by a wrongful onward disclosure offence.[56] It is an offence to disclose information to another otherwise than in connection with the exercise of an assessment function of the Secretary of State or a devolved authority if information relates to a person whose identity is specified in or can be deduced from the disclosure.[57] It is a defence that a person charged with the offence reasonably believed that the disclosure was lawful or that the information had already and lawfully been made available to the public.[58] The offence is punishable by up to two years' imprisonment, a fine or both and prosecution for an offence under the section may be instituted in England and Wales only with the consent of the Director of Public Prosecutions.[59]

Powers to make regulations

9.45 Many of the Department's gateways derive from statutory powers of the Secretary of State, and in some cases other officials,[60] to make regulations to permit information disclosure.[61] For example, the Welfare Reform Act 1999 contains wide regulation making powers. A large proportion of the Department's powers are therefore contained in secondary legislation that must be read in light of the provisions in, and the scheme of, the primary legislation. This adds to the complexity of comprehending the powers available.[62] A full Law Commission project would need to consider the benefits and disadvantages of heavy reliance on regulation making powers concerning data sharing between public bodies more generally.

[55] Education and Skills Act 2008, s 87(4).

[56] Education and Skills Act 2008, s 90(1)(a).

[57] Education and Skills Act 2008, s 90(2).

[58] Education and Skills Act 2008, s 90(3).

[59] Education and Skills Act 2008, s 90(4) and (5).

[60] For example, the Registrar General: Social Security Administration Act 1992, ss 124 and 124A.

[61] See, for example, Social Security Administration Act 1992, ss 5(1A) and 125; Pensions Schemes Act 1993, s 45B; Welfare Reform and Pensions Act 1999, s 72; Pensions Act 2004, ss 61, 190, 203; Education Act 2005, s 114; Pensions Act 2008, s 142; Welfare Reform Act 2009, s 41(4).

[62] A good example is s 124A of the Social Security Administration Act 1992, which provides that registrations made by the Registrar General under s 36 of the Civil Partnership Act 2004 may provide for the furnishing of certain information in relation to civil partnerships.

A power triggered by the consent of the individual concerned

Vehicle Excise and Registration Act 1994 and Road Vehicles (Registration and Licensing) (Amendment) (No.2) Regulations 2005, SI 2005 No 2713

9.46 Section 22ZA of the Vehicle Excise and Registration Act 1994 provides that information to which the section applies,[63] may, if the consent condition is satisfied, be supplied to the Secretary of State or to a person providing services to the Secretary of State for use for the purposes of relevant licence functions.[64] The relevant licence functions are the application and issue of licences for registered vehicles and other certain exempt vehicle nil licences in relation to the receipt of certain disability benefits.[65]

9.47 The consent condition is that the person who provided the information, if the information was provided by a person other than the data subject, or in any other case the person to whom the information relates has consented to the supply of the information and has not withdrawn that consent.[66] This is a puzzling provision on its face. It raises the question of to what extent consent provisions should be apparent on the face of statutory powers.[67]

9.48 The provision also has a control on onward disclosure. Section 22ZA(4) provides that information supplied under section 22ZA(2) shall not be supplied by the recipient to any other person unless it could be supplied to that person under section 22ZA or it is supplied for the purposes of any civil or criminal proceedings relating to the Act and shall not be used otherwise than for the purposes of relevant licence functions[68] or any such proceedings.

Obsolete provisions that are present due to constitutional convention

9.49 In consultation, it was suggested to us that some express statutory gateways are required, not because they are legally necessary, but because there is a desire to improve the legitimacy of a disclosure arrangement by securing Parliamentary approval. Although this is not a true constitutional convention, it shows that considerations of constitutional propriety can influence the proliferation of data sharing gateways.

[63] See Vehicle Excise and Registration Act 1994, s 22ZA(1) to (1B) and Road Vehicles (Registration and Licensing) Regulations 2002, SI 2001 No 2742, reg 33(8A) and (8B): s 22ZA applies to information of the following descriptions: the name of any person whom disability living allowance or mobility supplement is payable or disability living allowance has ceased to be payable and who would be entitled to receive the mobility component at the higher rate but for his failure to satisfy a condition referred to in sch 2(19)(2A)(b) of the Act.

[64] Vehicle Excise and Registration Act 1994, s 22ZA(2).

[65] Vehicle Excise and Registration Act 1994, s 22ZA(5).

[66] Vehicle Excise and Registration Act 1994, s 22ZA(3).

[67] We note that the consent of the person to whom information relates is a disclosure made with lawful authority for the purposes of Social Security Administration Act 1992, s 123(9)(e).

[68] Functions relating to applications for, and the issue of, vehicle licences in respect of vehicles to which para 1ZA of sch 1 applies, and nil licences in respect of vehicles that are exempt vehicles under paragraph 19 of sch 2 or para 7 of sch 4: Vehicle Excise and Registration Act 1994, s 22ZA(5).

9.50 A full Law Commission project would need to be aware of the constitutional propriety of any proposed framework for sharing, especially given that some aspects of the proliferation of gateways have been a response to such concerns.

CONCLUSIONS

9.51 Our examination of the Department's information disclosure legislation has added to our picture of the variety of issues that could usefully be addressed in a law reform project. A notable feature of the Department, in the present context, is the extent to which its activities overlap or are inter-related with some of the activities of HMRC and local authorities, leading to extensive data sharing between them and the Department. A similar picture of inter-related activities leading to information sharing will no doubt emerge from a full examination of other sectors, including the healthcare sector.

CHAPTER 10
THE TROUBLED FAMILIES PROGRAMME

INTRODUCTION

10.1 In this Chapter, we present the data sharing issues raised by the Department for Communities and Local Government in relation to its Troubled Families Programme. Unlike to two preceding chapters, which look at the statutory framework surrounding data sharing by HMRC and the Department for Work and Pensions, Chapter 10 produces information about the particular legal issues that were experienced in the delivery of a recent government policy that is dependent on data sharing for its effective implementation.

ISSUES RAISED IN CONSULTATION

10.2 A large number of consultees, both in meetings and written responses, discussed the Troubled Families programme led by the Department for Communities and Local Government (DCLG).[1] It is a striking illustration of the problems that can arise in projects that rely heavily on data sharing.

10.3 Underlying the project is the estimate that 120,000 troubled families cost the taxpayer £9 billion annually – £75,000 per family per year – of which £8 billion are spent purely in reacting to the families' problems, rather than improving their outcomes. The first phase of the programme sought to identity target families using four cumulative criteria: high levels of anti-social behaviour or youth crime, children excluded from or not attending school, adults claiming out-of-work benefits and a fourth criterion set by local authorities based on "local intelligence" as to the most significant problems in their localities.

