Law Commission

Consultation Paper No 214

DATA SHARING BETWEEN PUBLIC BODIES

A Consultation Paper

THE LAW COMMISSION – HOW WE CONSULT

About the Law Commission: The Law Commission was set up by section 1 of the Law Commissions Act 1965 for the purpose of promoting the reform of the law.

The Law Commissioners are: The Rt Hon Lord Justice Lloyd Jones, *Chairman,* Professor Elizabeth Cooke, David Hertzell, Professor David Ormerod QC and Frances Patterson QC. The Chief Executive is Elaine Lorimer.

Topic of this consultation: This consultation paper considers issues relating to data sharing between public bodies. The purpose of this consultation is to identify the causes of reported obstacles.

Geographical scope: This consultation paper applies to the law of England and Wales.

Availability of materials: The consultation paper is available on our website at http://lawcommission.justice.gov.uk/consultations/data-sharing.htm.

Duration of the consultation: We invite responses from 16 September to 16 December 2013.

Comments may be sent:

By email to data.sharing@lawcommission.gsi.gov.uk

OR

By post to Sarah Young, Public Law Team, Law Commission, Steel House, 11 Tothill Street, London SW1H 9LJ

Tel: 020 3334 0279 / Fax: 020 3334 0201

If you send your comments by post, it would be helpful if, whenever possible, you could also send them electronically (for example, on CD or by email to the above address, in any commonly used format).

After the consultation: In the light of the responses we receive, we will decide whether a full reform law reform project is needed. We will make recommendations accordingly and present them to Government.

Consultation Principles: The Law Commission follows the Consultation Principles set out by the Cabinet Office, which provide guidance on type and scale of consultation, duration, timing, accessibility and transparency.

The Principles are available on the Cabinet Office website at: https://update.cabinetoffice.gov.uk/resource-library/consultation-principles-guidance.

Information provided to the Law Commission

We may publish or disclose information you provide us in response to this consultation, including personal information. For example, we may publish an extract of your response in Law Commission publications, or publish the response in its entirety. We may also be required to disclose the information, such as in accordance with the Freedom of Information Act 2000.

If you want information that you provide to be treated as confidential please contact us first, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic disclaimer generated by your IT system will not be regarded as binding on the Law Commission.

The Law Commission will process your personal data in accordance with the Data Protection Act 1998.

THE LAW COMMISSION

DATA SHARING BETWEEN PUBLIC BODIES

CONTENTS

CHAPTER 1
INTRODUCTION

THE PROJECT

1.1 Data sharing is a common part of modern governance and the delivery of public services. Public bodies collect large amounts of data from individuals and other organisations in the exercise of their various functions and share these data with other public bodies. There are reported to be significant obstacles to effective data sharing. It is not, however, clear whether these obstacles are the result of inadequacies in the legal regime governing data sharing or the result of a number of practical or cultural barriers.

1.2 In 2010, the Law Commission consulted on the content of the 11th programme of law reform. A project on data sharing was proposed by three consultees with police backgrounds. Discussions with the Ministry of Justice suggested that there were general issues with data sharing.

1.3 The 11th programme was published on 18 July 2011. The objective of our project was stated as follows:

> There are persistent reports of problems with data sharing between public bodies. That there is at least the perception of a problem is attested to by the fact that Parliament has on a number of occasions chosen to legislate to create statutory "gateways", giving specified public bodies express powers to share data. But it is not clear what the nature of these perceived obstacles to data sharing is.[1]

1.4 In most other projects, we know that the law needs reforming. We are not certain that this is the case with this project. The problems with data sharing between public bodies may originate from a number of causes other than a deficit in substantive law, such as: a lack of guidance or education; insufficient technology; cultural blocks; inadequate organisation; or excessive sanctions. At this stage, we are carrying out a scoping exercise. The objective of this exercise is not to propose any reform to the current legal framework but to investigate the root causes of the reported obstacles to data sharing between public bodies. Once these causes are identified, we will decide whether a full law reform project is needed, and will make recommendations accordingly.

1.5 In this consultation paper, we do not make any provisional proposals for changes to the law. We have set out the law as background to the information we seek. The most important part of this paper is the series of questions at the end. We would be grateful for consultation responses that answer the questions that consultees feel are most appropriate to them. We would also be grateful for any further reflections or thoughts on data sharing.

1.6 Responses to this consultation paper must be submitted by 16 December 2013. Our final report containing our recommendations on the scope of any future project will be published in the spring of 2014.

[1] Eleventh Programme of Law Reform (2011) Law Commission No 330 at 2.19 and 2.20.

Benefits of and concerns about data sharing

1.7 Why should public bodies share data at all? A number of clear public benefits are claimed for data sharing, from controlling fraud and error in the state's financial relations with the citizen to improving the quality of policy making and service delivery. We set out these claims in Chapter 2.

1.8 We are also clear that there would only be a problem if it is *legitimate* data sharing that is being prevented. There are legal aspects to this but it also raises matters of principle. Sharing cannot be legitimate if it is unlawful. The laws of data protection and confidentiality place limits on lawful sharing. We explore these in Chapter 3 below. There are also questions as to whether public bodies *should* have the legal power to share data even where the sharing is not prevented by these prohibitions. There are important ethical limits on what the state should know about individuals at all; and further, on how information should be disseminated between different institutions within the state. We explore these issues in Chapter 2.

Geographical scope of the project

1.9 The project covers the law of the jurisdiction of England and Wales. We are, nonetheless, interested in views from public bodies and others in Scotland and Northern Ireland. We will be working with our sister Law Commissions in those jurisdictions to ensure that stakeholders there have the opportunity to comment.

BACKGROUND TO THE PROJECT

Types of data

1.10 There are different types of data which might be the subject of sharing between public bodies in different circumstances.

1.11 Data may be deliberately recorded by individuals, either manually, for example a form filled out manually at a GP's practice, or electronically, for example an on-line registration. They may also be automatically collected via diverse electronic devices such as a geo-location device or smart passes for highways.

1.12 In respect of the medium on which that information is contained, the concept of data includes information available in whatever form, for example alphabetical, numerical, graphical, photographical or acoustic, information on paper or stored in a computer memory, image and sound.[2]

Personal data

1.13 Personal data may be broadly defined as data relating to individuals, including "objective" information, for example biometric data provided by fingerprints, and "subjective" information, for example an assessment of the reliability of a borrower or insured, whatever its accuracy.[3]

[2] See Article 29 data protection working party, *Opinion 4/2007 on the concept of personal data* (20 June 2007), at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (last visited 30 August 2013).

[3] See Article 29 data protection working party, *Opinion 4/2007 on the concept of personal data* (20 June 2007).

1.14 Personal data are mainly regulated by the Data Protection Act 1998. This Act provides that personal data are data which relate to a living individual who can be identified from those data or from those data and other information. It includes any expression of opinion about the individual or any indication of the intentions of the data controller or any other person in respect of the individual.[4] It also defines the term "data" as information processed by means of equipment operating automatically in response to instructions given for that purpose; recorded with the intention that it should be processed by means of such equipment; recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; which forms part of an accessible record; or, if it does not fulfil any of these criteria, is recorded information held by a public authority.[5]

1.15 Personal data include sensitive personal data and less risky personal data, such as the service register of a car held by a garage containing the information about the car of an individual. For the purposes of the Data Protection Act, sensitive personal data are personal data consisting of information as to the racial or ethnic origin of a person; his or her political opinions; his or her religious beliefs or other beliefs of a similar nature; whether he or she is a member of a trade union; his or her physical or mental health or condition; his or her sexual life; the commission or alleged commission by him or her of any offence; or any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings or the sentence of any court in such proceedings.[6]

Anonymised data

1.16 Anonymised data are not personal data to the extent that they have had all personal elements likely to identify an individual removed, such as name, address, date of birth, national insurance number, national health service number or tax reference number. De-identified data or pseudonymised data, sometimes called "key-coded data", are a form of anonymised data presented at the individual level rather than aggregated, where individuals are distinguished by the use of a unique identifier which does not reveal their real identity. Among the different types of anonymised data, pseudonymised data pose a high level of re-identification risk.[7]

[4] Data Protection Act 1998, s 1.

[5] Data Protection Act 1998, s 1.

[6] Data Protection Act 1998, s 2.

[7] See Information Commissioner's Office, *Anonymisation: managing data protection risk. Code of practice* (November 2012), at http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/anonymisation_code.ashx?type=Finjan-Download&slot=00000141&id=00000940&location=0A64420E (last visited 30 August 2013); the UK Administrative Data Research Network, *Improving Access for Research and Policy* (Administrative Data Taskforce, December 2012) p 41, at http://www.esrc.ac.uk/_images/ADT-Improving-Access-for-Research-and-Policy_tcm8-24462.pdf (last visited 30 August 2013); Information Commissioner Office, *Proposed new EU General Data Protection Regulation: Article-by-article analysis paper* (12 February 2013) p 7, at http://www.ico.org.uk/~/media/documents/library/Data_Protection/Research_and_reports/ico_proposed_dp_regulation_analysis_paper_20130212_pdf.ashx (last visited 30 August 2013), in which the Information Commissioner, discussing the content of the future EU Regulation, takes the view that adopting a broad definition of personal data, including pseudonymised data, is desirable.

Other information

1.17 Not all information is personal data. For example, financial data about companies, or records of the performance of public services are obviously not personal data. Instead of relating to individuals, data may also relate, for example, to fauna or flora, buildings, civil structures, temperature, or quality of air or sea.[8]

1.18 In the category of information held by and relating to public services,[9] some information is factual and consists of "raw" or "source" data, such as "datasets".[10] However some other information includes an element of analysis going beyond calculation, for example an assessment of the risks of emergencies in the context of civil contingencies.[11] Data may qualify as official statistics within the meaning of the Statistics and Registration Service Act 2007.[12]

1.19 Some information may be protected by intellectual property rights or the law of confidentiality, as commercial or statistical information, or protected on the ground that it relates to defence or national security.[13]

Issues raised by data sharing

1.20 Data sharing raises, in any democratic society, fundamental issues regarding the respective weight of individuals' freedoms and the public interest. A balance needs to be struck between the need to protect the privacy of citizens and the necessity for public authorities to carry out their functions, such as taxation and the prevention of crime, in a fair and efficient way.

1.21 Protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by article 8 of the European Convention of Human Rights. Any encroachment on this right raises fears of the invasion of privacy. The potential threat to individual freedom posed by data sharing may be reinforced where the sharing occurs between a large number of entities and translates into a centralisation of records.[14]

1.22 The development of information technology brings with it pressures for the

8 Eg sensor networks used to monitor forests in order to prevent forest fires, the structural integrity of civil structures for localising damage in bridges, or for energy control purposes.

9 See, in respect of "public sector information", the Re-use of Public Sector Information Regulations 2005 SI 2005 No 1515, stemming from the Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the Re-Use of Public Sector Information Official Journal L 345/90 of 31.12.2003, recently amended by Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 Official Journal L 175/1 of 27.06.2013.

10 See the definition of dataset at s 11(5) of the Freedom of Information Act 2000.

11 As provided under Civil Contingencies Act 2004.

12 Statistics and Registration Service Act 2007, s 6(1).

13 In this respect, it is worth noting that most public sector information is published under the open government licence. See eg the *Draft national action plan: From Open Data to Open Government* (27 June 2013), mentioning 7959 datasets published on *data.gov.uk* under this type of licence, at https://www.gov.uk/government/consultations/open-government-partnership-uk-draft-national-action-plan-2013/ogp-uk-2013-draft-national-action-plan-from-open-data-to-open-government (last visited 30 August 2013).

14 See eg *Database State. A report commissioned by the Joseph Rowntree Reform Trust Ltd* (2009) p 4, at http://www.jrrt.org.uk/publications/database-state-full-report (last visited 30 August 2013).

dissemination of information about individuals. The existence of large computer databases means that data can be lost on a far larger scale than could occur historically. At the same time, storage practices are evolving. Third-party data storage services located in a foreign jurisdiction are increasingly widespread.[15] This has increased the vulnerability of data and the focus on security in their transmission.

Perception of obstacles

1.23 Sharing data brings with it many benefits. In particular, it helps public bodies to make informed and "joined-up" policy decisions through the delivery of evidence derived from an increasing number of policy areas. It unearths correlations that would otherwise remain invisible and thereby helps tackle multi-dimensional challenges. By reducing searching and processing time, it helps to speed up decision-making and improves efficiency in the provision of public services, while potentially cutting the administrative burden on data subjects. Taxation, fighting fraud, combating crime, tackling child poverty, and improving health care all depend on integrating information from multiple data sources. Establishing correlations between factors also allows research to make progress, which is fundamental in a knowledge-based economy.

1.24 Expectations of the public regarding the processing of their data are seen as increasing. The development of low cost information and communications technology makes it cheaper and easier to collect, share and combine information. As business is providing offers in line with people tastes and needs, on the basis of personalised data obtained from internet users, public services are equally expected to be better tailored to people's needs. Data sharing may be instrumental in improving public services.

1.25 However, there is a sense that the potential of data sharing is not fully realised. In line with the current government's policy agenda, better use of public sector data is promoted and underpins a number of ongoing initiatives.

1.26 The transparency and open data strategy is an important building block of this policy. Promoting publication of anonymised data about public services' performance, such as school grades, crime data, rail punctuality data or hospital waiting times,[16] this strategy also aims to increase the transparency and accountability of government action, help individuals to make informed choices and to encourage business to create value from these data.[17]

1.27 This policy is implemented by each government department through an open data strategy. It is supported by a series of statutes such as the Freedom of Information Act 2000, the Environmental Information Regulations 2004,[18] and the

[15] See OECD, *The evolving privacy landscape; 30 years after the OECD privacy guidelines* (April 2011) OECD Digital Economy Papers No 176 OECD Publishing p 18.

[16] In particular through the website www.data.gov.uk.

[17] On the anticipated economic benefits, see *Shakespeare review: An Independent Review of Public Sector Information* (May 2013), at https://www.gov.uk/government/publications/shakespeare-review-of-public-sector-information (last visited 30 August 2013).

[18] SI 2004 No 3391.

Re-use of Public Sector Information Regulations 2005,[19] and underpinned by the *Information Principles*,[20] which promote re-use and publication of public information.

1.28 Obstacles to data sharing are said to be partly legal, partly non-legal. Among the legal factors, uncertainty is often identified as one of the main obstacles preventing public bodies from sharing data.[21] The legal and regulatory environment is commonly criticised as complex and a source of diverse interpretations, giving rise to uncertainties and, as a result, an overly cautious approach. Guidance is not always sufficient to dispel such uncertainty.

1.29 Difficulties have also sometimes been attributed to insufficient powers to collect or share data. Against this background, a new statutory fast-track procedure has been seen as one of the ways of removing legal obstacles.[22] Past proposals to introduce such procedures have, however, been controversial.[23]

1.30 In some cases, it seems that a low public acceptance of data sharing and a low level of trust in the way it is undertaken by public services, along with negative media coverage, may constitute further hindrances. Anticipating this reluctance, by public bodies may prefer not to share data when they suspect that individuals would not give their consent, although consent is not always necessary.[24]

1.31 Qualitative problems of both legal[25] and practical relevance, such as incomplete, out of date, inconsistent or other low quality data may be an obstacle to the transfer and linkage of data. For example, the fact that there may be several different "unique identifiers"[26] in use can make it difficult to link datasets from different systems.[27]

[19] SI 2005 No 1515.

[20] *Information Principles* (December 2011), at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85987/Information_Principles_UK_Public_Sector_final.pdf (last visited 30 August 2013).

[21] See eg Scottish Government, *A Scotland-wide Data Linkage Framework for Statistics and Research: Consultation Paper on the Aims and Guiding Principles* (March 2012) p 14, at http://www.scotland.gov.uk/Resource/0039/00390444.pdf (last visited 30 August 2013).

[22] See eg R Thomas and M Walport, *Data Sharing Review Report* (July 2008), at http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/datasharingreview.pdf (last visited 30 August 2013). They recommend that primary legislation should provide the Secretary of State, in precisely defined circumstances, with a power by order, subject to the affirmative resolution procedure in both Houses, to remove or modify any legal barrier to data sharing by: repealing or amending other primary legislation; changing any other rule of law (eg the application of the common law of confidentiality to defined circumstances); or creating a new power to share information where that power is currently absent.

[23] See paras 4.21 to 4.22 below.

[24] Scottish Government, *A Scotland-wide Data Linkage Framework for Statistics and Research: Consultation Paper on the Aims and Guiding Principles* (March 2012) p 14. Pointing to this deficit in trust in how governments use personal data, see eg World Economic Forum, *Rethinking Personal Data: Strengthening Trust* (2012), at http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf (last visited 30 August 2013).