10.4 The data necessary for this exercise are held across a multiplicity of different local and central public sector agencies. A corresponding multiplicity of different data sharing agreements were required with different parts of government. The process was complex, produced patchy results and incurred high transaction costs. Some data sharing was not possible, such as identifying families with priority health problems, as no legal gateway could be found or devised.

10.5 Applying the crime/anti-social behaviour criterion relied on section 115(1) of the Crime and Disorder Act 1998, which provides a general power to disclose information to a relevant authority "where the disclosure is necessary or expedient for the purposes of any provision of this Act". In late 2012 this was challenged by the Police and the Information Commissioner's Office on the grounds that the legislation was only intended to permit sharing of information on a case-by-case basis rather than a 'bulk' transfer. In early 2013, the applicability of section 115 to this aspect of the Troubled Families Project was endorsed by the Home Office, the Association of Chief Police Officers and the Information Commissioner's Office in a guidance note to the police service, but all acknowledged the legal risks.[2]

[1] Consultation response no. 81 – Department for Communities and Local Government.

[2] Consultation response no. 81 – Department for Communities and Local Government.

10.6 The collection of information about school exclusion and truancy relied on section 17 of the Children Act 1989 as an implied legal gateway. Section 17 creates a general duty of every local authority to promote the welfare of children in need within their area and the upbringing of such children by their families. For this purpose children are in need if, among other things, their intellectual, social or behavioural development is likely to be impaired if the services are not provided. The section does not create any express information-gathering power. Some schools in the local authority areas, particularly Academies, challenged the existence of an implied power under this section to collect information for the purposes of identifying families for the Troubled Families programme; this was said not to be consistent with the legislative intention and not compliant with the wider expectations about data sharing communicated by the Department for Education.

10.7 For the purposes of the out-of-work benefits criterion it was necessary for Regulations to be made under the Welfare Reform Act 2012, to empower the Department for Work and Pensions (DWP) and Jobcentre Plus to supply benefits information to local authorities. Further amendments were required in 2013 to enable the local authorities in turn to share information provided by DWP with the third parties that were supporting the delivery of the programme, as well as to enable the local authorities to continue to share data with DWP for the purposes of working with the families and of evaluating the impact of the project.[3]

10.8 Lawyers for DWP saw this as an illustration of the system working as it should, rather than indicating a problem. They favoured having the detailed boundaries of information sharing set out in subordinate rather than in primary legislation. They felt that this ensures a good balance in terms of proportionality (with the law permitting information sharing only where required), transparency (with the details clearly set out in published legislation), Parliamentary scrutiny (with Parliament itself looking at the main principle during passage of the primary legislation, and the Secondary Legislation Scrutiny Committee looking on Parliament's behalf at the detail in the subordinate legislation), and flexibility (with the details able to change relatively easily and speedily through subordinate legislation).

10.9 Housing benefit dependency was regarded as relevant to identifying benefit-dependent families. Housing benefit is administered by local authorities, who consequently hold data about claimants. Problems over local authorities' powers to share data with others involved in the project meant that a complex and expensive system of centralised data sharing through DWP had to be created at a cost of £400,000 to DWP, excluding local authority and DCLG transaction costs, which DCLG told us were expected to be substantial.

10.10 In setting their fourth criterion based on local intelligence, local authorities identified domestic violence, substance and alcohol abuse and mental health as the top three issues they wished to prioritise. There was no gateway empowering local GPs or drug and alcohol support providers to share the required data. The lack of one necessitated a complex and expensive process of seeking families' consent to access this information before a decision could be taken to offer support under the programme, something which DCLG described to us as

[3] Consultation response no. 81 – Department for Communities and Local Government.

disproportionately bureaucratic.

10.11 DCLG maintained that retaining a system of narrow gateways would add to the complexity of data sharing under the programme, which was due to be expanded in scale. It said that local authorities and public bodies would continue to need to consider multiple pieces of legislation and the common law, leading to significant delays, increased transaction costs and an inability to identify, support and improve outcomes for target families. DCLG proposed a "cross-cutting permissive gateway" in order to enable families to be identified against the range of criteria envisaged for the expanded phase of the programme, matched by greater safeguards to minimise the amount of data being accessed by local authorities in respect of families that did not end up on the programme. They suggested that a proportionate approach would be to ensure that the data to identify troubled families were processed by a third party in a depersonalised and indexed form and only re-personalised when an individual or family was found to meet the criteria for assistance under the programme.[4]

10.12 We report these suggestions without comment at this stage. It is acknowledged that data of the sort involved in the project, relating to matters such as criminality, anti-social behaviour, educational problems, benefit dependency and medical/drug dependency issues are data of a particularly sensitive kind. Reducing the cost to society of troubled families, as well as improving conditions for the troubled families themselves, are objectives in the public interest. A law reform project will need to take a careful course between facilitating the work of such projects, maintaining due regard for the citizen's interest in the confidentiality of the most highly sensitive data about them and protecting members of the target families from unnecessary dissemination of data about them within the communities in which they live.

CONCLUSIONS

10.13 These three case studies help to illustrate the complexity of the statutory framework, the features of a statutory framework that any reform project will have to consider and the problems associated with that complexity.

[4] Consultation response no. 81 – Department for Communities and Local Government.

PART 4
NEXT STEPS

CHAPTER 11
DEVELOPING SOLUTIONS

INTRODUCTION

11.1 Problems with data sharing between public bodies are both practical and legal. Some might also be described as cultural. Cultural problems can be created in part by the legal framework. The legal framework can also reflect, and may have to respond to or even attempt to change, the institutional norms operating in public bodies in relation to data sharing, or their understanding of the public good. Other aspects of the problems surrounding data sharing are better described as disincentives to share. All of these problems must be understood and reflected in any solution proposed for law reform. Law reform can play a part in addressing such problems.

CONSULTEES' SUPPORT FOR REFORM

11.2 Consultees expressed broad support for simplifying and clarifying the law relating to data sharing, although consultees also argued for change beyond law reform. Many proposals were made, which would be followed up in a full law reform project. What follows is a representative selection.

The Information Commissioner's Office

11.3 The Information Commissioner is a key stakeholder, with extensive experience of data sharing and data security issues. The Commissioner's Office suggested to us areas where law reform would be helpful, but was unconvinced that the law prevented forms of data sharing that were reasonable and in the public interest.

11.4 We have found examples of a lack of power to share information which public bodies regarded it as being in the public interest for them to receive.[1] We also perceive a problem that is not one of lack of power to share so much as disinclination to use the powers in circumstances where sharing might be desirable. We nevertheless agree that a full review would need to ensure an adequate evidence base for any proposed changes to the law.[2]

11.5 The Information Commissioner's Office also urged us to pay particular attention to the relationship between the Data Protection Act 1998 and other laws affecting data sharing. The Information Commissioner's Office considered that the data protection principles administered by it have all the necessary features to protect citizens' privacy and to provide a positive framework for organisations to share personal data in a fair and lawful way for a defined purpose. Although it understood the relevance of other elements of the law, it felt that a more prominent place for data protection law would help to simplify the legal

[1] See the discussion of the Troubled Families Project in ch 10.

[2] Consultation response no. 21 – Information Commissioner's Office.

landscape. It found the current system of establishing "gateways" confusing for practitioners.

11.6 The Information Commissioner's Office considered that a more principles-based approach might facilitate the imaginative and flexible use of personal data that policy makers would like to see and safeguard individual information rights. The Office suggested that a possible model might be to build on its statutory Data Sharing Code of Practice, it issued in 2011. Although accepting the need to update and review this guidance, the Information Commissioner's Office was confident that it could become a central source of authoritative guidance on data sharing and be used as source material for other organisations wishing to produce their own in-depth organisational or sector-specific guidance. The Office was not generally supportive of mandatory sharing, noting that there was arguably too much guidance in circulation, perhaps needing to be rationalised and made more coherent. The Office also saw possible scope for creating incentives for organisations to follow codes, for example as part of an accreditation scheme. The Information Commissioner's Office also proposed that its powers of compulsory audit should be extended to local government and the NHS, providing more effective regulation of data sharing in these sectors.

11.7 The Information Commissioner's Office also invited us to consider whether data sharing legislation should always contain specific safeguards for individuals or whether it is sufficient to rely on the safeguards in data protection law. It saw it as important that the "recipe" for data sharing standards, such as security, transparency, and privacy impact assessments, was broadly consistent and contained meaningful safeguards for individuals, especially in light of the different levels of sensitivity and privacy impact that different types of data might have.

Civil Society Groups

11.8 Civil society organisations have expressed a strong interest in the formation of law and policy in this area – one in which advocacy, lobby and pressure groups are active. These groups are independent from government and other public interests.

11.9 Liberty was very supportive of a full Law Commission project on data sharing, arguing that balancing competing rights and interests lies at the heart of acceptable data sharing. Liberty considered it essential that well thought out principles underpinned a clear and understandable legal framework, pointing to different approaches taken by the successive Governments and criticising what Liberty saw as a lack of analysis and communication following consultations and pilots. The consequent lack of debate and clarity was unacceptable to Liberty, which feared it would leave individual rights open to violation.[3]

11.10 Nick Pickles of Big Brother Watch argued in a consultation meeting that an individual's data should only be shared for the purpose of decisions relating directly to that person, such as assessing eligibility for a benefit or investigating a specific crime, and not for the general possibility of some future good.[4] He saw transparency as an important element in data sharing: Government should

[3] Consultation response no. 40 - Liberty.

[4] Consultation meeting no. 31 – Big Brother Watch.

publish (or inform the individuals concerned about) the nature and content of the data held, where the data was obtained, with whom it was shared and for what purpose. He saw a need for a clear set of principles, together with appropriate safeguards, which would be preferable to the current multitude of individual gateways. In particular, the system should be person-centred: you should be at the centre of decision-making about your data.[5]

11.11 In a meeting with Privacy International, the importance of the principle of informational self-determination was stressed as necessary for understanding and to avoid citizens being discouraged from participation in society.[6] There was a need for a principled approach.[7] Similarly, a meeting of Open Rights Group, Mydex, and MedConfidential representatives expressed concern that an organisation-centric approach prevailed over an individual-centric one. They pointed out that historically, individuals had more control over their own data. The key issues were personal control over information about oneself, individual agency and recognising the economic and other value of personal information.[8]

CONSULTEES' CONCERNS ABOUT LAW REFORM

11.12 A number of consultees warned about the proper scope of any full reform project.

Concerns about UK law

11.13 Some information lawyers referred to the limitations of a national law reform project in an area seen as driven by European Union law, but noted the existence of limited areas of discretion over the means by which the Directive is implemented – though the scope for flexibility will be much reduced if the draft European Union Regulation passes into law. Similarly, the effect of article 8 of the European Convention on Human Rights was seen as outside the scope of a national reform project. Information lawyers did, however, support the review and reform of the statutory gateways, which was considered to be an important and useful exercise.

Concerns from the health sector

11.14 The British Medical Association stressed the fundamental role of confidentiality in the relationship between professionals and their patients, allowing patients to divulge sensitive information without concern that it will be disclosed to others without their consent except in very limited and exceptional circumstances. The British Medical Association expressed serious concerns about any legislation similar to that originally proposed in the Coroners and Justice Bill 2009 which, as drafted, permitted an unprecedented level of sharing of confidential health data between government departments. It saw streamlined processes for sharing sensitive healthcare information as seriously threatening confidentiality, with implications for both the care of patients and the achievement of key public health

[5] Consultation meeting no. 31 – Big Brother Watch.

[6] Informational self-determination refers to the ability of an individual to determine how data about them is stored, used and disclosed.

[7] Consultation meeting no. 35 – Privacy International.

[8] Consultation meeting no. 32 – Open Rights Group, Privacy International, MyDex, MedConfidential.

aims if patients withheld information due to fears about confidentiality.[9]

11.15 The British Medical Association explained that the Health and Social Care Act 2012 had added a further layer to the legal framework governing the disclosure of confidential health information, and referred to a number of uncertainties surrounding the sharing of data for purposes other than direct care at a local level since the abolition of primary care trusts and the reorganisation of the National Health Service on 1 April 2013. It argued that any breach of confidentiality would result in significant damage to public trust, which was fundamental to the relationship between patients and doctors. The British Medical Association was also concerned that a future government might decide to link health information with information held by other government departments or might see the commercial value of such data and legislate to enable its release. It stressed that such an outcome would be wholly unacceptable and must remain prohibited by law.

11.16 The National Aids Trust raised concerns in relation to sensitive personal confidential data, especially health and drug use data, pointing to particular sensitivities in the context of HIV positive status, which is a stigmatised health condition affecting approximately 100,000 people in the UK. The Trust referred us to its recent report on HIV Patient Information and NHS Confidentiality. The report considers that the current system of controls on the secondary use of personal confidential data is appropriate, including the ability of individuals to opt out of any use of health data for secondary purposes, which, it pointed out, is in some instances not enshrined in law but is a policy decision or "gift". The Trust called for the ability to opt out of one's health data being deployed under statutory powers to be enshrined in law, subject to a high public interest threshold.[10]

11.17 The Trust also warned of the deterrent effect on access to healthcare were there to be a perception that one's personal information was centrally shared. For example, it said that sharing information on drug use with bodies in the criminal justice and benefits systems would be a public health disaster. It saw a strong public policy rationale for taking a minimal, precautionary and consensual approach to the sharing of health-related data, especially in the light of provisions of the International Covenant of Economic, Social and Cultural Rights, the European Charter of Fundamental Freedoms and the European Convention on Human Rights.