[25] See para 3.40 below.

[26] Eg a number or code relating to a unique individual.

[27] Scottish Government, *A Scotland-wide Data Linkage Framework for Statistics and Research: Consultation Paper on the Aims and Guiding Principles* (March 2012) p 11.

1.32 Security issues, similarly addressed by the law,[28] are also a key hindrance in data sharing and linkage. Safe processing requires a suitable technological infrastructure, including the IT hardware and software. It also demands organisational protective measures.[29]

1.33 The limited capacity of public sector organisations to analyse and make use of linked data is another commonly cited problem.[30]

1.34 Finally, cultural issues are reported to assume a prominent role as obstacles to data sharing.

1.35 The Thomas-Walport review reported only a few specific examples of situations where data sharing was being prevented by the legal framework.[31] By contrast, it reported several cultural and institutional barriers to data sharing such as an attitude of risk aversion, a lack of funds or proper IT, unsatisfactory legal advice and an unwillingness to put required safeguards in place or to seek the necessary consents to use data.

1.36 The report also underlined that communication and training were key to the success of data sharing. Senior management had to implement good practice, supported by training programmes, which had to be communicated to the relevant staff. Clearer lines of responsibility and accountability structures were also necessary.[32]

1.37 The Caldicott review 2 published in April 2013 also stressed the need for a cultural change in health and social care to shift from a "risk-averse" culture to one of trust.[33] The review panel observed that mandatory training in information governance tended to focus more on processes rather than underlying principles and could be confined to a 'tick-box exercise". When staff knowledge of data sharing rules was insufficient, staff lacked the ability or confidence to share information appropriately. This encouraged risk-averse attitudes to sharing.

[28] See para 3.43 below.

[29] See eg Cabinet Office, *Data Handling Procedures in Government: Final Report* (June 2008), at https://www.gov.uk/government/publications/data-handling-procedures-in-government (last visited 30 August 2013).

[30] Scottish Government, *A Scotland-wide Data Linkage Framework for Statistics and Research: Consultation Paper on the Aims and Guiding Principles* (March 2012) p 12.

[31] R Thomas and M Walport, *Data Sharing Review Report* (July 2008).

[32] The nomination of a person specifically responsible for managing information is one possible response to these problems.This was the solution put forward in the 1997 *Review of the Uses of Patient-Identifiable Information,* at http://www.wales.nhs.uk/sites3/Documents/950/DH_4068404.pdf. This review, chaired by Dame Fiona Caldicott, recommended that a network of senior health professionals, referred to as "Caldicott Guardians", be established across the NHS, with the primary role of protecting patient information.

[33] F Caldicott, *Information: to share or not to share? The Information Governance Review* (March 2013) at https://www.gov.uk/government/news/health-secretary-to-strengthen-patient-privacy-on-confidential-data-use (last visited 30 August 2013).

1.38 The review recommended that the Law Commission should look at how the law surrounding deceased persons might be better harmonised and recommended removing the legal impediments to giving custodianship of individuals' health and social care data within their last will and testament. Caldicott also recommended that initiatives involving the creation or use of family records should be examined in detail from the perspective of article 8 of the European Convention on Human Rights. We will take account of these recommendations.

1.39 According to a roundtable discussion hosted by the Guardian in association with Objective in February 2013,[34] the main challenge is to change cultures in the public sector. There is a lack of awareness by staff of the value of data sharing, partly because management is not actively involved in this area and does not provide enough incentives to share data properly. Insufficient value attached to information management in workplace education and training is also identified as one of the causes of this failure. This lack of awareness leads to a lack of engagement by members of the organisation; data sharing is not integrated into the routine work. Further, trust between partner bodies is often insufficient.

1.40 These observations underline the relevance of the *Information Principles* which state that information is a valued asset and that in order to fully understand its value it is necessary to understand the purposes for which information is created and managed. This includes consideration of both the original purpose for which information is collected and also, as far as can be anticipated, any subsequent downstream use.[35]

1.41 In line with the Caldicott Review 2, the Scottish Government recently observed that an overly cautious approach prevailed in the public sector, fuelled by the fear of public disapproval of data processing. The Scottish Government also suggested that "a sense of 'territoriality' stemming from the level of resources already invested in developing approaches to data linkage" might explain a lack of willingness to share data.[36]

1.42 Moreover, where the processing of data takes place in a complex environment involving sub-contractors and different partners, sharing data may raise issues in terms of allocation of responsibility between public bodies. This uncertainty may in turn hinder the processing of data.[37]

Official initiatives

1.43 A number of initiatives have been taken by public authorities to provide better data sharing or linkage for research and statistical purposes and to better share

[34] Dan Jellinek, "Why sharing data can save services", *The Guardian*, 23 January 2013, at http://www.guardian.co.uk/public-leaders-network/2013/jan/23/public-sector-sharing-data (last visited 30 August 2013). Objective Corporation is a provider of content, collaboration and process management solutions for the public sector and regulated industries.

[35] *Information Principles* (December 2011), at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85987/Information_Principles_UK_Public_Sector_final.pdf (last visited 30 August 2013).

[36] See Scottish Government, *A Scotland-wide Data Linkage Framework for Statistics and Research: Consultation Analysis*, at http://www.scotland.gov.uk/Publications/2012/08/3287/4 (last visited 30 August 2013).

[37] See OECD, *The evolving privacy landscape; 30 years after the OECD privacy guidelines* (April 2011) OECD Digital Economy Papers No 176 OECD Publishing p 32.

personal information about individuals between organisations, for a more joined-up service. One response has been the multiplication of statutory gateways,[38] with a view to creating or reinforcing the powers of public authorities to share information.[39] Organisational experiments, such as multi-agency safeguarding hubs,[40] have also been carried out. Acknowledgements of the problem and attempts to remedy it have also been put forward in a series of reports.

1.44 In 2002, the report on *Privacy and Data Sharing* concluded that:

> there is great potential to make better use of personal information to deliver benefits to individuals and to society, including through increased data-sharing.[41]

1.45 The Walport-Thomas review[42] expressed a similar view and recommended the setting up of a new statutory fast-track procedure to remove legal obstacles, where necessary, subject to Parliamentary scrutiny. The review also suggested changes to training and accountability in relevant organisations and recommended reinforcing the powers of the regulator responsible for enforcing the rules and issuing guidance.

1.46 The Cabinet Office White Paper *Open Data*[43] was also concerned with realising the potential of a transparency policy, including easing anonymised data sharing between public bodies for non-operational purposes, subject to compliance with robust safeguards.[44]

1.47 How to make the best use of public sector information to support economic growth was also the subject of the *Shakespeare Review.*[45] Highlighting the potential benefits of using these data, it warned against a risk-averse approach likely to restrict the access to information, recommending instead increased penalties in case of misuse of data.[46]

1.48 In the area of research and statistics, the Administrative Data Taskforce identified

[38] Namely statutory provisions dealing with data sharing.

[39] See, for a recent example the consultation about giving HMRC greater flexibility to share and publish data, HMRC, *Sharing and publishing data for public benefit. Consultation document*, at https://www.gov.uk/government/consultations/sharing-and-publishing-data-for-public-benefit (last visited 3 September 2013). See chapter 4 for further developments on statutory gateways.

[40] Eg the “Mash” project brings together police, children's and adult social care teams, health services and others to collect and share information on vulnerable children, families and adults.

[41] Performance and Innovation Unit, *Privacy and data-sharing: The way forward for public services* (April 2002) p 2.

[42] R Thomas and M Walport, *Data Sharing Review Report* (July 2008).

[43] *Open Data. White paper*. *Unleashing the Potential* (2012) Cm 8353.

[44] *Open Data. White paper*. *Unleashing the Potential* (2012) Cm 8353. These data aim to facilitate analysis and improve the creation of evidence-based policy. They include eg data on offenders, benefit claimants and employees, shared between the Ministry of Justice, DWP and HMRC in order to analyse the employment and benefit outcomes for offenders.

[45] *Shakespeare Review: An Independent Review of Public Sector Information* (May 2013). See in particular Recommendation 5.

that the two main hindrances to access to and use of de-identified administrative data were data holders' concerns about disclosure of personal data and legal restrictions related to their use.[47] The report recommended the establishment of an Administrative Data Research Centre in each of the four countries of the UK in order to legally secure access to and linkage of data, supported by a generic statutory gateway. In the same area, the Scottish Government is setting up a *Data Linkage Framework for Statistics and Research* with a view to enhancing data linkage. A prior consultation revealed that uncertainty about the legalities and public acceptability of data sharing and linkage ranked first among the identified obstacles to data linkage.[48]

1.49 The Caldicott Review 2 called for a cultural change in the health and social sector in order to strike a new balance between sharing and protecting information, covering both anonymised and personal data. While the 1997 Caldicott review emphasised preventing misuse of patient information outside clinical control, the second review was primarily concerned with the lack of confidence of many clinicians about when it is safe to share information. Despite a perceived consensus among professionals and the public that safe and appropriate sharing in the interests of the individuals' direct care should be the rule, the review panel observed that a "risk-averse" culture generally prevailed:

> Over recent years, there has been a growing perception that information governance was being cited as an impediment to sharing information, even when sharing would have been in the patient's best interests.[49]

1.50 This does not mean that individuals have lower expectations about confidentiality. Criticism of insufficient information sharing among professionals had gone hand in hand with criticisms that the system did not protect confidential data and information sufficiently. Against this background, the review put forward a number of recommendations to the Government in order to improve data sharing. These included recognising that the duty to share information can be as important as the duty to protect patient confidentiality, changing the learning about information governance and reforming the approach to breaches.

1.51 Improvement of data sharing between health and care professionals and NHS organisations is also one of the objectives of the digitalisation strategy pursued by the NHS. In line with the EU Digital Agenda for Europe 2010-2020, the NHS plans to become paperless by 2018, with hospitals being able to share digital

[46] According to the Shakespeare review, increased penalties in cases of the misuse of data are more innovation friendly because pre-emptive action for data protection purposes, including eg limiting the access to data through an accreditation process, could prevent the re-use of data and ultimately stifle innovation.

[47] UK Administrative Data Research Network, *Improving Access for Research and Policy* (Administrative Data Taskforce, December 2012).

[48] Scottish Government, *Joined up data for better decisions: A strategy for improving data access and analysis* (2012) p 7, at http://www.scotland.gov.uk/Resource/0040/00408151.pdf (last visited 30 August 2013).

[49] F Caldicott, *Information: to share or not to share? The Information Governance Review* (March 2013) p 9.

data from April 2014.[50]

1.52 The Cabinet Office Minister Francis Maude announced in 2012 his intention to set up fast-track procedures in order for Government and public sector organisations to collect debt more efficiently.[51] It was envisaged that sharing information would, for example, help with the assessment of a debtor's ability to pay or help collectors know when debtors owe money to another department. In the Spending Round 2013, the Government announced that it will "establish a centre of excellence to reduce the complexity of sharing data between services, and will explore options for new legislation to that end."[52]

Sharing between whom?

1.53 Our primary concern in this consultation paper is data sharing between public bodies. That would cover data sharing between a public body and a private body processing data on behalf of a public body. Given the range of contractual arrangements now involved in delivering public services, there may be doubts about whether a particular body should be characterised as public or private.

1.54 It may be that there are particular further issues relating to the sharing of data between public bodies and individuals, or private or third sector bodies. There may also be further issues where a UK public body wishes to share data with foreign or transnational bodies or other bodies within the European Union. Although our focus is on data sharing between public bodies, we would nonetheless be interested to be informed of additional public to private sharing issues.

Outline of the consultation paper

1.55 This consultation paper is divided into five chapters.

(1) Introduction.

(2) The second chapter briefly outlines the claimed advantages of data sharing and, conversely, the principled objections based on privacy.

(3) The third chapter sets out the restrictions on data sharing.

(4) The fourth chapter considers the powers of public bodies to share data.

[50] Department of Health, *The Power of Information: Putting all of us in control of the health and social care information we need* (May 2012); see also Secretary of State for Health Jeremy Hunt's announcements of 16 January 2013, at https://www.gov.uk/government/speeches/16-january-2013-jeremy-hunt-policy-exchange-from-notepad-to-ipad-technology-and-the-nhs (last visited 30 August 2013). European Commission, *the Digital Agenda for Europe 2010-2020*, at http://ec.europa.eu/information_society/digital-agenda/index_ en.htm (last visited 30 August 2013).

[51] "Government revises plan for greater data-sharing between agencies", *The Guardian,* 24 April 2012, at http://www.guardian.co.uk/politics/2012/apr/23/government-plan-share-personal-data (last visited 30 August 2013). See also the keynote speech delivered on 15 October 2012 by Minister for the Cabinet Office Francis Maude at a Dods conference, at https://www.gov.uk/government/speeches/tackling-debt-owed-to-government-speech-by-francis-maude (last visited 30 August 2013).

[52] HM Treasury, *Spending Round 2013* (June 2013) para 1.31, at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/209036/spending-round-2013-complete.pdf (last visited 30 August 2013).

(5) The fifth chapter sets out a series of consultation questions.

1.56 Unlike other reports, consultation questions are presented in a separate chapter, as much relies on the practical input from stakeholders, distinct from any legal analysis.

CHAPTER 2
DATA SHARING: PRACTICAL ADVANTAGES AND PRINCIPLED CONCERNS

> There is a difficult balance to be struck between the undoubted advantages of wider exchange of information between Government Departments and the protection of personal data. The very real risks associated with greater sharing of personal data between Departments must be acknowledged in order for adequate safeguards to be put in place.[1]

2.1 In this chapter, we briefly describe some of the claimed benefits for data sharing by public bodies, and outline some of the principled objections to doing so. In neither case do we attempt to assess the claims made – that would be for a substantive law reform exercise, if one were to follow this project. But it would be meaningless to ask about obstacles to data sharing without some appreciation of the possible benefits that it could provide. Similarly, it would be wrong to characterise a check on data sharing as an "obstacle" if the data sharing it prevented could be illegitimate.

THE ADVANTAGES OF DATA SHARING

2.2 In 2002, the Performance and Innovation Unit report on *Privacy and Data Sharing* concluded that:

> there is great potential to make better use of personal information to deliver benefits to individuals and to society, including through increased data-sharing.[2]

Informed policy-making and improved provision of public services

2.3 Data sharing may help public authorities make more informed policy decisions to the benefit of society. It is also necessary in the provision of many services. The availability of evidence from a wide range of sources and greater quantities of data, which can reveal new correlations and patterns, can help public bodies tackle multi-dimensional challenges. Such data sharing can also support a joined-up approach to the provision of public services.[3]

1 Protection of Private Data, Report of the Justice Select Committee (2007-2008) HC 154 para 29.

2 Performance and Innovation Unit, *Privacy and data-sharing: The way forward for public services* (April 2002), at http://ctpr.org/wp-content/uploads/2011/03/Privacy-and-data-sharing-the-way-forward-for-public-services-2002.pdf (last visited 30 August 2013).

3 R Thomas and M Walport, *Data Sharing Review Report* (July 2008) para 2.15; Performance and Innovation Unit, *Privacy and data-sharing: The way forward for public services* (April 2002) p 76; Department of Health, *The Power of Information: Putting all of us in control of the health and care information we need* (May 2012) p 6.

2.4 The ability to share and process data concerning different potential causes of illness is said to facilitate better preventative strategies in the field of public health by improving decision-makers' understanding of the underlying causes. Such analysis can also inform equality policies and strategies.[4]

2.5 Action to secure child protection and alleviate child poverty and the management of families with multiple problems by social services may also be facilitated by data sharing, which can contribute to a joined-up approach. The analysis of large datasets may help to improve policy making and activity by public bodies in relation to taxation, fraud and debt collection. Law enforcement and public protection may also be enhanced by data sharing.[5]

2.6 Collecting performance data on a local and national level may enable public bodies to "help benchmark performance, facilitate improvement and promote accountability". [6]

2.7 Improved information may allow public bodies to understand better the populations they serve. Processing data can also enable public bodies to more accurately target services to the needs of smaller groups. Services can be more easily personalised. Effective information sharing also allows regulators and other organisations to prevent issues from escalating at an earlier stage.[7]

Emergency planning and response

2.8 In emergency situations such as terrorist incidents or natural disasters, relevant data is often required quickly from multiple sources.

[4] See Department of Health, *The power of information: putting all of us in control of the health and social care information we need* (May 2012) p 4. Note also the work of the Social Mobility Transparency Board which aims to improve the sharing of data between the Department for Education, the Department for Business, Innovation and Skills and HMRC with a view to assessing the progress students make between starting school, leaving school and their destinations after school.