11.18 The Medical Protection Society argued for a comprehensive review, finding the current situation bewildering, confusing and difficult to comprehend. It said that doctors take their duty of confidentiality extremely seriously but the requirements placed on them have become ever more complex and difficult to apply in practice.[11]

11.19 The Royal College of Psychiatrists was particularly concerned about information sharing with commissioning bodies in the National Health Service. Although accepting the commissioning bodies' need for some information, the Royal

[9] Consultation response no. 22 – British Medical Association.

[10] Consultation response no. 34 – National AIDS Trust.

[11] Consultation response no. 44 – Medical Protection Society.

College saw no requirement for the level of detail and quantity of personal and sensitive information currently provided. Monitoring should, the Royal College suggested, be conducted through the use of SMART outcome measures[12] and not through sharing of clinical documents with significant amounts of clinical and sensitive information.[13]

11.20 Mind referred to the profound consequences for individuals of sharing information about their mental health status, treatment or care. Trust was important in the delivery of such healthcare, creating need for more practical training and implementation and more accessible means of redress for individuals in the case of breaches.[14]

11.21 Karen Thompson, Head of Information Governance at NHS England (responding in a personal capacity and not representing the views of her employer) thought it helpful to give consideration to codifying the common law duty of confidence, at least in respect of the duty owed in the context of health and social care by professionals and the organisations within which they work. She gave the example of the codification of the common law in respect of mental capacity, finding that the legislation and extensive code of practice that resulted has improved practice in that area.[15]

Child safeguarding

11.22 Another important and highly sensitive area for data sharing is child safeguarding. The NSPCC told us that effective information sharing could not be driven by the law alone, but should be factored into legal, professional and organisational arrangements. Professionals who work with children must have clear instructions, both in law and guidance, and have regular training to develop cross-professional understanding. Professionals must not fear the consequences of inappropriate but well-intentioned sharing. Serious care reviews often discuss instances where different organisations held many separate pieces of disparate information raising low levels of concern, which if seen together would have pointed to a more serious issue that required immediate action.[16]

11.23 Although professionals have some understanding of information sharing laws in their specific areas, they do not necessarily understand the law and practice of other professionals. Current law and guidance fails adequately to provide solutions to the tensions that arise between different services. The NSPCC expressed particular concern in relation to the impact of the decision in *R (AB and CD) v Haringey London Borough Council* on data sharing for early

[12] SMART measures are those that are specific, measurable, attainable, realistic and timely.

[13] Consultation response no. 46 – Royal College of Psychiatrists.

[14] Consultation response no. 71 – Mind.

[15] Consultation response no. 79 – Karen Thompson.

[16] Consultation response no. 28 – NSPCC.

prevention.[17] The NSPCC invited us to consider whether the various guidance documents properly reflect the law and assist practitioners to understand it.

11.24 The Office of the Children's Commissioner also supported a review of all the statutory gateways relating to individual data sources to enable a rationalisation of legislation or guidance as necessary, seeing a need for nationally and locally agreed information sharing protocols.[18]

OTHER CONSIDERATIONS

11.25 Linda Damerell saw public bodies' increasing reliance on external service providers as requiring greater transparency about the ways that data are used. Transparent information on outcomes was required to empower local people to see what is working well so that best practice can be shared. There was a concern that a "data divide" will otherwise become entrenched.[19]

11.26 Birmingham City Council saw the operational model of Councils and other public authorities as moving away from being a service provider to more of a commissioning body role, often procuring services in conjunction with other organisations. This increased the sharing of personal data beyond the control of the Council, with consequently increasingly complex data governance arrangements. As more innovative solutions were found, there would be increasingly more complex governance structures required, and potentially greater risks for privacy.[20]

11.27 Hazel Grant, in addition to organising and hosting a consultation meeting which became the response of the Society for Computers and Law, also suggested in a separate meeting that other models for addressing data security breaches that we might look at included those in Nordic countries, which – in contrast to the fines, audits and prosecutions in most European states – have a consultative phase followed by a published decision containing a risk matrix and recommendations based upon it.[21]

11.28 As discussed above, the system of monetary penalties under the Data Protection Act 1998 could form part of the review of data sharing.[22]

Caldicott Review requests to the Law Commission

11.29 In her report, *Information: To share or not to share? The Information Governance Review (Caldicott 2)*, Dame Fiona Caldicott recommended that the Law Commission look at how the law surrounding deceased persons might be better

[17] *R (AB and CD) v Haringey Borough Council* [2013] EWCA 416 (Admin); [2013] Fam Law 965. Parents successfully sought judicial review of the local authority's decision to conduct an enquiry under the Children's Act 1989, s 47 to enable the local authority to decide whether it should take action to safeguard and promote the welfare of the child. The High Court found that the local authority had failed to make a proper decision precedent to engaging their duty under s 47. The decision to conduct a s 47 inquiry was quashed.

[18] Consultation response no. 23 – Senior Traffic Commissioner.

[19] Consultation response no. 11 – Tapestry Innovation Ltd, Linda Damerell.

[20] Consultation response no. 69 – Birmingham City Council.

[21] Consultation meeting no. 15 – Hazel Grant, Bristows.

[22] Monetary penalties are discussed in ch 1 above.

harmonised and recommended removing the legal impediments to giving custodianship of individuals' health and social care data within their last will and testament, either to another individual or to a research databank. [23]

11.30 This recommendation raises important questions and as information technology, genetic and medical science develop, there may be increasing demands for information to be made available after a person's death and, conversely, for a person to seek to protect their information from disclosure after death.

11.31 Our recommended law reform project would look at the disclosure of information held for public purposes by public bodies (or those delivering public services) to other public bodies (or those delivering public services). The questions raised in the Caldicott II Reoprt are not focussed on the sharing of information between such bodies, but on a person's ability to have some control over decisions made after their death over information not amounting to intellectual property. They are, it seems to us, outside the scope of the project that we are contemplating.

Multi-agency safeguarding projects

11.32 During consultation, we were informed of the challenges and good practice developing in Multi-agency Safeguarding Hubs. Following cases where deaths of children occurred in circumstances where there had been inadequate information sharing between local organisations working with the family, local authorities now tend to have multi agency safeguarding teams in order to identify risk more accurately and at an earlier stage.[24]

11.33 A project called Improving Information Sharing and Management was developed by Bradford Metropolitan District Council, Leicestershire County Council and the 10 local authorities in Greater Manchester in order to do just that, with toolkits, guidance and training for other local authorities. The project ran from the beginning of 2012 through the summer of 2013, supported by the Department for Communities and Local Government, the Local Government Association, the Information Commissioner's Office and others. An Information Sharing Centre of Excellence is now in development to provide practical support to those making decisions on the disclosure of information in the public sector.

11.34 During the consultation period we visited Leicestershire County Council, where we were hosted by representatives of the Public Service Transformation Network.[25] In Leicester, the multi-agency information sharing hub has developed simple ways of displaying complex information from multiple sources about complex family situations so that appropriate front line staff could make effective use of that information before children reached the point where a safeguarding decision had to be made.

11.35 Like the Caldicott Reviews, the Information Sharing Centre of Excellence is an example of the work which can be done to improve data sharing within the

[23] F Caldicott, Information: to share or not to share? The Information Governance Review (March 2013) at https://www.gov.uk/government/publications/the-information-governance-review (last visited 1 July 2014).

[24] See for example, Lord Laming, *The Protection of Children in England: A Progress Report* (2009) HC 330.

current law. There are lessons to be learned from these organisations in terms of the principles and concerns being applied in these areas, which could be integrated more clearly into the legal framework for decision-making.

11.36 We saw several examples of effective multi-agency safeguarding hubs, including at Leicestershire County Council, where a simple family chart was used to ensure that the agencies had as detailed a picture of the family as they could, in order to identify risks and offer appropriate services to help the families. For example, the Housing Department might be aware of two children, but the Social Services Department might be aware that the child of a new partner also stays at the same address sometimes, or that the children of the household sometimes stay with their maternal aunt. A genogram, a pictorial representation of who a family are and linking the households of a family, can be prepared from several sources. School absences can be helpful and findings of the health visitor and school nurse, as well as the child and family mental health services for each child can be set out side by side in pictorial form as well as in prose in order to build up a picture of the family's lives.

11.37 Significant steps have been taken towards improving the sharing of information in order to prevent safeguarding situations from arising. However, local authorities did describe hurdles in creating and carrying out the work of these hubs. Local authorities also reported that the success of a safeguarding hub was heavily dependent upon the development of good working relationships between the various agencies. It might be possible to engage with a local NHS Trust or group of general practitioners where a good relationship has developed with the relevant member of staff, but a change of personnel could cut off that source of important information. These findings reflected the work carried out by sociologists and academics in information technology, social policy and management.[26]

11.38 It is necessary to ask whether the law does enough to support careful attempts to develop innovative ways of sharing information appropriately and securely for the public good.

Birmingham City Council[27]

11.39 Birmingham City Council considered that in broad terms the current law strikes the right balance between the ability of public bodies to share data and the need to protect privacy or other rights of data subjects. However, where there are multi agency safeguarding projects, there is often a gap between the legal objectives and the legal powers to enable the parties to share information to meet these objectives.

Birmingham City Council case study: multi agency safeguarding

11.40 The Council gave the following example:

[25] Consultation meeting no. 18 – Leicestershire Centre of Excellence.

[26] See for example, Susan Baines, Rob Wilson and Sarah Walsh, "Seeing the full picture? Technologically enabled multi-agency working in health and social care" (2010) 25(1) *New Technology Work and Employment* 19.

[27] Consultation response no. 69 – Birmingham City Council.

There are a number of projects that require the input of different agencies to support either an individual or a family in crisis. The information that individual agencies holds for their own purpose e.g. drug and alcohol dependency, medical information, criminal records, which are relevant to the service that the individual agency provides, and if effectively shared, would shape how the agencies, when working together, would best achieve their shared objectives.

However, the circumstances in which the information was obtained from the service user, e.g. sensitive personal data, there is a heightened risk of the service user disengaging with these agencies if the sensitive personal data is shared, e.g. troubled families, children at risk.

Birmingham City Council case study: central care record

11.41 The Council gave the following example:

> The Council is involved in a project with a number of Care Commissioning Groups, hospital trusts and other local authorities, totalling 17, to implement a central care record system covering over 1.2 million individuals.
>
> The purpose of this project was to allow all parties involved to have access, where required, to key information relevant to the care of an individual. This included the development of :-
>
> a) a Practitioner Portal – A web portal allowing practitioners across the 17 organisations to see health and social care data from all partner organisations, based on role based access. This would allow practitioners access to information about an individual's Medication, on-going conditions/allergies, Reason for last hospital visit, other professionals involved (e.g. social workers) and results from tests/scans.
>
> This would allow a doctor/consultant/triage nurse to have additional information that could affect the appropriate care of the patient.
>
> b) a Patient Portal – A web portal allowing patients to have access to their health records; and
>
> c) a Data Warehouse – A data warehouse containing all health and social care data to inform commissioning decisions and prevention activity.

11.42 Availability of this information will drastically reduce duplication and time spent investigating and confirming information. This means that expectations of the public with respect to data sharing could frequently be in conflict with each other.

A LAW REFORM PROJECT

11.43 Although consultees considered that there is a need for better training and management of data sharing between public bodies – more resourcing; systems to provide advice and guidance and to disseminate best practice – there are

difficulties in pursuing these options in the current economic climate. Some organisations are however already taking important steps towards addressing this need, such as in local authorities through and the multi-agency information sharing hubs that we discuss above.

11.44 There are aspects of the law that are beyond the scope of a national law reform project because they derive from European Union law – such as the 1995 Data Protection Directive and, potentially, new Directives and Regulations – or the European Convention on Human Rights. Whilst we cannot usefully propose reform of these supranational instruments, consideration could be given to the scope left by them for a more nuanced approach to implementation of the 1995 Directive or to the margin of appreciation left by article 8 of the Convention.

11.45 Similarly, although structural reorganisation of public administration, in particular the National Health Service, could reduce the number of occasions on which a need is perceived to share information between separate bodies, such a task plainly raises issues going beyond any sensible Law Commission remit. The task to be undertaken in a law reform project is rather to design rules that accommodate the increase in the numbers and types of organisations that engage in the provision of public services in modern Britain whilst guarding against the information security risks posed by the dissemination of personal data amongst an increasing number of service providers.

11.46 A useful starting point for a review could be an investigation of the principles that should determine the categories of information that should be disclosed and the circumstances in which and purposes for which disclosure is legitimate. We have discussed this topic in Chapter 2. Such an investigation should be accompanied by further consideration of the dangers of breaches of data security and of the role of restrictions of disclosure in forestalling them.

11.47 There is a clear need for rationalisation of the statutory framework of rules (the "gateways") that create powers to disclose and limitations upon disclosure and upon onward disclosure. An unwieldy profusion of legislative powers, conditions, limitations and offences has developed, often in an ad hoc and unprincipled fashion, creating an unnecessary degree of legal complexity. There is scope for a substantial overhaul of the statutory framework.

11.48 We have received clear indications that the key to facilitating appropriate information sharing does not lie in conferring wide powers. These are if anything counter-productive from the point of view of encouraging such sharing of information as is thought appropriate: officials both lack confidence in the apparent scope of widely drawn powers and are wary of disclosing information otherwise than with the safeguards represented by the controls upon onward disclosure that are typical of many of the existing gateway provisions. Disclosure of sensitive data without such onward controls is in any event problematic from the point of view of civil liberties.