[5] Such as plans to link children's NHS Accident and Emergency records with registers held by local authority children's services departments (F Caldicott, *Information: to share or not to share? The Information Governance Review* (March 2013) p 93; Department of Health, *New child abuse alert system for hospitals announced*, 27 December 2012, at http://www.dh.gov.uk/health/2012/12/abuse-alert-system/, last visited 30 August 2013). See also initiatives such as "Mash" (see para 1.43 above); McKinsey Global Institute, *Big Data: The next frontier for innovation, competition, and productivity* (May 2011), at http://www.mckinsey.com/mgi/publications/big_data/index.asp (last visited 30 August 2013); "Government revises plan for greater data-sharing between agencies", *The Guardian,* 24 April 2012; keynote speech delivered on 15 October 2012 by Minister for the Cabinet Office Francis Maude at a Dods conference; R Thomas and M Walport, *Data Sharing Review Report* (July 2008) para 2.5. In the area of national security, see HM Government, *Data protection and sharing – Guidance for emergency planners and responders,* at http://security.homeoffice.gov.uk/news-publications/publication-search/general/lessons-learned (last visited 30 August 2013).

[6] E Munro, *The Munro Review of Child Protection: Final report. A child-centred system* (May 2011) para 19; see also McKinsey Global Institute, *Big Data: The next frontier for innovation, competition and productivity* (May 2011) p 5.

[7] McKinsey Global Institute, *Big Data: The next frontier for innovation, competition and productivity* (May 2011) p 5; Performance and Innovation Unit, *Privacy and data-sharing: The way forward for public services* (April 2002) p 3; Department of Health, *The power of information: Putting all of us in control of the health and care information we need* (May 2012) p 4.

Research and the knowledge-based economy

2.9 It is said that data sharing can allow the full value of existing data to be realised with widespread public benefits. It encourages research based on public sector activities. As the economy is increasingly based on the use of information and the production of knowledge, the Performance and Innovation Unit argued that effective data sharing may provide "considerable knock-on benefits for the transition to a knowledge economy". Such research may have significant economic value.[8]

2.10 Data sharing is said to contribute to improving the quality and consistency of data across public bodies when large datasets are merged. The organisations that share data not only benefit from the greatly increased analytical power of the combined data, but also learn from each other to improve their performance.[9]

2.11 Administrative data is routinely collected by public bodies. The Administrative Data Taskforce argues that the anonymised use of such data could "provide a robust UK-wide evidence base to inform research, thereby guiding the development, implementation and evaluation of policy". Administrative data can be used in research projects by government departments. For example, such research can address social mobility by linking data on education, training, employment, unemployment, income and benefits; inform policies to tackle poverty by linking data on housing conditions, health, incomes and benefits; construct indicators for the provision of social care for children by linking childcare, parental employment and social background; and study reoffending by linking data on health, income and benefits.[10]

Efficiency and cost effectiveness

2.12 Where public bodies need to collect data, it can be more efficient to obtain the data from a public body that has already collected the data, rather than go back to the data source. Shared datasets can reduce search and processing times and therefore help to speed up decision-making. Obstacles to data sharing, even where the sharing is ultimately permitted, can increase the costs of sharing, impose onerous requirements on it or delay the process. Sometimes these costs can undermine the value of sharing the data at all.[11]

[8] Department for Business, Innovation and Skills, *Market Assessment of Public Sector Information written by Deloitte* (May 2013), at https://www.gov.uk/government/publications/public-sector-information-market-assessment (last visited 30 August 2013); R Thomas and M Walport, *Data Sharing Review Report* (July 2008) para 2.28; Performance and Innovation Unit, *Privacy and data-sharing: The way forward for public services* (April 2002) para 1.09; McKinsey Global Institute, *Big Data: The next frontier for innovation, competition and productivity* (May 2011).

[9] Scottish Government, *Joined up data for better decisions: A strategy for improving data access and analysis* (2012) p 7; the UK Administrative Data Research Network, *Improving Access for Research and Policy* (Administrative Data Taskforce, December 2012) p 1.

[10] The UK Administrative Data Research Network, *Improving Access for Research and Policy* (Administrative Data Taskforce, December 2012) pp ii and 1.

[11] The UK Administrative Data Research Network, *Improving Access for Research and Policy* (Administrative Data Taskforce, December 2012) p ii.

2.13 A survey published by the Guardian in January 2013 involving 33,000 public servants found that 90% of respondents had a business requirement to share files, but 71% said they were restricted from doing so.[12]

2.14 Data sharing may also cut the administrative burden on individuals, who would not have to provide the same information to different public bodies.

2.15 Effective data sharing may also be necessary to meet the expectations of the public concerning the use of data in the effective and efficient provision of public services.[13]

2.16 Changes to the way that public services are delivered have increased demands for data sharing. If a public service once delivered in house is now in part delivered by private or third sector contractors, information flows which hitherto took place within a single body now require sharing of data between a number of different bodies. Data about the private or third sector contractors delivering those public services may also need to be shared with other public bodies to coordinate their activities.

Transparency

2.17 Data sharing may ultimately improve transparency in public services. Data, when made public, help individuals to make informed choices about the use of public services. Businesses may also create value from such data, fostering economic growth and job creation.[14]

[12] D Jellinek, "Why sharing data can save services", *The Guardian*, 23 January 2013.

[13] Performance and Innovation Unit, *Privacy and data-sharing: The way forward for public services* (April 2002) p 2; R Thomas and M Walport, *Data Sharing Review Report* (July 2008) para 1.4.

[14] See V Bogdanor, *Freedom of information: the constitutional aspects* in A McDonald and G Terrill (ed), *Open Government – Freedom of information and privacy* (1998); K O'Hara, *Transparent Government, Not Transparent Citizens: A Report on Privacy and Transparency for the Cabinet Office,* at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61280/transparency-and-privacy-review-annex-b.pdf (last visited 30 August 2013); Department of Health, *The power of information: Putting all of us in control of the health and social care information we need* (May 2012); McKinsey Global Institute, *Big Data: The next frontier for innovation, competition, and productivity* (May 2011).

2.18 The transparency and open data strategy calls for access to anonymised data about public services' performance.[15] Transparency is supported by the Freedom of Information Act 2000, recently amended to facilitate the use of datasets; the Environmental Information Regulations 2004; the Re-use of Public Sector Information Regulations 2005; and the 2009 UK INSPIRE Regulations, which promote the publication of information held by public bodies.[16]

2.19 It is worth noting that these claims are not un-contested. Critics accuse governments of making exaggerated claims for data sharing.

PRINCIPLED PRIVACY CONCERNS ABOUT DATA SHARING

2.20 Even if there *are* practical advantages to society of sharing data, there are also claims of principle which contest sharing. These are ultimately founded on a value judgement about the importance of privacy to individuals.

2.21 The concept of privacy is notoriously difficult to define. Both the Younger Report (1972) and the Lindop Report (1978) declined to attempt a definition, although the latter noted that there was an extensive range of attitudes towards the proper definition of "privateness", in relation to "data privacy", which varied by individual characteristics and personality, social and cultural factors, time and place, and the purposes or conditions of data collection and use in a particular case.[17]

[15] Cabinet Office*, Open Data. White Paper*. *Unleashing the Potential* (June 2012), at https://www.gov.uk/government/publications/open-data-white-paper-unleashing-the-potential (last visited 30 August 2013). See Cabinet Office's website and in particular https://www.gov.uk/government/policies/improving-the-transparency-and-accountability-of-government-and-its-services (last visited 30 August 2013); see also letters sent by the Prime Minister to government departments in 2010 and 2011 instructing them to release data on a number of areas, including health, education, crime and justice: http://www.number10.gov.uk/news/letter-to-government-departments-on-opening-up-data/ and http://www.number10.gov.uk/news/letter-to-cabinet-ministers-on-transparency-and-open-data/ (last visited 30 August 2013); consultation *Making Open Data Real,* at http://www.data.gov.uk/sites/default/files/Open%20Data%20consultation%20August%202011.pdf (last visited 30 August 2013); the *Open Public Services White Paper,* at http://files.openpublicservices.cabinetoffice.gov.uk/OpenPublicServices-WhitePaper.pdf (last visited 30 August 2013).

[16] Protection of Freedoms Act 2012, s 102; SI 2004 No 3391; SI 2005 No 1515; and SI 2009 No 3157.

[17] See generally: R Wacks, "The Poverty of Privacy" (1980) 96 *Law Quarterly Review* 73; G Marshall, "The Right to Privacy: A Sceptical View" (1975) 21 *McGill Law Journal* 242; D Feldman, "Secrecy, Dignity or Autonomy? Views of Privacy as a Civil Liberty" (1994) 47 *Current Legal Problems* 41, 49; J Cohen, "What is Privacy for?" (2012) 126 *Harvard Law Review* 1904; R A Posner, "The Right of Privacy" (1978) 12 *Georgia Law Review* 393; Report of the Committee on Privacy (1972) Cmnd 5012 (Younger Report) p 5 (which focussed on press intrusion, and did not consider public bodies); Report of the Committee on Data Protection (1978) Cmnd 7341 (Lindop Report) p 10.

2.22 Privacy has nonetheless given rise to an extensive literature, especially in the United States. This literature identifies a number of principled concerns related to the value of privacy.[18] Data sharing by public bodies in some contexts may threaten this value, while in other cases it may be harmless. It has been accepted by some proponents of greater data sharing that data sharing should not be seen as an "unconditional good" without considering its impact on privacy.[19]

2.23 A number of different concerns for the protection of privacy and its underlying value can be identified.

A right to be let alone

2.24 Early privacy advocates formulated privacy as the right "to be let alone". Privacy concerns were rooted in a desire to protect the inviolability, dignity and convenience of individuals and their affairs from undesired publicity where the community has no legitimate concern in those affairs. The concerns built on notions of propriety and the appropriate division between public and private life.[20]

2.25 This concern for privacy first arose out of intrusive newspaper coverage of the details of individual sexual relations. Early concerns about privacy were reactions against the "prurient curiosity" displayed by newspapers and the trivialisation of public discussion this threatened. However, such concerns did not originally extend to state institutions. The earliest privacy advocates in fact argued for an exception to the right of privacy where it would prohibit communications of any private matter in the courts, legislative bodies or public or quasi-public bodies.[21]

Protection of interests in reputation, peace, or intangible property

2.26 Four interferences with the right to privacy have been identified in the development of the United States tort of invasion of privacy:

(1) intrusion upon an individual's seclusion or solitude;

(2) public disclosure of private facts;

(3) negative publicity about an individual;

(4) appropriation of an individual's name or likeness.[22]

[18] R Wacks, *Privacy* (1993); F Schoeman, *Philosophical Dimensions of Privacy: an Anthology* (1984); J C Innes, *Privacy, Intimacy and Isolation* (1992); J W DeCew, *In Pursuit of Privacy: Law, Ethics and the Rise of Technology* (1997); Law Reform Commission Report on Privacy: Surveillance and the Interception of Communications (LRC57-1998) paras 1.9 to 1.16; R Wacks, *Personal Information* (1989).

[19] Surveillance: Citizens and the State, Second Report of the House of Lords Constitution Committee (2008-2009) HL 18 para 36; R Thomas and M Walport, *Data Sharing Review Report* (July 2008).

[20] The seminal founding text for privacy was an 1890 article written by Samuel Warren and Louis Brandeis: S Warren and L Brandeis, "The Right to Privacy" (1890) 4 *Harvard Law Review* 193 pp 205 to 215.

[21] S Warren and L Brandeis, "The Right to Privacy" (1890) 4 *Harvard Law Review* 193 pp 196 to 220.

[22] W Prosser, "Privacy" (1960) 48 *California Law Review* 383, 389.

2.27 The privacy interests underlying these torts included the protection of reputation and intangible property and protection against emotional distress. These views became highly influential in the development of the United States tort of invasion of privacy and continue to influence ideas in English-speaking legal systems.[23] Data sharing may impact on these interests.

Human dignity

2.28 The concept of privacy has also been understood as supported by a dignitarian approach. On that view, privacy is the protection of individual independence, dignity and integrity, which an intrusion into privacy can demean. Dignitarians argue that freedom from certain kinds of intrusion is inherent in individuality. Personal freedom and dignity require a degree of personal isolation within the control of an individual and freedom from unrestrained intrusion, especially by state institutions. The ease of storage, correlation and retrieval of personal data by government increases fears of intrusion.[24]

Seclusion of or limited acquaintance with individuals

2.29 Privacy has been understood to protect a limited acquaintance with individuals and an interest in seclusion. Privacy is argued to be a desirable state of affairs in itself. The state of privacy has been described as "the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited."[25]

2.30 The value of privacy is understood as the value of a degree of seclusion or anonymity. Others have also stressed the psychological benefits of privacy.[26] This is threatened by inappropriate data sharing.

[23] W Prosser, "Privacy" (1960) 48 *California Law Review* 383; see *Prosser on Torts* (1962 3rd ed) and his work on the *Second Restatement of Torts* (1965); E Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 *New York University Law Review* 962, 964.

[24] E Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 *New York University Law Review* 962.

[25] H Gross, "The Concept of Privacy" (1967) 42 *New York University Law Review* 34, 36; see generally, R A Posner, "Privacy, Secrecy and Reputation" (1979) 28 *Buffalo Law Review* 1; R Gavison, "Privacy and the Limits of Law" (1980) 89 *Yale Law Journal* 421; A Moore, "Privacy: Its Meaning and Value" (2003) 40 *American Philosophical Quarterly* 215: W Prosser, "Privacy" (1960) 48 *California Law Review* 383, 389.

[26] S M Journard, "Some Psychological Aspects of Privacy" (1966) 31 *Law and Contemporary Problems* 307; O M Ruebhausen and O G Brim, "Privacy and Behavioural Research" (1965) 65 *Columbia Law Review* 1184.

Intimacy and managing social relationships

2.31 Privacy has also been acknowledged as important in creating the space needed for people to develop relationships of varying degrees of intimacy. It is argued that privacy is the necessary context for that intimacy, which has a high importance for personal development and flourishing. Respect for the privacy of individuals, by state institutions and private individuals, is an essential precondition for relationships of greater intimacy. Relationships of greater intimacy are based on the mutual relinquishment of such entitlement for the sake of each other to create reciprocal relationships. Without a right to keep certain kinds of information private, there would not be scope for sharing intimate details within relationships.[27] Intrusive data sharing may therefore reduce the opportunities for building genuine intimate relationships.

2.32 Control over information serves an entitlement to "dignity and autonomy within a social circle". Privacy allows individuals to control their social boundaries and maintain relationships of "varying degrees of intimacy". Extensive data sharing may undermine this control of varying levels of intimacy. One further fear is the risk that the products of invasions of privacy may be used for purposes adverse to the individuals concerned and harm this form of dignity and autonomy.[28]

Control of dissemination, use and retention of personal information

2.33 Data sharing has implications for control over information. The value of privacy has been identified in the control of personal information. This has taken different forms. Some subjects are considered simply to be "nobody else's business" and are the proper subject for individual control. For others there is an interest in making only selective disclosures of information.[29]

> Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.[30]

[27] C Fried, "Privacy", (1968) 77 *Yale Law Journal* 475, 477 to 484; see generally C Fried, *An Anatomy of Values: Problems of Personal and Social Choice* (1971); C Fried, "Privacy", (1968) 77 *Yale Law Journal* 475; R Gerstein, "Intimacy and Privacy", in F Schoeman, *Philosophical Dimensions of Privacy: an Anthology* (1984); J Rachels, "Why Privacy is Important" (1975) 4 *Philosophy and Public Affairs* 323; J H Reiman, "Privacy, Intimacy, and Personhood" (1976) 6 *Philosophy and Public Affairs* 26; R Post, "The Social Foundations of Privacy: Community and Self in the Common Law Tort" (1989) 77 *California Law Review* 957, 974.

[28] D Feldman, "Secrecy, Dignity or Autonomy? Views of Privacy as a Civil Liberty" (1994) 47 *Current Legal Problems* 41, 51 to 62; Surveillance: Citizens and the State, Second Report of the House of Lords Constitution Committee (2008-2009) HL 18 para 102.

[29] D Feldman, "Secrecy, Dignity or Autonomy? Views of Privacy as a Civil Liberty" (1994) 47 *Current Legal Problems* 41, 53; E L Beardsley, "Privacy: Autonomy and Selective Disclosure" in Pennock and Chapman, *Privacy: NOMOS XIII* pp 56 to 70; see generally, R A Posner, "The Right of Privacy" (1978) 12 *Georgia Law Review* 393; G J Stigler, "An Introduction to Privacy in Economics and Politics" (1980) 9 *Journal of Legal Studies* 623; W Parent, "Privacy, Morality and the Law" (1983) 12 *Philosophy and Public Affairs* 269.