11.49 For these reasons, "gateways" may well remain the appropriate tool. However, there is a clear need for a smaller number of them, with a scope determined by the application of principles governing what is appropriately shared rather than, as often in the existing law, by the needs of a particular policy or project. A review of gateways could codify and simplify the existing law; provide an opportunity to

remove unnecessary duplication or overlap of powers; address powers that are not functioning effectively or appropriately; and consider whether the statutory conditions and limitations on disclosure are justified and appropriate.

11.50 A full review could also consider mechanisms for cooperation, breaking deadlock or enabling a third party to make a determination where parties to an information transfer cannot agree.

11.51 Particular issues in the common law of confidentiality, including understanding how that law operates in practice, would benefit from simplification and exposition. A review of the professional and sector-specific regulation of information disclosure could produce a set of reforms aimed at the clarification of these areas and the removal of unnecessary duplication of regulation. This might result in codification, explanation or guidance.

11.52 A full project would also explore a better procedure for creating new powers to disclose information, subject to proper scrutiny and adequate safeguards. Gateways should have proper locks and gatekeepers. A streamlined procedure for authorising information disclosure systems could improve scrutiny and safeguards, provide more certainty for front line officials, and maintain flexibility in light of legal and technical developments.

11.53 A full project would also consider the potential role of the Information Commissioner as a facilitator of appropriate disclosure or another body capable of issuing authoritative opinions on proper practice. A number of consultees argued for the Information Commissioner's role to be increased in this respect.

11.54 Rapid technological development makes it difficult to envisage what societal norms will be in the future and what protection will be needed. As a recent report to the President of the United States of America explained

> The challenges to privacy arise because technologies collect so much data (for example, from sensors in everything from phones to parking lots) and analyze them so efficiently (eg, through data mining and other kinds of analytics) that it is possible to learn far more than most people had anticipated or can anticipate given continuing progress. These challenges are compounded by limitations on traditional technologies used to protect privacy (such as de-identification). PCAST [the President's Council of Advisors on Science and Technology] concludes that technology alone cannot protect privacy, and policy intended to protect privacy needs to reflect what is (and is not) technologically feasible.[28]

11.55 Their answer to the problems of future-proofing was that policy should "focus primarily on whether specific uses of information about people affect privacy adversely." What is needed is

[28] Executive Office of the President of the United States of America, President's Council of Advisors on Science and Technology, *Report to the President: Big Data and Privacy – A Technological Perspective* (May 2014), available at: http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (last visited 1 July 2014).

policy focus on outcomes, on the "what" rather than the "how," to avoid becoming obsolete as technology advances.[29]

11.56 The problems identified in effective data sharing will not be resolved by law reform alone. Any solutions will have to involve consideration of how to use technology and sociological and behavioural questions about the incentives, disincentives and relationships between the organisations and individuals sharing information and the people whose information is being shared.

11.57 In addition to the uses to which data can be put there remain legitimate questions about the ways in which data can be processed and whether different types of processing require different approaches. For example, there is a difference between data matching to identify inconsistency which might demonstrate either error or fraud (such as individuals telling mutually inconsistent things to different Departments at the same time) and predictive analytics that might suggest the present or even future occurrence of error or fraud (such as inferring from other data the probability of an individual taking fraudulent or erroneous action). In particular, there are questions about the potentially discriminatory effects of such processing methods themselves; the risk of false positives having adverse effects on innocent individuals and accordingly the safeguards that would need to be in place were such processing to be undertaken by public bodies.

11.58 Dr Rob Wilson and Mike Martin of Newcastle University described law reform and the systems of information governance as the "architecture" of information management and argued that this is an inadequate approach to service provision today. They argue that at the heart of effective information systems, including the legal and technological systems, are good, working relationships at a local level and the information systems need to support the development of these relationships.[30]

11.59 We make three recommendations, set out in Chapter 1 above, for a UK-wide law reform project to be conducted on the disclosure of information between public bodies and those engaged in public services.

CONCLUSIONS

11.60 The law of data sharing is continually under reform, but that reform is piecemeal, time-bound and adds to the complexity and confusion which make data sharing practice so difficult for those making the day-to-day decisions. In order to achieve effective, sustainable reform of data sharing law and practice, a full survey of the law and a deep analysis of both law and practice are needed.

11.61 A full law reform project by the Law Commission would be a three year process, including the publication of a consultation paper, policy papers and a formal open

[29] Executive Office of the President of the United States of America, President's Council of Advisors on Science and Technology, *Report to the President: Big Data and Privacy – A Technological Perspective* (May 2014), available at: http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (last visited 1 July 2014).

consultation, in addition to ongoing engagement.

11.62 An essential first step in undertaking a thoroughgoing reform is to understand the law. We would conduct a detailed mapping exercise of the existing statutory framework and how it interacts with data protection, human rights and the common law. One of the key issues raised by Government departments and public bodies during the scoping stage was the sheer number and complexity of statutory gateways and a lack of understanding of what law currently exists. There is no map or single table of existing legislative data sharing powers. This would produce the most comprehensive overview of the current law to date and would identify areas of legal uncertainty and inconsistency.

11.63 We would gather evidence and views from all government departments and interested public bodies, on what forms of data they collect or hold and what they would like to do with data that they cannot already do. This would establish the most comprehensive evidence base to date of the demand for statutory reform and enable us to consider the impact reform would have.

11.64 The quality of the engagement with a broad range of non-governmental organisations would be a critical element of the project. We would create an advisory group bringing together groups with a privacy focus with a wide range of non-governmental organisations and groups with technological expertise, to understand concerns about data sharing and the appropriate safeguards needed to control data sharing in light of the pace of change in technology and government.

11.65 Reform of the law relating to data sharing is a difficult and ambitious task. We would not expect to solve all problems. Indeed, we do not think law reform is an answer to all of the problems identified in our consultation. However, we do think there are several important things a full law reform project could achieve.

11.66 First, a full law reform project would build significantly on the existing evidence base for reform and provide a comprehensive understanding of the data sharing landscape. We were surprised in consultation to find that there was such widespread misunderstanding and confusion about the statutory framework and its relationship with data protection, human rights and the common law. Confusion and misunderstanding around the statutory framework contributes to an overly cautious attitude, missed opportunities, wasted resources and unnecessary delays. Discussion and debate about reforming approaches to data sharing is also inhibited by such confusion and misunderstanding. We think that an independent exposition of the law is an essential underpinning to sustainable law reform in this field.