[30] C Fried, "Privacy", (1968) 77 *Yale Law Journal* 475, 482.

2.34 Concern for control over the retention of information has also driven proposals for a "right to be forgotten".[31]

2.35 The large amounts of data held by public bodies give rise to concerns about the security of that information. Human error and theft have accounted for numerous high profile losses of data by public bodies have reinforced such concerns.[32] Developing larger and more sophisticated databases through data sharing increases the potential harm of data leaks and the potential for individuals to lose control of their information.

Autonomy

2.36 The concept of privacy also has a close affinity with ideas about autonomy. The right to privacy "comes closer than any other right to the essence of liberty itself".[33] This finds its clearest expression in literature on substantive privacy protections in US constitutional thought.

2.37 The concept of privacy protection rests on a particular social structure and ethic. This is expressed as a liberal conception resistant to a "normalizing state" dictating life choices. The exercise of choice in individual preferences can be inhibited by publicity. According to this view, privacy controls seek to place "limits on the extent of control and direction that the state exercises over the day-to-day conduct of individual lives". This is based on a fear of enforced standardisation and uniformity. The concern of privacy protections is, on this view, to limit the impact of state action on the lives of individuals. Any substantial increase in state power to control private matters resulting from increased data sharing is understood as a threat to autonomy in this sense. Improvements in technology and the sheer amount of data mean that a risk of government misuse of data is a greater threat than was the case historically.[34]

[31] E Reid, "Data Protection: the Right to be Forgotten", (2012) 114 *Human Rights Updater* 14; J L Gray, "A Right to be Forgotten: The Far-reaching Implications" (2011) 8(5) *Data Protection Law and Policy* 14; A Roosendaal, "Right to be Forgotten vs Need to be Remembered" (2012) 22(6) *Computers and Law* 10.

[32] Liberty's website, *Databases*, at http://www.liberty-human-rights.org.uk/human-rights/privacy/databases/index.php (last visited 30 August 2013); Cabinet Office, *Data Handling Procedures in Government: Final Report* (June 2008); R Thomas and M Walport, *Data Sharing Review Report* (July 2008) p I and para 1.13; "Extent of data losses is revealed", *BBC News*, 19 August 2008, at http://news.bbc.co.uk/1/hi/uk_politics/7570611.stm (last visited 30 August 2013); "Government's record year of data loss", *The Telegraph*, 6 January 2008, http://www.telegraph.co.uk/news/politics/1574687/Governments-record-year-of-data-loss.html (last visited 30 August 2013).

[33] D Feldman, "Secrecy, Dignity or Autonomy? Views of Privacy as a Civil Liberty" (1994) 47 *Current Legal Problems* 41; see generally, J Hirschleifer, "Privacy: its Origin, Function and Future" (1980) 9 *Journal of Legal Studies* 649; see also Surveillance: Citizens and the State, Second Report of the House of Lords Constitution Committee (2008-2009) HL 18 paras 100 and 144.

[34] J Hirschleifer, "Privacy: its Origin, Function and Future" (1980) 9 *Journal of Legal Studies* 649, 649; D Feldman, "Secrecy, Dignity or Autonomy? Views of Privacy as a Civil Liberty" (1994) 47 *Current Legal Problems* 41, 53; J Rubenfeld, "The Right to Privacy" (1989) 102 *Harvard Law Review* 737 pp 784 to 807; R Thomas and M Walport, *Data Sharing Review Report* (July 2008) para 1.6.

Safeguarding social norms

2.38 The particular areas that are considered private are at least partially determined by convention in society. It is argued that privacy safeguards the "rules of civility" in a community. Personality, as well as dignity, is harmed by interferences with privacy. Such social norms play a valuable role in constituting both the individual and the community. The rules of civility shape personality and so their violation can damage it.[35] There is a role on this account for community norms to shape the privacy protections of individuals. Ideas about privacy are to some extent culturally contingent and may change over time. There is a tension between this account and other accounts that build privacy on a different understanding of the relationship between the individual and society.

Liberal democracy

2.39 Privacy is also understood to have an important role in constituting and sustaining liberal democracy. Privacy is important for personal expression and choice. It is also valuable for fostering creativity and innovation.[36]

2.40 Privacy is seen as indispensible to liberal democracy because it protects a space for the development of "informed and reflective citizenship" from public and commercial pressures which encourages conformity and predictability. Citizenship requires privacy to flourish. Innovation, which is an important feature of liberal democracy, requires privacy to encourage "the processes of play and experimentation" that foster it. Self-determination and critical perspectives, which are required for self-government, are diminished in the absence of privacy.[37]

[35] C Fried, "Privacy" (1968) 77 *Yale Law Journal* 475, 487; R Post, "The Social Foundations of Privacy: Community and Self in the Common Law Tort" (1989) 77 *California Law Review* 957.

[36] Surveillance: Citizens and the State, Second Report of the House of Lords Constitution Committee (2008-2009) HL 18 para 14; F Schoeman, Privacy and Social Freedom (1992); M A Weinstein, "The Uses of Privacy in the Good Life" (1971) 13 *Nomos XIII* 88; J Cohen, "What is Privacy for?" (2012) 126 *Harvard Law Review* 1904.

[37] J Cohen, "What is Privacy for?" (2012) 126 *Harvard Law Review* 1904, 1915 to 1912.

2.41 The use of data in networks may present a particular risk. Networks may subtly shape a person's beliefs about and understandings of politics, society and economics. The ability to process large amounts of data which allow the predictive analytical targeting of consumers can influence consumer preferences and the way in which knowledge is produced, for example by only suggesting certain options or giving particular ideas greater prominence. Although technology itself is "policy blind", there might be concerns about the governance and use of technology. Research agendas are not neutral and reflect the underlying ideological and cultural assumptions of those who develop them. This can ultimately threaten political dialogue where such processes are depended upon to generate knowledge. Some fear that some techniques involving "Big Data" in particular could facilitate intrusive and extensive profiling. Concerns have also been expressed about the potential of large databases to be used for data mining and data profiling.[38] This creates risks for effective citizenship in a liberal democracy.

DATA SHARING WITHIN THE STATE

2.42 The principles underlying concern for privacy are to some extent intertwined or overlapping. Inappropriate data sharing may threaten the values expressed in the concept of privacy. Equally, appropriate data sharing may bring benefits and preserve privacy. Any attempt to assess the legal obstacles to data sharing must be aware of these concerns and balance them appropriately against the benefits of data sharing.

2.43 Data sharing between public bodies may raise more subtle privacy concerns. It is not merely a question of whether information should be shared with the state but also with which parts of the state information should be shared. Data sharing raises questions of institutional design and the appropriate relationship between different public bodies as well as the relationship between the state and the individual. It raises issues concerning the proper division of knowledge about individuals between public bodies with different functions or roles.

2.44 This requires a careful analysis of the institutions that share data. The possession of information is dispersed among public bodies and between public and private bodies. This gives rise to complex and dynamic relationships which must be taken into account when considering issues of institutional design and the relationships between public bodies, including dataflows. "Information asymmetry" can also influence the balance of power between bodies in ways that may affect privacy.[39]

[38] J Cohen, "What is Privacy for?" (2012) 126 *Harvard Law Review* 1904, 1913 to 1920; "Big Data" refers to datasets so large or complex that it is beyond the ability of ordinary software to manage and analyse the data. Big Data techniques use trends and patterns in Big Datasets to draw inferences and make predictions. See McKinsey Global Institute, *Big Data: The next frontier for innovation, competition and productivity* (May 2011) p 1; Liberty's website, *Databases*, at http://www.liberty-human-rights.org.uk/human-rights/privacy/databases/index.php (last visited 30 August 2013). Data mining consists of identifying unusual patterns in large datasets of personal information. One concern is that the results of data mining could be used to inform surveillance priorities without independent evidence to support the need for such surveillance.

[39] On information asymmetry generally, see C Scott, "Analysing Regulatory Space: Fragmented Resources and Institutional Design" (2001) *Public Law* 329, 330 to 336.

2.45 Most theorising about privacy relies on a monolithic concept of the state. Such a concept of the state does not take into account the divisions of power and responsibility between the different institutions and bodies that make up the state. Nor does it consider the nature of the relationships between public bodies internal to the state and how those relationships impact upon the collection of data from diverse private bodies.[40]

2.46 It might be appropriate for some public bodies to hold a great deal of highly sensitive information, such as medical records in the NHS, but it might be undesirable for information to be held by or shared with other bodies performing different functions. An assessment of the obstacles to data sharing must be sensitive to the diverse functions of public bodies which may wish to share data and the environment within which they operate.[41]

[40] C Scott, "Analysing Regulatory Space: Fragmented Resources and Institutional Design" (2001) *Public Law* 329, 347.

[41] See eg A Kennedy, "Winning the information wars: collecting, sharing and analysing information in asset recovery investigations" (2007) *Journal of Financial Crime* 372; for an example from Canada, see D Murphy, "Disclosure and sharing of sensitive information: revisiting risk in co-operating regulatory regimes" (2006) *Journal of Financial Crime* 420.

CHAPTER 3
RESTRICTIONS ON DATA SHARING

INTRODUCTION

3.1 However extensive the power a public body has to share data, it can only do so in accordance with the law restricting data sharing. In this chapter, we set out in broad terms those parameters, under the following headings:

(1) the Data Protection Act 1998; and

(2) the law of confidence, as reshaped by the right to respect for private life set out in article 8 of the European Convention on Human Rights.

3.2 These sources of regulation differ in important respects. In terms of subject matter, the private law of confidentiality, developed by the courts, protects information characterised as "confidential" or "private"; whereas the Data Protection Act 1998 deals with "personal data". Similarly, procedure and remedies in respect of confidentiality are those available as part of the general law, including damages and injunctions. The Data Protection Act 1998 has its own adjudication procedure by way of a tribunal and data protection is overseen by the Information Commissioner. However, these two sources also display similarities, both drawing on European Union law and the European Convention on Human Rights.

3.3 Restrictions on the disclosure of information may also come from contractual clauses and employment obligations.

3.4 These rules are complemented by professional obligations, which are not legally binding but may have serious consequences for practitioners who breach them. These rules may be more stringent than the Data Protection Act 1998 in respect of data sharing. For example, solicitors must abide by a duty of confidentiality regarding the affairs of their clients even after the end of the retainer and the death of their client, subject to exceptions.[1] Similarly, registered doctors must respect patients' right to confidentiality, including after their death, subject to exceptions.[2]

3.5 There may be greater risks of professional consequences when sharing information incorrectly in a way that could breach confidentiality than risks of professional consequences for not sharing information.[3]

[1] Eg when disclosure may be justified to prevent a client or a third party committing a criminal act that the solicitor reasonably believes likely to result in serious bodily harm, or when the threat to a child's life or health, both mental and physical, is sufficiently serious (Solicitors Regulation Authority, *Code of Conduct* (2011)).

[2] General Medical Council, *Confidentiality* (2009) p 30 onwards. Note that s 38 of the Freedom of Information (Scotland) Act 2002 includes a deceased person's medical records within the definition of personal information.

[3] C Bessant, *The duty of confidence* in C Bessant (ed) *Information Sharing Handbook* (2009) p 128.

3.6 In addition to these rules, data sharing may be regulated by non-legally binding guidance and data sharing agreements.

3.7 Guidance on data sharing has been released by the Information Commissioner's Office[4] and the Ministry of Justice,[5] as well as in specific sectors, including health and home affairs.[6] Although guidance has the merits of clarifying legal issues, the quantity of guidance may be seen as a source of confusion. In addition to its volume, guidance is sometimes criticised for its overly theoretical or legal-oriented approach, which does not meet the fact-specific questions asked by practitioners.[7]

3.8 A data sharing agreement is a set of common rules between organisations involved in a data sharing initiative. It usually specifies the basis for sharing, gives precise advice about which datasets may be shared, the rules for the retention and deletion of shared data items and sets out the data quality requirements and the technical and organisational security arrangements.[8] In the absence of such agreements, data sharing may suffer critical delays, for example in emergency situations as contemplated under the Civil Contingencies Act 2004.

DATA PROTECTION ACT 1998

3.9 The Data Protection Act is the main piece of legislation applicable to data sharing.

3.10 Attempts to regulate data collection and processing in the interests of privacy, in the light of the increasing use of computers, go back to the late 1960s. These included activity both at the international level and a number of proposals for domestic legislation.[9] In 1972, the Younger Committee put forward a series of principles to regulate the use of personal data held on computers.[10] In 1978, the Lindop Committee's report[11] recommended legislation, and a white paper was

4 Information Commissioner's Office, *Data sharing code of practice* (May 2011), at http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx (last visited 30 August 2013).

5 Ministry of Justice, *Public Sector Data Sharing: Guidance on the Law*, annex H to the *Data sharing protocol* p 19, at http://www.justice.gov.uk/downloads/information-access-rights/data-sharing/annex-h-data-sharing.pdf (last visited 30 August 2013).

6 Home Office, *Information sharing for community safety: Guidance and practice advice* (2010), at https://www.gov.uk/government/publications/information-sharing-for-community-safety (last visited 30 August 2013).

7 R Thomas and M Walport, *Data Sharing Review Report* (July 2008) paras 5.31 and 5.32.

8 Information Commissioner's Office, *Data sharing code of practice* (May 2011) p 40.

9 See eg A White QC and C Darwin, *Relationship between freedom of information and data protection* in *Freedom of Information Handbook* (3rd ed) p 241.

10 Report of the Committee on Privacy (1972) Cmnd 5012.

11 Report of the Committee on Data Protection (1978) Cmnd 7341.

published in 1982.[12] Building on this and prompted by a Council of Europe Convention,[13] the Data Protection Act 1984 was passed.

3.11 In 1995, EC legislation followed with the General Data Protection Directive, which built on the Council of Europe convention.[14] The Directive had a twofold objective: facilitating the flow of personal data across the EU, which was seen as being hindered by the differing levels of rights protection across the EU, and safeguarding the fundamental rights of individuals, notably the right to privacy.

3.12 This Directive was implemented by the Data Protection Act 1998, which came into force on 1 March 2000.

The information concerned

Automatically processed and structured information

3.13 Data covered by the Data Protection Act 1998 include the following:[15]

(1) All automatically processed information and information recorded with the intention that it should be processed. This category essentially covers electronic information, held for example on computers, mobile phones, memory sticks, and digital cameras.[16]

(2) Some manual records, namely information recorded as part of a relevant filing system. In order to be "relevant", a filing system must :

(a) constitute a "set" of information;

(b) be structured by reference to individuals or criteria relating to individuals; and

(c) be structured in such a way that specific information relating to a

[12] Data Protection: The Government's Proposals for Legislation (1982) Cmnd 8539.

[13] Convention 108 for the protection of individuals with regard to automatic processing of personal data, 28 January 1981, at http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm (last visited 30 August 2013). The Convention entered into force on 1 October 1985, for the UK on 1 December 1987.

[14] General Data Protection Directive 95/46/EC Official Journal L 281 of 23.11.95 p 31. The Directive was adopted on 24 October 1995. The deadline for transposition was 24 October 1998. This EU legislation is currently under review, following the proposal for a regulation put forward by the European Commission in 2012 (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) COM(2012)11 final).

[15] Data Protection Act 1998, s 1(1).

[16] Data must be stored on a computer and not just created on one, ie a hardcopy file typed on a computer (but not stored) is not caught: *Smith v Lloyds TSB Bank plc* [2005] EWHC 246 (Ch).

particular individual is readily accessible.[17]

(3) "Accessible records", defined in section 68 and schedules 11 and 12 as health records, educational records and accessible public records, for example local authority housing records or social services records.

(4) Any other recorded information held by a "public authority".[18]

Personal data

3.14 "Personal data" are concerned with living natural persons, not legal persons.[19] Personal data are defined as data which relate to an individual who can be directly identified from those data (for example, by name), or from those data when combined with other information in the possession or likely to come in the possession of the data controller. They also include any expression of opinion about an individual and any indication of the intentions of the data controller or any other person in respect of the individual.

3.15 In *Durant v Financial Services Authority*,[20] the Court held that for a datum to be personal, it must have affected the subject's privacy in personal, family, business or professional life, as opposed to relating to a life event which did not compromise privacy. In this regard, two relevant indicators were whether the information was significantly biographical; and whether it had the data subject as its focus, rather than someone else. Although *Durant* has been largely criticised as difficult to reconcile with the case law of the Court of Justice of the EU[21] and impractical, it is still the law domestically.[22]

[17] In *Durant v Financial Services Authority (Disclosure)* [2003] EWCA Civ 1746, [2004] FSR 28, the Court of Appeal set a high bar for the relevant filing system test, holding that it must be "on a par with that provided by a computerised filing system," enabling identification of relevant information "with a minimum of time and costs". This interpretation has been criticised as overly restrictive and was subsequently nuanced by the Information Commissioner's Office guidance.

[18] As defined by the Freedom of Information Act 2000. Only the provisions on subject access, accuracy and rights of rectification and compensation are applicable to these data.

[19] Data Protection Act 1998, s 1(1).

[20] *Durant v Financial Services Authority* [2003] EWCA Civ 1746, [2004] FSR 28.

[21] As set out in particular in case C-101/01 *Criminal Proceedings against Lindqvist* [2003] ECR I-12971 at [24] and joined cases C-465/00 and C-138/01 *Rechnungshof* [2003] ECR I-4989 at [75].

[22] *Durant* was applied in *Johnson v Medical Defence Union Ltd* [2004] EWHC 2509 (Ch), [2005] 1 WLR 750 and *Smith v Lloyds TSB Bank plc* [2005] EWHC 246 (Ch). In *Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47, [2008] 1 WLR 1550, the House of Lords did not rely on *Durant*. In order to remedy this tension between domestic and EU law, the Information Commissioner's Office guidance on the definition of personal data has adopted a more expansive scope of "personal data". This is reportedly the interpretation which is followed by practitioners (D Welfare, "Clarifying the scope of personal data" (2012) 12(7) *Privacy and Data Protection* 7).

3.16 The risk of combination of data means it is not always straightforward to distinguish between anonymised data and personal data.[23] In order to assess the risk of "re-personalising" anonymised data, the Information Commissioner put forward a test based on the existence of a "motivated intruder", reasonably competent and diligent, having access to free resources. Since information technology developments facilitate the combinations of data, and the growing amount of available data makes it easier to re-personalise data, the assessment of the risk of re-personalisation should be carried out periodically.[24]

3.17 Because it is difficult to draw a bright line between anonymised and personal data, some practitioners have recommended the creation of a third category of data, "potential personal data" or "data for limited disclosure", subject to specific rules of protection.[25]

Sensitive personal data

3.18 Additional requirements apply to a sub-set of data, namely "sensitive personal data", as their misuse has a greater potential to harm individuals. They are defined as personal data consisting of information as to racial or ethnic origin, political opinions, religious and similar beliefs, trade union membership, physical or mental health, sexual life, and the commission or alleged commission of any offence or criminal proceeding.[26]

[23] See eg *Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47, [2008] 1 WLR 1550. It is worth noting that anonymous data do not lose their status because one organisation is able to make a link between these data and the individuals, as long as this organisation will not release information enabling such link to be made and have in place appropriate security measures. See *R (Department of Health) v ICO* [2011] EWHC 1430 (Admin), (2011) 155 (17) SJLB 31: in this case, the Department of Health declined to provide, at the request of a pro-life's group, anonymised statistical information regarding the number of patients who had late terminations on medical grounds, as they feared that publication would allow the public identification of vulnerable women and medical practitioners. The court held that anonymised data that would not lead to the identification of a living person were not personal data, even though individuals could be identified from the statistics taken together with the other information in the Department's possession. In the Upper-tier Tribunal judgement *All Party Parliamentary Group on Extraordinary Rendition v ICO* (2011) (mentioned in Welfare "Clarifying the scope of personal data" *in* (2012) 12(7) *Privacy and Data Protection*), the Tribunal similarly held that fully anonymised data remained personal data in the hands of the data controller as long as he can continue to identify the individuals involved but cease to be personal data in the hands of the recipient where the public cannot identify any individual from it. See also Information Commissioner Office, *Determining what is personal data* (2012) p 27, at http://www.ico.org.uk/ (last visited 30 August 2013); and Information Commissioner Office, *Proposed new EU General Data Protection Regulation: Article-by-article analysis paper* (12 February 2013) p 7.

[24] Information Commissioner's Office, *Anonymisation: managing data protection risk. Code of practice* (November 2012).

[25] See eg R Thomas and M Walport, *Data Sharing Review Report* (July 2008) p 37; F Caldicott *Information: to share or not to share? The Information Governance Review* (March 2013) p 55.

[26] Data Protection Act 1998, s 2. In *Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47, [2008] 1 WLR 1550, the House of Lords held that sensitive personal data is a subset of personal data.

Processing

3.19 The wide definition of "processing" [27] can include virtually anything that could be done with data. It includes for example obtaining data, loading data on an internet page, reading a piece of information on a computer screen, digitally storing information, using data and communicating information. Where a body shares data with another body, both "process" the data.

The limitations placed on the sharing of personal data

3.20 In a process of information sharing, at least two data controllers are involved and each of them has the duty to comply with the data protection principles. A data controller is the natural or legal person, such as a public authority, which alone or jointly with others determines the purposes and means of the processing of personal data.[28] Further, whenever legislation provides for the processing of data by a specific body, expressly or impliedly, the person required to process such data is the data controller.[29] Alongside data controllers, there may be a number of data processors, who are natural or legal persons which process personal data on behalf of the controller but they do not have any statutory obligations under the Act.[30]

Prior notification

3.21 The obligations in relation to data sharing include a duty of prior notification.[31] Data controllers must give a notification to the Commissioner specifying the so-called "registrable particulars", including a description of the personal data, of any recipient to whom the data are to be disclosed; and of the purpose(s) for which the data are to be processed. The notification should also include a general description of the measures to be taken in order to comply with the security requirements.

3.22 Such particulars should therefore include information on the public body to which information will be communicated, in a data sharing process.

The data protection principles

3.23 The eight data protection principles set out in schedule 1 part 1 of the Data Protection Act 1998 and explained in part 2 of schedule 1 form the core of data protection regulation, with which each controller must comply, subject to some

[27] Data Protection Act 1998, s 1(1).

[28] Data Protection Act 1998, s1(1). In order for the controller to be regulated by the Data Protection Act 1998 when processing personal data, he or she must be established in the UK or using equipment in the UK for processing the data otherwise than for the purposes of transit (Data Protection Act 1998, s 5(3)).

[29] Data Protection Act 1998, s 1(4).

[30] Data Protection Act 1998, s 1(1). On the difficulty to identify roles in increasingly complex relationships, see OECD, Working Party on Information Security and Privacy, *The evolving privacy landscape; 30 years after the OECD privacy guidelines* (April 2011) p 27.

[31] Data Protection Act 1998, ss 16 to 18. This obligation is subject to derogations, eg for maintenance of a public register and information which is not processed by means of equipment operating automatically.

exemptions.[32] These principles essentially revolve around legitimacy (determining when data sharing may occur); transparency (imposing duties of informing the data subjects); purpose limitations (narrowing the use of the data on first and subsequent transfer); proportionality (restricting the amount of information that may be shared and for how long); quality of data; compliance with data subjects' rights; and security.

LEGITIMACY OF DATA SHARING

3.24 The legitimacy principle, as derived from the first principle of the Data Protection Act 1998,[33] requires not only that data sharing must not be prohibited by the law, but also that it must be based on one of the limited available legal grounds for processing data.

3.25 This means that all legal sources regulating the processing of data, such as contract, statutory provisions or common law duties (for example, breach of confidence), should be complied with. Further, processing data, including sharing data, can legitimately occur in a limited number of circumstances where the data subject consents, or where it is necessary. These circumstances are set out in schedule 2.

3.26 It is not always straightforward to establish whether the data subject has given consent. The condition will be met if the data subject has capacity to consent, is aware of the purpose(s) of the data processing and has given consideration to this question, on the basis of the specific circumstances existing at the time of the consent.[34] Further, the data subject should feel that there is a genuine choice. The extent to which implied consent, widely relied on in some areas such as health care, is acceptable, is debatable.[35]

3.27 However, consent cannot always be obtained, or only at a great expense. Further, it may not be meaningful or appropriate, as it could put at risk the security of others, involve an element of pressure, or compromise the operation of a system underpinned by the compulsory participation of all.[36] Non-consensual sharing may be justified to protect the vital interests of the data subject, such as medical emergency.[37]

[32] Data Protection Act 1998, s 4(4).

[33] "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".

[34] See the definition of the consent in F Caldicott, *Information: to share or not to share? The Information Governance Review* (March 2013) p 36 and the stress on its fleeting character. See also, emphasising the increasing difficulty for individuals to understand and make decisions about the use of their personal data: OECD, Working Party on Information Security and Privacy, *The evolving privacy landscape; 30 years after the OECD privacy guidelines* (April 2011) p 4.

[35] The question also arises whether an implied consent conforms with art 2(h) of Directive 95/46 requiring that consent be "specific".

[36] Eg in the context of regulatory or enforcement functions, or research.

[37] Data Protection Act 1998, sch 2 para 4. Information Commissioner's Office, *Data sharing code of practice* (May 2011) p 16: eg disclosure of a person's medical history to an Accident and Emergency department treating the data subject for serious injuries.

3.28 When consent is not available, sharing may alternatively be required by the performance of any legal obligation to which the data controller is subject, other than an obligation imposed by contract – including statutes, EU law or the common law.[38]

3.29 Sharing data is also expressly authorised for the exercise of public functions, including the administration of justice; the exercise of any functions of either House of Parliament; the exercise of any functions conferred on any person by or under any enactment; the exercise of any functions of the Crown, a Minister of the Crown or a government department; and the exercise of any other functions of a public nature exercised in the public interest by any person.[39] It is probably the most common legal ground for data processing by public bodies.

3.30 Sharing data may also be necessary for the purposes of legitimate interests pursued by the data controller or the recipients of the data, provided these interests are not overridden by the rights, freedoms and interests of the data subject.[40] Article 8 of the European Convention on Human Rights is of major relevance in this exercise of weighing up the respective interests, rights and freedoms at stake. There is some doubt as to whether the "legitimate interests condition" can be used by public bodies.[41]

3.31 If sensitive personal data is being shared, processing is generally prohibited unless one of a number of limited exemptions apply. For example, the consent of the data subject must be "explicit",[42] and where processing is necessary in order to protect the vital interests of the data subject, a number of other requirements apply.[43] Other circumstances are specified by order.[44]

TRANSPARENCY

3.32 The first principle requires not only that processing be lawful, but also that it be fair. What is or is not "fair" processing is explained in schedule 1, part 2 of the Data Protection Act 1998. Personal data are not to be regarded as being processed fairly where the data subject has been deceived or misled as to the

[38] Data Protection Act 1998, sch 2 para 3.

[39] Data Protection Act 1998, sch 2 para 5.

[40] Data Protection Act 1998, sch 2 para 6. The Secretary of State has not specified particular circumstances as provided for in para 6(2).

[41] Although it is not excluded by either the Directive or the Data Protection Act 1998, it is likely that in most cases the public body would satisfy another condition. The Information Commissioner's Office recommends that public bodies rely on this condition only where no other condition can be satisfied. It is worth noting that the draft Regulation expressly excludes such legal basis for public bodies.

[42] In the absence of definition of what "explicit consent" means, either in the Data Protection Act 1998 or the Directive, this term should be construed in its ordinary meaning. See the Information Commissioner's Office guidance stating that the consent must be absolutely clear and involve detailed explanations on the processing from the controller.

[43] Data Protection Act 1998, sch 3 para 3. This ground can only be resorted to where consent cannot be given by or on behalf of the data subject, or reasonably expected. Further, while processing data may be generally justified for the exercise of any function of a public nature carried out in the public interest by any person, such ground does not exist for sensitive data.

[44] Data Protection Act 1998, sch 3 para 10 and the Data Protection (processing of Sensitive Data) Order 2000 SI 2000 No 417.

purpose of processing.[45] Further, the data subject must be provided with sufficient information, either prior to, at the time that the processing such as data sharing first takes place, or very soon afterwards. The information that should be provided to the data subject includes the identity of the data controller or any nominated representative; the purposes for which the data are intended to be processed; and any further information that is necessary in order for the processing to be considered fair having regard to the specific circumstances.

3.33 Usually this requirement is complied with through the provision of "fair processing notices" informing the data subject about any possible communication of the data to another body.[46]

3.34 Exemptions are provided for, including where it would involve disproportionate effort, or where the recording or disclosure of the data is necessary for compliance with a legal obligation.[47]

3.35 One of the aims pursued by these provisions is to provide an individual with the opportunity to access data relating to processing and to ensure that processing is carried out in observance of the Data Protection Act 1998 principles.[48]

PURPOSE LIMITATION

3.36 The purpose limitation rule derives from the second principle, which provides that at the point of the initial collection of personal data, the purposes must be specified and lawful, and that subsequent use must not be incompatible with those purposes.[49] This principle partly overlaps with the transparency requirement flowing from the first principle.[50]

PROPORTIONALITY

3.37 Proportionality implies that the amount of data and the duration of its storage be commensurate with the purpose for which it is acquired and processed. It covers the third and the fifth principles of the Data Protection Act 1998.

[45] Eg in the *Campbell* and *Douglas v Hello! Ltd* cases, it was held that photographs obtained surreptitiously had not been fairly obtained (*Campbell v MGN Ltd* [2002] EWHC 499 (QB), [2002] EMLR 30; *Douglas v Hello! Ltd* (No6) [2003] EWHC 786 (Ch), [2003] 3 All ER 996 at [236]); see also *R v Broadcasting Standards Commission, ex parte British Broadcasting Commission* [2001] QB 885.

[46] In its guidance, the Information Commissioner's Office gives the example of a local authority including on an application form for "meals-on-wheels" services a statement that the information provided may be supplied to the Department for Work and Pensions in order to assess whether the data subject is entitled to any other benefits and will not be used for any other purpose.

[47] Data Protection Act 1998, sch 1 part 2 para 3.

[48] Opinion of Advocate General Ruiz-Jarabo Colomer, case C-553/07 *College van burgemeester en wethouders van Rotterdam v MEE Rijkeboer* [2009] ECR I-3889 at [66].

[49] Data Protection Act 1998, sch 1 part 2 para 5.

[50] See, for extensive developments on this principle, Article 29 Data Protection Working Party, *Opinion 3/2013 on purpose limitation* (2 April 2013) WP 203, at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (last visited 30 August 2013).

3.38 The third principle, amounting to a "minimality" requirement,[51] reads as follows: "personal data should be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed". It is subject to a number of exceptions listed under part 4 of the Data Protection Act 1998. The result is that in exempted areas, bulk transfers of data including irrelevant material could be lawful where separating particular fields or records from a dataset prior to a transfer would be impracticable or prohibitively expensive. Privacy Impact Assessments, to be carried out by a government department when introducing new policies or processes involving personal data, enable the departments to reach an informed decision about how much information needs to be shared.

3.39 Moreover, according to the fifth principle, personal data should not be kept longer than is necessary in relation to the purpose for which it was collected. It means that the body which receives the information must make provision to ensure that the personal data it has received is kept no longer than is necessary for the purpose of the transfer. The retention period may be specified by statute; other retention periods will be determined by business need or risk analysis.[52] Section 33 of the Data Protection Act 1998 provides an exemption to this principle, allowing data controllers to keep personal data indefinitely where necessary for historical, research or statistical purposes, provided that certain conditions are met. Further exemptions from this principle are allowed, when they are necessary to safeguard some overarching objective such as national security or economic interests.

QUALITY OF DATA

3.40 The fourth principle requires that personal data is accurate, and, where necessary, kept up-to-date. In the context of data sharing, it means, as explained in part 2 of schedule 1, that the receiving body must take reasonable steps to ensure the accuracy of the information they receive, having regard to the purpose(s) for which the data was obtained and further processed.[53]

COMPLIANCE WITH THE RIGHTS OF THE DATA SUBJECTS

3.41 The sixth principle requires processing to be in accordance with the rights of data subjects conferred by the Act. These rights are set out in part 2 of the Data Protection Act 1998. The data subject is entitled:

(1) to be informed whether personal data are being processed and be given appropriate information about the processing (including a description of the personal data, the purpose of the processing, the possible recipients of the data and their source). The personal data of which the individual is the data subject must be communicated to him in an intelligible form.

[51] Lee A Bygrabe, *Data protection law. Approaching its rationale, logic and limits* (2002) p 59.

[52] A Watson and C Bessant, *Information sharing and data protection* in C Bessant (ed) *Information sharing handbook* (2009) p 41.