11.67 We have also frequently heard criticism, made both inside and outside government departments and public bodies, that there is insufficient analysis into the need for greater data sharing. The criticism is not that no need exists: it is that insufficient evidence has been collected and analysis conducted to support

[30] See the "Mary Story" case study in Wilson, Martin, Walsh and Richter, "Re-Mixing Digital Economies in the Voluntary Community Sector? Governing Identity Information and Information Sharing in the Mixed Economy of Care for Children and Young People" (2011) *Social Policy and Society* 379.

reform. Our scoping consultation was able to scratch the surface of this and discover the areas where more detailed evidence should be gathered and analysed. Consultation showed a belief in some parts of government that significant advantages can be gained from the effective use of data but these advantages are ill-defined. This lack of careful evidence-gathering and analysis stifles the development of fruitful discussion about data sharing. We think that an independent evidence-gathering exercise, conducted alongside a thorough exposition of the current law, would build significantly on the present evidence base and analysis.

11.68 Secondly, a full law reform project would build on this evidence and analysis to recommend a set of simplifications and rationalisations to remove or mitigate unnecessary areas of complexity or confusion and reinforce effective safeguards, placing a sophisticated and technologically-informed understanding of privacy concerns at the centre of such reform. Such a set of reform recommendations would not necessarily seek to increase the legal scope of data sharing but would reduce unnecessary delay and cost, improve efficiency and reduce waste. It could propose different safeguards where these would be more effective. One of the problems in data sharing is the restrictive interpretation of powers by those working in information governance and making day-to-day decisions, stemming from a number of incentives to be cautious and disincentives to disclose. This work would also help decision makers to act in a more confident manner where it is lawful to do so.

11.69 Thirdly, a full law reform project would seek to make recommendations to accommodate the fast pace of change in technology and government. The current legal landscape is struggling to keep pace with rapid and important changes in technology and the structure of public service delivery. There is a clear need for an agile and responsive legal landscape to ensure that data is used effectively and appropriately by public bodies. There is a danger that rapid change will harm individual privacy. We would examine what alternative mechanisms exist and make recommendations for a more streamlined process that can remain responsive to changes in technology and government with proper oversight and safeguards to protect individual rights.

11.70 The following options should be considered, along with others:

(1) a statutory code setting out principles to be applied to any decision on data sharing, criteria which must be considered and weighed and appropriate safeguards, in place of statutory gateways;

(2) accepting the need for particularisation of statutory gateways and providing certainty for front-line officials while making them more flexible, principled, consistent and transparent;

(3) a combination of these two, with model gateways to be selected by Ministers and introduced by secondary legislation where needed;

(4) a streamlined, transparent and independent decision-making process for approving new data sharing gateways without the need for bespoke primary or secondary legislation.

11.71 Any system of data sharing should be sufficiently flexible to adapt to changes in modes of service delivery and to policy, legal and technological developments.

(*Signed)* DAVID LLOYD JONES, *Chairman*
ELIZABETH COOKE
DAVID HERTZELL
DAVID ORMEROD
NICHOLAS PAINES

ELAINE LORIMER, *Chief Executive*
1 July 2014

APPENDIX A
LIST OF WRITTEN RESPONSES

A.1 Written responses were received from:

(1) Somerset County Council;

(2) Welwyn Hatfield Borough Council;

(3) Flintshire County Council:

(4) Worcestershire County Council;

(5) Nottinghamshire Police;

(6) Shropshire Fire and Rescue;

(7) Veterinary Medicines Directorate;

(8) Public and Commercial Services Union Land Registry Group;

(9) Nottingham and Nottinghamshire Local Resilience Forum;

(10) West Midlands Fire and Rescue Service;

(11) Linda Damerell, Tapestry Innovation Ltd;

(12) Paul Miloseski Reid, London Borough of Richmond upon Thames Trading Standards Service;

(13) Betsi Cadwaldr University Local Health Board;

(14) East Sussex Fire and Rescue;

(15) Kent Fire and Rescue Service;

(16) Stephen Berry, Gaist Solutions;

(17) Leeds City Council;

(18) Marion Oswald, University of Winchester;

(19) The Insolvency Service;

(20) Humberside Fire and Rescue Service;

(21) Information Commissioner's Office;

(22) British Medical Association;

(23) Senior Traffic Commissioner;

(24) Tendring District Council;

(25) Royal Statistical Society;

(26) Cheshire Fire and Rescue Service;

(27) Hertfordshire County Council;

(28) National Society for the Prevention of Cruelty to Children;

(29) Social Landlords Crime and Nuisance Group;

(30) Information Records and Management Society;

(31) Her Majesty's Land Registry;

(32) NHS National Services Scotland;

(33) The UK Cards Association;

(34) National AIDS Trust;

(35) Dr Ashley Savage, Dr Richard Hyde, Mr Jamie Grace and Ms Bansi Desai;

(36) London Fire Brigade;

(37) London Borough of Camden;

(38) Wiltshire Fire and Rescue Service;

(39) Office of the Children's Commissioner;

(40) Liberty;

(41) Sue Richardson, University of Bradford;

(42) The Payments Council;

(43) The Welsh Government;

(44) Medical Protection Society;

(45) Association of Chief Police Officers;

(46) Royal College of Psychiatrists;

(47) Monitor;

(48) Hampshire County Council;

(49) DAC Beachcroft;[1]

(50) Wakefield Metropolitan District Council;

(51) CIFAS (formerly the Credit Fraud Avoidance Service);

(52) Chief Fire Officers Association;

(53) Merseyside Fire and Rescue Service;

(54) Wolverhampton City Council;

(55) Office for National Statistics;

(56) Manchester City Council;

(57) Derbyshire Fire and Rescue Service;

(58) NHS Protect;

(59) Missing People;

(60) UK Anti-Doping;

(61) Transport for London;

(62) Department for Environment, Food and Rural Affairs;

(63) Cheshire West, Cheshire Council and West Cheshire Clinical Commissioning Group (Joint Response);

(64) Karen Heath;

(65) Independent Information Governance Oversight Panel, chaired by Dame Fiona Caldicott;

(66) Neath Port Talbot Council for Voluntary Service;

(67) Tunbridge Wells Borough Council;

(68) Lincolnshire City Council;

(69) Birmingham City Council;

(70) David Stone, Kaleidoscope Consultants;

(71) Mind;

(72) Manchester Fire and Rescue Service;

[1] DAC Beachcroft organised a series of discussion sessions with its clients and contacts in the health and social care sector. These events were attended by individuals from a total of 38 organisations, including local authorities, clinical commissioning groups, NHS providers, national bodies, private and third sector providers of services and consultants working with organisations in the sector.

(73) Society for Computers and Law;

(74) Scottish Government;

(75) General Pharmaceutical Council;

(76) Northumbria University;

(77) Department of Health;

(78) Rosemary Jay, Hunton and Williams LLP (in her personal capacity);

(79) Karen Thomson, NHS England (in her personal capacity);

(80) Sheffield City Council;

(81) Department for Communities and Local Government;

(82) Rosemary Harrison;

(83) Department for Education;

(84) Lawrence Serewicz, Principal Information Governance Officer, Durham County Council;

(85) Vocalink;

(86) Leicester City Council;

(87) Tangent Securities Ltd.