[53] Ministry of Justice, *Public Sector Data Sharing: Guidance on the Law*, annex H to the *Data sharing protocol* p 19: should such checks be performed, the principles should not be regarded as being contravened if the information turns out to be inaccurate, having been inaccurately transmitted by the first body. However, if the data subject has informed the receiving authority that the data are incorrect, this authority should take action, either to rectify or indicate on the data that their accuracy is disputed.

These rights are subject to the right of others not to have their personal data disclosed[54] and to restrictions in the context of "unstructured" personal data held by public authorities;[55]

(2) to require the data controller to cease or not to process personal data, in particular where this would cause substantial and unwarranted damage or distress to him, subject to some exceptions;[56]

(3) to be compensated for failure by a data controller to comply with the Data Protection Act 1998 where the individual suffers damage or distress because of that failure;[57] and

(4) to apply for the court to order the rectification, blocking, erasure or destruction of data.[58]

3.42 In the context of public sector data sharing, both the sender and the recipient of the data have to comply with these rights.

SECURITY

3.43 Security requirements are dealt with by the seventh principle, which reads:

> 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.[59]

3.44 This principle requires for example that data controllers must take reasonable steps to ensure the reliability of any employee who has access to the personal data.[60] Further, if a data controller resorts to a data processor, the processor must comply with appropriate security guarantees on the basis of a written contract.[61]

3.45 High-profile data losses have resulted in greater emphasis on security and the imposition on all central government departments of mandatory minimum security measures.[62]

[54] Data Protection Act 1998, s 7.

[55] Data Protection Act 1998, s 9A.

[56] Data Protection Act 1998, s 10(1).

[57] Data Protection Act 1998, s 13.

[58] Data Protection Act 1998, s 14.

[59] Data Protection Act 1998, sch 1, part 1, para 5.

[60] Data Protection Act 1998 sch 1 part 2 para 10.

[61] Data Protection Act 1998, sch 1 part 2 para 12. On the debated question of the respective roles of processors and controllers, *Encyclopaedia of Data Protection*, Sweet and Maxwell para 1-206.

[62] Ministry of Justice, *Mandatory Minimum Measures for Protection of Personal Data*, annex E to the *Data Sharing Protocol*, at http://www.justice.gov.uk/downloads/information-access-rights/data-sharing/annex-e-mandatory-minimum-measures.pdf (last visited 30 August 2013).

3.46 Where data sharing agreements are made between agencies, they should set out the security arrangements incumbent on each party, both technical (such as encryption, secure e-mail, passwords and virus protection) and organisational (including for example the rules regarding the access to data and storage).

3.47 Sharing de-identified data for research purposes raises specific organisational challenges. Common responses to these challenges include establishing "safe havens", removing personal identifiers and restricting the access to data to authorised researchers.[63]

3.48 Trust in the security of the second public body's information management is crucial to a successful data sharing. However, too often information management is not seen as a priority and suffers the consequences of cuts, resulting in insufficient investment in technology. This vulnerability leads to trust issues and is an important hindrance to data sharing.[64]

EXEMPTIONS

3.49 The Data Protection Act 1998 provides exemptions from some or all of the data protection principles in a number of situations.

3.50 For example, personal data are exempt from the data protection principles when this exemption is required for the purpose of safeguarding national security under section 28.[65]

3.51 Moreover, where personal data are processed for (a) the prevention or detection of crime; (b) the apprehension or prosecution of offenders; or (c) the assessment or collection of any tax or duty or of any imposition of a similar nature, the first principle (to the extent that it sets down transparency requirements) and the rights of information of data subjects contained in section 7 are disapplied.[66] The exemption is not automatic but may only be applied to the extent to which the application of the exempted provisions would be "likely to prejudice" any of these

[63] "Safe havens" may be defined as a secured data access facility where access to personal data can be controlled, in particular stand-alone (not networked) computers within secure premises, which only accredited researchers can use: see Scottish Government, *A Scotland-wide Data Linkage Framework for Statistics and Research: Consultation Paper on the Aims and Guiding Principles* (March 2012) p 15; the UK Administrative Data Research Network, *Improving Access for Research and Policy* (Administrative Data Taskforce, December 2012) p 42.

[64] Dan Jellinek, "Why sharing data can save services", *The Guardian*, 23 January 2013.

[65] Data Protection Act 1998 s 28 provides for an optional certification procedure by which a Minister of the Crown certifies that exemption is required for the purpose of safeguarding national security. This certificate is conclusive evidence of that fact, subject to a right of appeal to the National Security Appeals Panel, a separate section of the Information Tribunal.

[66] So, for example, provided that the processing of data occurs for one of these purposes and necessary for the exercise by a public body of any function conferred by an enactment or common law powers, the public body would not have to inform an individual that it is gathering personal information about him or her.

objectives. This provision has been interpreted as requiring a more significant than merely fanciful chance of prejudice.[67]

3.52 Subject information requirements may be waived in relation to health, education and social work data;[68] data processed by regulatory bodies for the purposes of protection of the public from misconduct of various sorts, subject to a "likely to prejudice" test;[69] de-personalised data processed for research purposes, including statistical or historical purposes.[70]

Enforcement of the Data Protection Act 1998 and consequences of non-compliance

Information Commissioner's powers

3.53 The Information Commissioner has a duty to promote good practice, disseminate information, give advice and issue codes of practice,[71] in particular on data sharing,[72] and is responsible for enforcing the Data Protection Act 1998.[73] The Information Commissioner has powers to investigate alleged breaches of the requirements of the Act and failure to comply with an enforcement notice, information notice or special information notice is a criminal offence.

3.54 The Information Commissioner may serve an information notice requiring the data controller to supply specified information relating to processing activities, including data sharing, for the purposes of determining whether the data protection principles have been complied with.[74]

3.55 The Information Commissioner may serve an enforcement notice where he is satisfied that any of the data protection principles are being contravened. An enforcement notice may require the data controller to stop processing personal data, to take certain steps to remedy the unlawful processing within a certain time and to rectify, block, erase or destroy inaccurate data and notify third parties.[75] For example, in the context of data sharing, the Information Commissioner could

[67] *R (Lord) v Secretary of State for the Home Department* [2003] EWHC 2073 (Admin), [2004] Prison Law Reports 65 at [99] and [100].

[68] Data Protection Act 1998, s 30. These exemptions are detailed in the Data Protection (Subject Access Modification) (Health) Order 2000, SI 2000 No 413; the Data Protection (Subject Access Modification) (Education) Order 2000, SI 2000 No 414; the Data Protection (Subject Access Modification) (Social Work) Order 2000, SI 2000 No 415; and the Data Protection (Subject Access Modification) (Social Work) (Amendment) Order 2011 No 1034.

[69] Data Protection Act 1998, s 31.

[70] Data Protection Act 1998, s 33. These data are also generally exempted from the second and fifth data protection principles.

[71] Data Protection Act 1998, s 51.

[72] Data Protection Act 1998, s 52E. A breach of the data sharing code is not actionable in any court or tribunal, but the code will be admissible as evidence in any legal proceedings and any relevant provision of the code must be taken into account by the Information Commissioner or by a court or tribunal when determining a question arising in legal proceedings or in connection with the exercise of that jurisdiction.

[73] As well as the Freedom of Information Act 2000: Data Protection Act 1998, s 6(1).

[74] Data Protection Act 1998, s 43.

[75] Data Protection Act 1998, s 40.

conclude that the amount of data is excessive and issue an enforcement notice requiring the bodies to share only specific relevant data.

3.56 A data controller has a right of appeal to the Information Rights Tribunal against the service and extent of these notices.[76] The appeal is a full appeal on facts and law. A further appeal on a point of law lies to the Upper Tribunal Administrative Appeals Chamber.

3.57 The use of information and enforcement notices is relatively rare. Informal resolution is the most common regulatory approach.[77]

3.58 Section 50 and schedule 9 provide the Information Commissioner with powers of entry and inspection, subject to the issue of a warrant by a circuit or a district judge.

Misuse of information – accountability and sanctions

Civil remedies and penalties

3.59 Data subjects have a statutory cause of action under section 13. Compensation may be awarded if the data subject has suffered damage, or distress and damage, as a result of any contravention by a data controller of any of the requirements of the Act.

3.60 In addition, the Information Commissioner now has power, under sections 55A to 55E, to impose a civil monetary penalty on any data controller who commits a serious contravention of the data protection principles. The penalty is subject to a right of appeal.

Criminal sanctions

3.61 A number of criminal offences are created by the Data Protection Act 1998 such as processing without notifying[78] or failing to comply with an information or enforcement notice.[79] Criminal proceedings under the Act may only be instituted by the Information Commissioner or by, or with the consent of, the Director of Public Prosecutions.[80] A government department is not liable to prosecution.[81]

3.62 Section 55 creates the criminal offence of unlawfully obtaining personal data. It is subject to various defences, including a public interest defence.

[76] The Information Rights Tribunal is part of the First-tier Tribunal in the General Regulatory Chamber and formally to be referred to as the First-tier Tribunal (Information Rights): see the Transfer of Tribunal Functions Order 2010 SI 2010 No 22, art 5(1) and sch 2 paras 24 and 25(b).

[77] C Bessant, *The duty of confidence* in C Bessant (ed), *Information Sharing Handbook* (2009) p 32.

[78] Data Protection Act 1998, s 21.

[79] Data Protection Act 1998, s 47.

[80] Data Protection Act 1998, s 60.

[81] Data Protection Act 1998, s 63(5).

3.63 Anecdotal evidence suggests that the severity of the sentences applicable in case of unlawful disclosure of data sharing may create a risk-averse environment for data sharing.

Judicial review

3.64 When the person who shared the information is a public body, it is subject to judicial review. If a decision to share data, for instance, is illegal, irrational or procedurally improper, the Administrative Court may quash it, and in some circumstances it may make a mandatory order requiring the public body to take a specified action.

CONFIDENTIAL AND PRIVATE INFORMATION

3.65 Public bodies may be unable to share information that is confidential or private.

3.66 The long-standing action for breach of confidence protects private information from disclosure.[82]

3.67 Disclosure may be prevented irrespective of the existence of a prior relationship between a confider and a confidant, provided the information is "private".[83] The right to respect for private life, protected by article 8 of the European Convention on Human Rights, is integral to the modern action for breach of confidence.

3.68 Breach of confidence protects a variety of confidential information, whatever its form or nature: personal, commercial, artistic, or governmental. Written documents, photographs, verbal information, etchings, sound recording, pharmaceutical data or video recordings can all be protected.

From an action for breach of confidence to a right to respect for private information

3.69 The contemporary action for breach of confidence reflects developments following the coming into force of the Human Rights Act 1998. Originally revolving around the breach of a trust underpinning a confidential relationship, it has come to centre on the private nature of the information itself. The House of Lords explained these developments in the *Campbell* case, which has been followed in many subsequent judgements.[84]

[82] The modern action for breach of confidence developed from the mid-19th century: see *Prince Albert v Strange* (1849) 2 De G & Sm 652. This case was for example referred to as "seminal" in *Campbell v MGN Limited* [2004] UKHL 22, [2004] 2 AC 457 at [43]. See also Breach of Confidence (1981) Law Com No 110 at 3.2; T Aplin, L Bently, P Johnson and S Malynicx (eds), *Gurry on breach of confidence* (2012) ch 2 , commenting that "courts have been willing to protect confidentiality pragmatically by whatever mechanism is at hand".

[83] *Campbell v MGN Limited* [2004] UKHL 22, [2004] 2 AC 457 at [13] and [14].

[84] *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]. However, this change is viewed by some as a distortion of the original cause of action: Lord Phillips of Worth Matravers in *Douglas v Hello* (No 3) [2005] EWCA Civ, [2006] QB 125 at [53].

3.70 These developments reflect the obligation of the courts, as public bodies, to act compatibly with human rights, including in the development of the common law, and to take into account the case law of the European Court of Human Rights.[85]

3.71 In the *Campbell* case, Lord Nicholls of Birkenhead stated that:

> the gist of the cause of action was that information of this character had been disclosed by one person to another in circumstances "importing an obligation of confidence"... . Now the law imposes a "duty of confidence" whenever a person receives information he knows or ought to know is fairly and reasonably to be regarded as confidential. Even this formulation is awkward... . The more natural description today is that such information is private. The essence of the tort is better encapsulated now as misuse of private information.[86]

The main elements of the action for misuse of private information

The information is not in the public domain

3.72 The private and confidential nature of the information is a prerequisite for any action for breach of confidence. Information must not be in the public domain if it is to be protected.[87]

3.73 Information may lose its private nature by dissemination or the passage of time, although the question is one of degree taking into account the number of recipients, the content and form of the information, and what impact further dissemination will make.[88] The duration of the dissemination of information, the period during which the data are available to other parties, is a relevant consideration to assess whether information remains confidential.[89] Private information which is shared with a limited group may not lose its confidential character, for example, publication on an expert website does not amount to a full disclosure destroying the duty of confidence.[90] Where a piece of information has

[85] Human Rights Act 1998, s 6; *R (Alconbury Development Ltd) v Secretary of State for the Environment, Transport and the Regions and other cases* [2001] UKHL 23, [2003] 2 AC 295 at [26]; *Kay v Lambeth London Borough Council* [2006] UKHL 10, [2006] 2 AC 465 at [43] and [44].

[86] *Campbell v MGN Limited* [2004] UKHL 22, [2004] 2 AC 457 at [13] and [14].

[87] *Attorney-General v Guardian Newspapers Ltd (No 2)* (the "Spycatcher" case) [1988] 2 WLR 805*;* "public property" or "public knowledge" are sometimes alternatively referred to: see eg *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* (1948) 65 RPC 203, 215; *Coco v A N Clark (Engineers) Ltd* [1969] FSR 415; see also T Aplin, L Bently, P Johnson and S Malynicx (eds), *Gurry on breach of confidence* (2012) para 5.14, referring to the "inaccessibility" of the information.

[88] Sir John Donaldson MR in *Attorney-General v Guardian Newspapers Ltd (No 2)* [1988] 2 WLR 805, 868B.

[89] It results that a transitory and brief disclosure may not be enough to remove the confidential character of the information. See eg the Australian case *G v Day* [1982] 1 NSWLR 24, referred to in T Aplin, L Bently, P Johnson and S Malynicx (eds), *Gurry on breach of confidence* (2012) para 5.23.

[90] *Barclays Bank plc v Guardian News and Media Ltd* [2009] EWHC 591 (QB) at [22]; the same approach has been taken for information about the effect of a drug already subject of television coverage in *Schering Chemicals Limited v Falkman Limited* [1982] QB 1.

been used in open court, however, its confidentiality is deemed to be destroyed.[91] Whether further disclosure has the potential to affect the interests of the person concerned may also be a relevant consideration.[92] The intention of the person to whom the duty of confidence is owed as to the extent of the publication is a key consideration. It is only where the publication of the confidential information was made by this person with the intention to publish at large that the duty of confidence ceases.[93] Such an intention must be clear.[94]

3.74 A detailed assessment is made of the relevant information. Both the information's form and content are relevant.[95]

3.75 Public information may become private with the passage of time.[96] However, to the extent that the relevance of information decreases over time, the need to protect it may diminish. This becomes relevant in balancing a potential infringement of privacy against the public interest in disclosure.

3.76 Information is capable of retaining its private character after the death of the individuals concerned. This was the approach taken in relation to medical data in the *Bluck* case by the Information Tribunal, in view in particular of the fundamental importance of such data in the case law of the European Court of Human Rights.[97] The High Court in *Lewis v Secretary of State for Health* was similarly inclined to accept that "an obligation of confidence imposed on the conscience of the confidant does survive, or at least is capable of surviving, the death of the confider".[98] The European Court of Human Rights held that protection of medical confidentiality of a deceased person may constitute a legitimate interest overriding the right to freedom of expression, but recognised that this balance was highly time-sensitive.[99]

Information imparted in confidence

3.77 In order for a breach of confidence to occur, there must be a violation of a pre-existing duty to maintain the confidentiality of the information. This obligation

[91] *Marcel v Commissioner of Police of the Metropolis* [1991] 2 WLR 1118, 1127H. However, the effect of time has to be taken into account.

[92] *Speed Seal Products Ltd v Paddington* [1985] 1 WLR 1327, 1332H.

[93] *Speed Seal Products Ltd v Paddington* [1985] 1 WLR 1327, 1331E to 1332B; *Mustad and Son v Dosen* [1964] 1 WLR 109; *Associated Newspapers v Prince of* Wales [2006] EWCA Civ 1776, [2008] Ch 57 (partial disclosure).

[94] See *Attorney General v Jonathan Cape Ltd* [1976] QB 752.