APPENDIX B
LIST OF CONSULTATION MEETINGS

B.1 We had consultation meetings with:

(1) Public Service Information Network;

(2) Cabinet Office and Ministry of Justice;

(3) Richard Thomas, Information Commissioner from 2002 to 2009;

(4) Ministry of Justice EU Data Protection Team;

(5) Rushmoor Borough Council;

(6) Worcestershire County Council;

(7) Amberhawk Conference attendees;

(8) Marion Oswald, University of Winchester, and Paul Gibbons, FOIMan blogger and consultant;

(9) London Information Rights Forum attendees;

(10) Information Commissioner's Office;

(11) Her Majesty's Revenue and Customs;

(12) Dr Rob Wilson and Professor Mike Martin, Newcastle University Business School;

(13) Making Digital Government Work Panel Debate attendees;

(14) City of London Police Economic Crime Directorate;

(15) Hazel Grant, Bristows LLP;

(16) Sue Richardson, University of Bradford;

(17) Rosemary Jay, Hunton and Williams LLP (in her personal capacity);

(18) Leicestershire County Council and Hinckley and Bosworth Borough Council;

(19) Royal Statistical Society;

(20) Health and Social Care Forum attendees;

(21) National Association of Data Protection Officers Conference attendees;

(22) Sally Taber, Independent Healthcare Advisory Services;

(23) Office for National Statistics;

(24) Northumbria University Information Law Centre Conference attendees;

(25) A water company;

(26) Dr Rob Wilson and Professor Mike Martin, Newcastle University Business School;

(27) Birmingham City Council: Legal;

(28) Birmingham City Council: Service Delivery Officials;

(29) Department of Health;

(30) Jeremy Taylor, National Voices;

(31) Nick Pickles, Big Brother Watch;

(32) Open Rights Group, Privacy International, MyDex, MedConfidential;

(33) Department for Communities and Local Government, Troubled Families Programme;

(34) Department for Education, National Pupil Database;

(35) Privacy International;

(36) Health and Social Care Information Centre;

(37) Timothy Pitt-Payne QC, 11King's Bench Walk Chambers;

(38) Vocalink;

(39) Rob Paley North East London NHS Trust Information Governance;

(40) National Society for the Prevention of Cruelty to Children;

(41) UK Anonymisation Network;

(42) Dr Emma Young, Barts NHS Trust (in her personal capacity);

(43) Simon Howarth, Deputy Senior Information Risk Officer, North West London Hospitals NHS Trust and Ealing Hospital NHS Trust;

(44) Department for Work and Pensions;

(45) Fuel Poverty Workshop attendees, National Centre for Social Research;

(46) Effective Information Sharing Conference attendees;

(47) Cabinet Office and Involve Open Policy Process attendees;

(48) Conference on Trust, Risk and Information Law attendees;

(49) Citizen's Advice Bureau;

(50) The Department for Environment, Food and Rural Affairs and the Environment Agency.

APPENDIX C
GOVERNMENT INITIATIVES AND PUBLICATIONS ON DATA SHARING

C.1 This list contains all reports and initiatives which we have been alerted to in consultation, in chronological order, but is not an exhaustive list of Government initiatives on data sharing:

(1) Department of Health: Report of the Review of Patient Identifiable Information (December 1997) (Caldicott Review);

(2) Performance and Innovation Unit, Privacy and Data Sharing: The Way Forward for Public Services (April 2002);

(3) DWP, Social Security Fraud Act 2001 Code of Practice on Obtaining Information (April 2002);

(4) HM Government, Data Protection and Sharing: Guidance for Emergency Planners and Responders. Non Statutory Guidance to Complement Emergency Preparedness and Emergency Response and Recovery. (February 2007);

(5) Co-ordinated Action Against Domestic Abuse, Disclosure of Information Before and After MARAC Meetings (September 2007);

(6) Justice Committee on Human Rights, Protection of Private Data (December 2007);

(7) Justice Committee on Human Rights, Data Protection and Human Rights (March 2008);

(8) Cabinet Office, Data Handling Procedures in Government: Final Report (June 2008);

(9) Richard Thomas and Mark Walport, Data Sharing Review Report (July 2008);

(10) Justice Committee on Human Rights, Legislative Scrutiny: Coroners and Justice Bill (March 2009);

(11) Department for Education, Information Sharing: Guidance for Practitioners and Managers (March 2009);

(12) Department for Education, Information Sharing: Further Guidance on Legal Issues (March 2009);

(13) Ministry of Justice, Undertaking Privacy Impact Assessments: The Data Protection Act 1998 (August 2010);

(14) Department of Health, Liberating the NHS: An Information Revolution (October 2010);

(15) Quality Care Commission, Code of Practice on Confidential Personal Information (December 2010);

(16) OEDC, The Evolving Privacy Landscape: 30 Years After the OEDC Privacy Guidelines (April 2011);

(17) Munro Review of Child Protection: Final Report A Child Centred System (May 2011);

(18) McKinsey Global Institute, Big Data: The next frontier for innovation, competition and productivity (May 2011);

(19) HM Government, Information Principles (December 2011);

(20) Department of Health, The Power of Information: Putting all of us in control of the health and care information we need (May 2012);

(21) Cabinet Office, Open Data: Unleashing the Potential. White Paper (June 2012);

(22) World Economic Forum, Rethinking Personal Data: Strengthening Trust (2012);

(23) The Scottish Government, A Scotland Wide Data Linkage Framework for Statistics and Research (2012);

(24) The UK Administrative Data Research Network: Improving Access for Research and Policy (December 2012);

(25) Shakespeare Review: An Independent Review of Public Sector Information (May 2013);

(26) Department of Health, The Information Governance Review: To Share or Not to Share (March 2013) (Caldicott 2);

(27) Wales Accord on Sharing Personal Information: Guidance on the Development of an Information Sharing Protocol (May 2013);

(28) The Government Response to the Shakespeare Review of Public Sector Information (June 2013);

(29) Accessibility, Sustainability, Excellence: how to expand access to research publications. Report of the Working Group on Expanding Access to Published Research findings (June 2013);

(30) Kieron O'Hara, Transparent Government, Not Transparent Citizens: A Report on transparency and Privacy for the Cabinet Office (Date not available);

(31) Home Office, Information Sharing for Community Safety: Guidance and Practice Advice (Date not available).

C.2 Other initiatives involved with data sharing:

(1) Tell Us Once;

(2) Troubled Families;

(3) Wales Accord on Sharing Personal Information;

(4) Scottish Accord on Sharing Personal Information;

(5) BIS Business Support Programme.