[95] Accordingly, an event may take place in a public place (*Campbell* and *Murray* cases), or be publicly known (*Douglas* case), but photographs illustrating it remain confidential. See also *S v Information Commissioner and General Register Office* EA/2006/0030, 9 May 2007: a letter recalling some facts known to the applicant was still confidential.

[96] "Convictions are made and sentences are imposed in public. But as the conviction recedes into the past, it becomes part of the individual's private life": *R (T and JB) v Secretary of State for Justice* [2013] EWCA Civ 25, [2013] 2 All ER 813 at [31].

[97] *Bluck v Information Commissioner and Epsom and St Helier University NHS Trust* EA/2006/0090.

[98] *Lewis v the Secretary of State for Health* [2008] EWHC 2196 (QB), [2008] LS Law Medical 559. See also *Toulson and Phipps on Confidentiality* (2nd ed 2006) para 11-053.

[99] See *Plon v France (*2006) 42 EHRR 36 (App No 58148/00), relating to the publication of information about the health of the late President F Mitterand.

arises in relation to private information. It may also arise out of a contract or implied contract or flow from a specific relationship between the parties such as between solicitor and client, bank and client, employer and employee, social worker and child, husband and wife, or friends. There is no closed list or hard and fast rule for ascertaining the nature of such a relationship. The test is whether "the circumstances are such that any reasonable man standing in the shoes of the recipient of the information would have realised that … the information was being given to him in confidence".[100]

3.78 Third parties with notice of the obligation of confidentiality can be bound by it.[101]

3.79 Trivial information may fall outside the scope of confidential information. However, caution is required in this regard, as it is often difficult to appreciate the value of information taken in isolation.[102]

3.80 The action for breach of confidence does not require the claimant to show that damage has resulted or will result from disclosure.[103]

3.81 A duty of confidentiality may also attach to certain Government information. Information is protected by the action for breach of confidence where disclosure would "obstruct the proper functioning of a recognized part of the constitutional machinery", such as the operation of collective ministerial responsibility, or impair the exercise of Government functions.[104]

Respect for private life

3.82 The concept of ''private life'' is a broad one, not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person, and a person's social identity and image. Interactions by a person with others in a public context may also fall within the scope of private life.[105] It does not, however, extend to legal persons.[106]

3.83 The following information has been considered to fall within the definition of "private information": a person's health, including mental health, diet issues and drug dependency; sexual relationships and sexual orientation; personal feelings and opinions, more generally any personal information that an individual wishes

[100] *Coco v A N Clark (Engineers) Ltd* [1969] FSR 415, 421.

[101] *Prince Albert v Strange* (1849) 2 De G & SM 652; *Stephens v* Avery [1988] Ch 449. It includes cases where the information has been acquired unlawfully: *Francome v Mirror Group Newspapers Ltd* [1984] 1 WLR 892.

[102] *Attorney-General v Guardian Newspapers Ltd (No 2)* [1988] 2 WLR 805, 870G.

[103] *Duchess of Argyll v Duke of Argyll* [1967] Ch 302; *Coco v A N Clark (Engineers) Ltd* [1969] FSR 415; *Mc Kennitt v Ash* [2006] EWCA Civ 1714, [2008] QB 73.

[104] T Aplin, L Bently, P Johnson and S Malynicx (eds), *Gurry on breach of confidence* (2012) para 6.46; Australian case *Commonwealth of Australia v John Fairfax and Sons Ltd* 147 CLR 39 at [51] and [52]; *Attorney-General v Guardian Newspapers Ltd (No 2)* [1988] 2 WLR 805*; Attorney General v Jonathan Cape Ltd* [1976] QB 752*.*

[105] See, among a wealth of case law on this matter, *Van Hannover v Germany* (2005) 40 EHRR 1 (App No 59320/00) at [50].

[106] Unless their official title identifies one or more natural persons: see eg *Amann v Switzerland* [GC] (2000) 30 EHRR 843 (App No 27798/95) (Grand Chamber decision) at [65].

to keep to himself; the details of the physical arrangements of a home; an individual's finances or professional income; the physical appearance of an individual; an individual's ethnic identity; fingerprints, DNA profiles and cellular samples; someone's reputation and image.

3.84 Information may have been publicly available at one point and still subsequently become private. For example, past convictions become part of the individual's private life over time,[107] as well as personal information gathered from open sources.[108] The address of a person may be private information, even though that information was already publicly available.[109] A photograph of an individual going about their lawful business in the street, as well as permanent or systematic recording of individuals' public activities, fall within the remit of article 8.[110]

3.85 A key consideration is whether the person to whom the information relates had any expectation that the information was kept confidential. Within the private sphere, the individual is in command of the facts about his privacy and controls whether others should or should not have access to private information.[111]

3.86 Public figures, especially those performing public functions, do not have the same expectation of privacy.[112]

3.87 The existence of protective measures may be indicative of private information. Such measures must not be notional or inconsistent. If a document is marked confidential and in practice not treated as such, it will not necessarily be held to be confidential.[113]

3.88 The classification of information as private may be difficult. In that case, instead of looking into the nature of the information, it is often more practical to ask whether the disclosure falls within an exception to the duty of confidence and

[107] *R v Chief Constable of the Northern Wales Police, ex parte AB* [1999] QB 396, 414, 416 and 429; *R (L) v Commissioner of Police of the Metropolis* [2009] UKSC 3, [2010] 1 AC 410 at [25] to [27]; *R (T and JB) v Secretary of State for Justice* [2013] EWCA Civ 25, [2013] 2 All ER 813 at [31].

[108] *R (on the application of Catt) v Association of Chief Police Officer* [2013] EWCA Civ 192, [2013] HRLR 20.

[109] *Wife and children of Omar Othman v English National Resistance* [2013] EWHC 1421 (Admin).

[110] See *Wood v Commissioner of Police for the Metropolis* [2009] EWCA Civ 414, [2010] 1 WLR 123; *Segerstedt-Wiberg v Sweden* (2007) 44 EHRR 2 (App No 62332/00); *Rotaru v Romania* 8 BHRC 449 (App No 28341/95).

[111] *Wood v Commissioner of Police for the Metropolis* [2009] EWCA Civ 414, [2010] 1 WLR 123.

[112] *Van Hannover v Germany* (2005) 40 EHRR 1 (App No 59320/00) at [63] and [64]; *Murray v Express Newspapers plc and another* [2008] EWCA Civ 446, [2009] Ch 481.

[113] T Aplin, L Bently, P Johnson and S Malynicx (eds), *Gurry on breach of confidence* (2012) para 5.77, referring inter alia to the patent case *Dalrymple's Application* [1957] RPC 449; see also Information Commissioner's Office, *Subject access: code of practice. Dealing with requests from individuals for personal information* (August 2013) p 32.

whether disclosure is compatible with the individual's human rights, including the right to private life.[114]

Exceptions to the duty of confidence: countervailing public interest

3.89 Private information will not always be subject to a duty of confidence. Confidentiality can be waived by consent. Further, even though an obligation of confidence has arisen, a public body is allowed to pass on the information to another public body when the law requires this communication.[115]

3.90 Disclosure will also be lawful when it meets a prominent public interest and does not go beyond what is necessary to reach this purpose. This public interest was understood initially as justifying a breach of confidence, in accordance with the so-called "iniquity rule", when the secret hid a crime or a fraud. The exception to the rule of confidentiality was then extended to civil wrongs or misdeeds and finally came to cover any important public interest, for example engaging safety or even value for money.[116]

3.91 Under the influence of the European Convention on Human Rights, this examination of the public interest defence has taken a more structured form of a balancing exercise in which the public and private interests in the preservation of confidentiality are weighed against other countervailing public interests requiring disclosure of information.[117] For a disclosure to another public body of confidential or private information to be lawful, the "interference" with the right to respect for private life must be "in accordance with the law", pursue a legitimate aim and be necessary for achieving that aim.[118]

3.92 Disclosure must be based on law, failing which there will be a breach of the right to respect for private life.[119] The law must be formulated with sufficient precision to clarify the scope of discretion conferred on the competent authorities and the manner of its exercise. Instructions, administrative practices and guidance may be taken into account, in so far as they are clear and sufficiently publicised.[120] The degree of clarity required depends on the field concerned. For example, telephone tapping, secret surveillance, covert intelligence-gathering and other secret controls demand detailed and clear rules about scope and safeguards for individuals, including duration of storage and access of third parties.[121]

[114] See eg for a recent case *R (T and JB) v Secretary of State for Justice* [2013] EWCA Civ 25, [2013] 2 All ER 813.

[115] The defence of the "compulsion of law". See Chapter 4 on statutory gateways.

[116] *Gartside v Outram* (1857) 26 LJ Ch 113, 114; *Beloff v Pressdram Ltd* [1973] 1 All ER 241, 260; *Lion Laboratories Ltd v Evans* [1985] QB 526; *Initial Services Limited v Putterill* [1968] 1 QB 396; *Hubbard v Vosper* [1972] 2 QB 84; *London Regional Transport v The Mayor of London* [2001] EWCA Civ 1491, [2003] EMLR 4.

[117] *Attorney-General v Guardian Newspapers Ltd* (No 2) [1990] 1 AC 109, 282.

[118] European Convention on Human Rights, art 8.

[119] *Sciacca v Italy* (2006) 43 EHRR 20 (App No 50774/99).

[120] *Silver v United Kingdom* (1983) 5 EHRR 347 (App Nos 5947/72 6205/73, 7052/75, 7061/75 7107/75, 7113/75, 7136/75) at [88] to [89].

3.93 The performance of the balancing test also demands an examination of the degree of interference. Several elements may come into play in an operation of data sharing, including the way in which the information is used and can be used in the future.[122] The fact that no immediate detriment is caused does not reveal an absence of interference.[123]

3.94 Data sharing is likely to constitute an interference with private life in some contexts.[124] The disclosure of a person's medical record by a clinic to a Social Insurance Office for purposes of investigating fraud and the communication of information in the context of security checks performed on applicants have both been held to be interferences.[125] The retention of data by a second public body may constitute interference within the meaning of article 8, regardless of the subsequent use of the stored information.[126] The retention of photographs may also engage article 8, depending on a number of factors (photographs taken in a way that invades individual privacy, such as in an individual's home; photographs taken in the public place, where the individual could not expect them to be taken; filling in a database; efforts made to identify the person on the photograph; purpose for which the photographs were taken).[127]

3.95 The interference must also be proportionate to the legitimate aim pursued, which means that a "pressing social need" must be identified; the means chosen to limit the right must be adequate; and the impact on the right must be as minimal as

[121] *S and Marper v United Kingdom* (2009) 48 EHRR 50 (App Nos 30562/04 and 30566/044) (Grand Chamber decision); *Leander v Sweden* (1987) 9 EHRR 433 (App No 9248/81) at [51]; *MM v United Kingdom* App No 24029/07 (unreported); *R (on the application of Catt) v Association of Chief Police Officer* [2013] EWCA Civ 192, 3 All ER 583.

[122] *S and Marper v United Kingdom* (2008) 48 EHRR 50 (App Nos 30562/04 and 30566/044) (Grand Chamber decision).

[123] See eg *S and Marper v United Kingdom* (2009) 48 EHRR 50 (App Nos 30562/04 and 30566/044) (Grand Chamber decision) at [73]; *Hilton v UK* App No 12015/86 (Commission decision); joined cases C-465/00 and C-138/01 *Rechnungshof* [2003] ECR I-4989 at [75]; *Amann v Switzerland* (2000) 30 ECHR 843 (App No 27798/95) (Grand Chamber decision) at [70].

[124] See *Marcel v Commissioner of Police of the Metropolis* [1991] 2 WLR 1118, 1130.

[125] See eg *MS v Sweden* (1999) 28 EHRR 313 (App No 20837/92); joined cases C-465/00 and C-138/01 *Rechnungshof* [2003] ECR I-4989 at [74]; *Hilton v UK* App No 12015/86 (Commission decision).

[126] This is the case for example when data contains unique information about the individual concerned capable of affecting his or her private life, despite their objective and irrefutable character and the fact that they are not intelligible to the untutored eye. *S and Marper v United Kingdom* (2009) 48 EHRR 50 (App Nos 30562/04 and 30566/044) (Grand Chamber decision) on DNA profiles which provide a means of identifying genetic relationships between individuals and assessing the likely ethnic origin of the donor; *Van der Velden v the Netherlands* App No 29514/05 (unreported), about cellular material including information on an individual's health and relatives.

[127] See eg *Wood v Commissioner of Police for the Metropolis* [2009] EWCA Civ 414, [2010] 1 WLR 123 at [43]: the fact that the police did not do something familiar and expected was taken into account; *Friedl* (1996) 21 EHRR 83 (App No 15225/89) at [49] to [51]; *S and Marper v United Kingdom* (2009) 48 EHRR 50 (App Nos 30562/04 and 30566/044 (Grand Chamber decision).

possible.[128] In addition, the decision-making process must be fair and such as to ensure due respect for the interests safeguarded by article 8.[129]

3.96 Article 8(2) expressly provides for legitimate interference "for the prevention of disorder or crime" [130] or "in the interests of…. public safety" or "the protection of rights and freedom of others". Transparency and accountability in the use of public money are other legitimate aims.[131]

3.97 There is a margin of appreciation in the balancing exercise. The extent of the margin of appreciation will depend, among other matters, on the nature of the right impugned, the nature of the interference and the object pursued. The margin will tend to be narrower when it comes to interference with the right to the protection of personal data. This is because this right is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life and the community as a whole. On the other hand, its core principles (proportionality in data collection and duration of storage, security) benefit from a strong consensus among the states.[132]

3.98 The interference with private life is smaller where an organisation is itself subject to an obligation of confidence. Interference is greater when publication is to the world.[133] The benefit of disclosure to the individual concerned, for example, if it means that the individual may establish a defence or obtain a benefit, is also taken into account. The potential for serious damage to the individual heightens scrutiny of the interference.[134]

3.99 When information relates to a risk posed by an individual to other individuals, additional requirements include the assessment of evidence of the risk on the balance of probabilities, the need for taking into consideration the time elapsed since the relevant events contained in the information, the interest of the recipient

[128] *R v Shayler* [2002] UKLH 11, [2003] 1 AC at [59].

[129] *Turek v Slovakia* (2006) 44 EHRR 861 (App No 57986/00) at [111]. See also *W v United Kingdom* (1987) 10 EHRR 29 (App No 9749/82); pre-Human Rights Act 1998 judgements applying the same principle: *R v Chief Constable of North Wales ex parte AB* [1999] QB 396: before deciding to disclose the identity of paedophiles to the public, the police must require as much information as possible, and in most situations the subject of the possible disclosure himself should be requested to provide information; *Woolgar v Chief Constable of Sussex Police* [2000] 1 WLR 25.

[130] Including the identification of offenders: *S and Marper v United Kingdom* (2009) 48 EHRR 50 (App Nos 30562/04 and 30566/044) (Grand Chamber decision); *R (Wood) v Commissioner of Police of Metropolis* [2009] EWCA Civ 414, [2010] 1 WLR 123 at [79].

[131] See eg joined cases C-92/09 and C-93/09 *Volker* [2010] ECR I-11063 at [68].

[132] See eg *S and Marper v United Kingdom* (2009) 48 EHRR 50 (App Nos 30562/04 and 30566/044) (Grand Chamber decision) at [103].

[133] See eg *Francome v Mirror Group Newspapers Ltd* [1984] 1WLR 892; *Lion Laboratories Ltd v Evans* [1985] QB 526; *Initial Services Ltd v Putterill* [1968] 1 QB 396, 405-406.

[134] Eg the decision of the police as to whether or not to disclose the identity of paedophiles to members of the public is a highly sensitive one given its consequences for the individuals concerned: *R v Chief Constable of North Wales ex parte AB* [1999] QB 396; see also *R (Wright) v Secretary of State for Health* [2009] UKHL 3, [2009] 1 AC 739.

of the information and an assessment of the risks posed in case of non disclosure.[135]

Remedies for breaches of the duty of confidence

3.100 A breach of confidence is most commonly remedied by seeking damages or an injunction to prevent or stop a breach. It is also possible for a court to order an account of profits.

[135] *R v Local Authority in the Midlands and another, ex parte LM* [2000] 1 FLR 612; *Woolgar v Chief Constable of Sussex Police* [2000] 1 WLR 25; *R(L) v Commissioner of the Police for the Metropolis* [2009] UKSC 3, [2010] 1 AC 410; *JR 57 Application for Judicial review (QB)* (NI) [2013] NIQB 33.

CHAPTER 4
THE POWER TO SHARE DATA

4.1 The rule of law requires that public bodies have a legal power to act and act within their powers.[1]

4.2 This principle requires that a power exists to share data. Such a power may be:

(1) express in a statute;

(2) implied from statutory powers or functions; or

(3) derived from other non statutory sources of authority.

EXPRESS STATUTORY GATEWAYS

4.3 Some legislation includes explicit "gateways" through which information can be disclosed or received for particular purposes.

4.4 Individual gateways enabling data sharing between organisations may constitute one or two clauses in large Acts or make up the exclusive subject matter of the Act. The gateways applicable to one organisation may spread over several independent pieces of legislation, as is the case for the Department for Work and Pensions.[2]

4.5 Provisions on gateways state that an authority may require or disclose some specific information from or to a specific authority, in certain circumstances and for specific purposes.[3] Gateways may be directly created by primary legislation or primary legislation may provide for regulations to be adopted including such gateways.

4.6 Primary legislation may directly create powers to require disclosure. For example, Section 1 of the Television Licenses (Disclosure of Information) Act 2000 provides that the Secretary of State may, at the request of the BBC, supply the BBC with social security information. Section 1 of the Statistics of Trade Act 1947 is another illustration of this model, stating that: "it shall be lawful for a competent authority by notice in writing served on any person carrying on an undertaking to require that person to furnish [such information]".

[1] D Feldman, *English Public Law* (2004) para 3.99; H W R Wade and C F Forsyth, *Administrative Law* (8th ed 2000) p 21.

[2] See Performance and Innovation Unit, *Privacy and data-sharing: The way forward for public services* (April 2002) p 104 listing a series of Acts containing information gateways for DWP, including Social Security Contributions (Transfer of Functions) Act 1999; Tax Credits Act 1999; Access to Justice Act 1999; Welfare Reform and Pensions Act 1999; Immigration and Asylum Act 1999; Television Licences (Disclosure of Information) Act 2000; Local Government Act 2000; Social Security Fraud Act 2001.

[3] This information must generally be "in the possession or control" of the person concerned (see eg Criminal Appeal Act 1995, s 17(1)) or "in the custody or under the control" of this person (National Audit Act 1983, s 8(2)).

4.7 Statute may also provide that orders or regulations may make provision for a mandatory disclosure of information,[4] alter the list of recipients laid down by primary legislation,[5] or apply further restrictions.[6]

4.8 As regards the objectives of the gateways, a distinction must be drawn between permissive gateways which create a discretionary power to disclose data, even if it is not requested,[7] and mandatory ones, which make it compulsory for some organisations to provide or disclose information to another, either at the request of another entity or on the initiative of the holder of the information.[8]

4.9 These gateways make the following kinds of provision:

(1) Who may request or be supplied the information. Provision may also be made to address the case where another person acts on behalf of the relevant authority.[9]

(2) From whom the information may be requested.

(3) The purposes for which the information may be used. The relevant Act may provide that receiving a request for disclosure is not enough to make the disclosure lawful; an additional requirement may be that it is requested by an authority for the purpose of carrying out its functions under the Act.

The primary legislation may specify the purpose in question,[10] or provide more generally that the information may be used for the purposes of the functions conferred by the Act.[11] The recipient may be given a written notice by the holder of the information specifying the purposes for which the information may be used.[12]

4 See eg Local Government Finance Act 1992, sch 2 para 11; Welfare Reform and Pensions Act 1999, s 45.

5 See eg Crime and Disorder Act 1998, s 115(3).

6 See eg Statistics of Trade Act 1947, s 2.

7 See eg Local Government Finance Act 1992, sch 2 para 16 (1) which provides that regulations under this schedule may include provision that an authority may supply relevant information to another authority, even if it is not requested, subject to a number of conditions, including if it believes it would be useful to the other authority.

8 See eg Local Government Finance Act 1992, sch 2 para 11(1): "Regulations under this schedule may include provision that any person mentioned… shall supply to a billing authority such information as fulfils the following conditions … (b) the authority requests the person concerned to supply it". By contrast, as an example of mandatory disclosure on the initiative of the holder of the information, see part 2 of the Public Health (Control of Disease) Act 1984, requiring medical practitioners to share patient information with the local authority where the patient has food poisoning or a notifiable disease such as cholera and plague.

9 See eg Crime and Disorder Act 1998, s 115(1)(b) ("person acting on behalf of [an] authority"); Social Security Contributions (Transfer of Functions, etc) Act 1999, sch 6, para 121F(1)(b) ("by a person providing services to the Secretary of State").

10 Eg the Local Government Finance Act 1992, sch 2 para 18A (1) sets out that: "an authority may use information it has obtained for the purpose of carrying out its functions under part 1 or part 2 of this Act for the purpose of— (a) identifying vacant dwellings, or (b) taking steps to bring vacant dwellings back into use."

11 Employment and Training Act 1973, s 4(5)(e).

12 Employment and Training Act 1973, s 4(5)(c).

These purposes may be described in varying degrees of detail. Further, the breadth of the power varies in terms of the way that the relationship between the processing and the purpose is expressed. At one end of the spectrum, both the purpose itself, and its link with the processing, are expressed in a general way. For example, the power to disclose is allowed "for the purposes of any provision of this Act," and where "necessary or expedient".[13] In contrast, the purposes may be more narrowly specified, in relation to specific functions[14] while the link between the processing and the purposes may be more strictly defined. Legislation may provide, for example, that disclosure must be necessary – as opposed to "necessary or expedient" - for the purposes of any provision of the Act or for carrying out a specific function under the Act. Intermediary qualifications include references to reasonableness.[15]

Purposes of disclosure may be broader for non-personal information. For example, the Local Government Finance Act 1992 provides that non personal information may be supplied for a purpose which is not covered by the relevant parts of the Act, provided it was obtained by the authority for the purpose of carrying out its functions under the relevant parts of the Act.[16]

(4) The type of information that may be used or required.

(5) The amount of information that may be processed: a proportionality requirement may be explicitly set out.[17] Acts may have higher requirements for personal information.[18]

(6) The type of information that may not be used or required. This category includes for example information which came to the authority in receipt of the request in an unlawful way; information requested for a purpose that does not fall within the authorised purposes; information prohibited by the Data Protection Act 1998.[19]

(7) The offences applying to any failure to furnish information or to furnish false information. For example, pursuant to the Statistics of Trade Act 1947, a person required to furnish estimates or returns who fails to do so commits a summary offence.[20]

(8) Whether the information is to be supplied according to a specific

[13] Crime and Disorder Act 1998, s 115(1).

[14] See eg Local Government Finance Act 1992, sch 2 para 18: power to use information for the purpose of carrying out its functions under part 1 [or part 2] of this Act for the purpose of (a) identifying vacant dwellings, or (b) taking steps to bring vacant dwellings back into use.

[15] Eg National Audit Act 1983, s 8(1): "such documents as he may reasonable require"; Criminal Appeal Act 1995, s 17(2)(b): "where it is reasonable to do so".

[16] Sch 2 para 17.

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

[18] See eg Local Government Finance Act 1992, sch 2 para 18A.

[19] See eg Local Government Finance Act 1992, sch 2 para 11(1A); Anti-terrorism, Crime and Security Act 2001, s 19(7).

[20] Statistics of Trade Act 1947, s 4(1).

procedure, for example following due consultation of a specific authority or after taking into account some relevant elements;[21] or in a prescribed form and within a prescribed period of the request being made.[22]

(9) Limitations on further disclosure of the information. Compliance with proportionality principle may be required.[23] Conditions for lawfully disclosing may include obtaining consent from the primary recipient of the information as well as the person to whom it relates.[24]

(10) Whether the document or a copy may be taken away or disposed.[25]

4.10 Although the statutory gateways should make clear what information can be shared, there are concerns that specific statutory gateways do not necessarily remove all uncertainty.[26] At the same time, statutory gateways may create a false reassurance that information can be shared, or, conversely, foster the notion that information cannot be shared in the absence of a gateway.[27]

Interaction with other legal requirements

4.11 Statutory provisions interact with other legal requirements in different ways.

4.12 First, gateway provisions may be presented as default provisions, which are applicable only to the extent that there would not be already any power to disclose information[28] and do not affect powers to disclose information existing elsewhere.[29]

4.13 Some provisions override other statutory provisions preventing the disclosure of information. An example is given by section 4(3) of the Employment and Training Act 1973 which states 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.

[21] See eg National Audit Act 1983, s 8(5).

[22] See eg Local Government Finance Act 1992, sch 2 para 11(3); National Audit Act 1983, s 8(1), providing for "a right of access at all reasonable times".

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

[24] See eg Financial Services and Markets Act 2000, s 348.

[25] See eg Criminal Appeal Act 1995, s 17(2); Immigration and Asylum Act 1999, s 20(2A).

[26] Performance and Innovation Unit, *Privacy and data-sharing: The way forward for public services* (April 2002).

[27] R Thomas and M Walport, *Data Sharing Review Report* (July 2008) para 5.29; Performance and Innovation Unit, *Privacy and data-sharing: The way forward for public services* (April 2002).

[28] Local Government Finance Act 1992, sch 2 para 16; Crime and Disorder Act 1998, s 115.

[29] Offender Management Act 2007, s 14(6)(a).

4.14 By contrast, statutory gateways may state that they cannot override another provision contained in an enactment preventing disclosure of the information.[30] Statute may also require that the disclosing body is authorised by a specific enactment to share the data and that the use of these data is not prohibited. For example, section 18 of the Local Government Finance Act 1992 provides that regulations may include provision that an authority may use information which is obtained under another enactment but "does not fall within any prescribed description of information which cannot be used."

4.15 Gateways may also clarify common law duties or more general obligations as to secrecy, including professional codes of conduct. For example, they may state that regulations may include provisions that no duty of confidentiality or obligation as to secrecy may prevent the relevant authority from disclosing information. This is the case of regulations under section 251 of the National Health Service Act 2006, which allow the common law duty of confidence to be set aside in specific circumstances. [31]

4.16 The same information may be subject to various restrictions according to the purpose of the disclosure. For example, section 8 of the Statistics of Trade Act 1947 provides that if any information to be obtained for the purposes of a census under the Act is also obtainable under any other enactment which restricts the disclosure of information obtained thereunder, the Board may by order provide for the application of these additional restrictions, with or without any modifications.

The variety of approaches to statutory gateways

4.17 There is substantial variety in the form of statutory gateways. This reflects the fact that gateways are drafted in response to the detailed policy needs of the public bodies which rely upon them and the particular circumstances within which they operate. This in turn can make it difficult to draft broad general gateways for data sharing. This can result in highly detailed express provisions, such as section 14 of the Offender Management Act 2007 or section 105 of the Utilities Act 2000.

4.18 Even where the ordinary principles of interpretation would imply the data sharing powers necessary to carry out statutory functions, there can be a desire to draft more detailed express provisions. Even where the purposes of an express power are not made explicit, they will often be found as a matter of interpretation.

4.19 The relationship between statutory gateways and legal restrictions on sharing, including the Data Protection Act 1998, can be difficult to ascertain. This can lead to a pressure to draft more specific provisions about information in certain contexts. Fears of a failure to comply with the Data Protection Act 1998 or Human Rights Act 1998 can encourage the drafting of gateways that are more explicit than legally necessary. Such a practice can in turn reinforce existing misconceptions that explicit gateways are necessary in order to share data.

[30] See eg Offender Management Act 2007, s 14(6)(b).

[31] See also Local Government Finance Act 1992, sch 2 para 15(1); Anti-terrorism, Crime and Security Act 2001, s 19; Criminal Appeal Act 1995, s 17(4); Health and Social Care Act 2012, s 13Z3 (2).

4.20 Statutory gateways often fall short of compelling sharing. It may be felt that compulsion is undesirable in certain policy areas and it is better to preserve the professional judgment of the data sharer, for example in police and probation powers, such as section 14 of the Offender Management Act 2007. However, this can mean that the practice of data sharing is dependent on that judgement and the policy of public bodies. Express statutory powers, however, play a role in day-to-day data sharing, by giving public bodies a clear source of authority to which they can point when sharing data or encouraging others to do so.

Proposals for a general power and Parliamentary opposition

4.21 Both the 2002 report *Privacy and data-sharing – The way forward for public services*[32] and the Walport-Thomas review[33] proposed the enactment of a general power to enable information sharing gateways to be created by secondary legislation. An attempt to legislate such a power was made during the passage of what is now the Coroners and Justice Act 2009. Parliamentary opposition to the creation of such a wide power led to its withdrawal.[34]

4.22 Statutory gateways in general have raised concerns in terms of the adequacy of safeguards and parliamentary scrutiny. The Joint Committee on Human Rights, in a report in the Parliamentary session 2007-08,[35] observed that in recent years there had been a marked increase in the number of provisions in Government bills authorising wide powers to share personal information, including within the public sector. The Committee expressed its fundamental disagreement with the Government's approach of including very broad enabling provisions in primary legislation and leaving data protection safeguards to secondary legislation. It highlighted that mere compliance with the Human Rights Act and Data Protection Act was not enough and that setting out the purposes of data sharing and the limitations of data sharing powers in primary legislation would give a clear message to public sector staff about data protection, given the insufficient respect in the public sector for the right to respect for personal data.[36]

A positive obligation to share data: the Human Rights Act

4.23 In some circumstances, the Human Rights Act 1998 can impose a duty on public bodies to share data. Section 6(1) of the Human Rights Act provides that it is unlawful for a public authority to act in a way that is incompatible with Convention rights. Both article 2, the right to life and article 3, freedom from torture and inhuman or degrading treatment, imply positive obligations on the state to undertake proper investigations and take preventive measures.

[32] Performance and Innovation Unit, *Privacy and data-sharing: The way forward for public services* (April 2002). The report suggested introducing "changes to legislative processes for establishing data-sharing gateways, to allow data-sharing gateways to be introduced through secondary legislation, subject to a codified list of tangible safeguards and adequate Parliamentary scrutiny."

[33] R Thomas and M Walport, *Data Sharing Review Report* (July 2008).

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

[35] Data Protection and Human Rights, Report of the Joint Committee on Human Rights (2007-08) HL 72, HC 132.

[36] Data Protection and Human Rights, Report of the Joint Committee on Human Rights (2007-08) HL 72, HC 132 p 3.

4.24 For example, the European Court of Human Rights concluded in *Edwards* v *United Kingdom*[37] that the failure of state employed medical professionals, the police, and prosecutors to pass on information about the risk posed by a mentally ill detainee, resulted in a breach of the UK obligation to protect the life of his cellmate.

4.25 Similarly, where the relevant authorities (social services, school and health authorities) systematically failed to exchange information which could have been expected to avoid or at least minimise the risk of sexual abuse of children from a stepfather, article 3 was breached.[38]

POWERS IMPLIED FROM THE BODY'S OTHER STATUTORY POWERS AND FUNCTIONS

4.26 The nature and extent of a public authority's statutory power has to be found in the intention of Parliament in the relevant Act.[39] Where necessary, powers may be implied, as well as stated expressly.

4.27 Statutory powers are interpreted generously by the courts, impliedly authorising everything which can be regarded as incidental or consequential to the power itself.[40]

4.28 Requesting and disclosing data is often incidental to other statutory functions. The courts have accepted that disclosure of information may be necessary for the performance of a public duty or the public interest attaching to the functioning of a body. For example, in *Woolgar* v *Chief Constable of Sussex Police*, disclosure by the police of comments made in police interviews to a regulatory body was justified by the public interest in the proper functioning of the regulatory body, in circumstances where the general confidentiality of the information was maintained. The court also considered in this case that the police could, on its own initiative, disclose material, even without a request for disclosure from a regulatory body, if they felt it was necessary.[41]

4.29 The courts, however, will not condone the use for other purposes, in particular private interests, of information obtained by a public body for a different specific purpose.[42]

[37] *Edwards v United Kingdom* (2002) 35 ECHR 19 (App No 46477/99) at [61] to [64].

[38] *E v United Kingdom* (2003) 36 EHRR 31 (App No 33218/96) at [88].

[39] H W R Wade and C F Forsyth, *Administrative Law* (8th ed 2000) p 219.

[40] *Attorney General* v *Great Eastern Railway Co* [1880] 5 App Cas 473, by Lord Selborne LC.

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

[42] *Marcel v Commissioner of Police of the Metropolis* [1991] 2 WLR 1118. See also *Morris v Director of the Serious Fraud Office*, Chancery Division (Companies Court) [1993] Ch 372 3 WLR 1.

4.30 Some statutory powers are drafted in very broad terms. Section 111(1) of the Local Government Act 1972 provides that a local authority "shall have power to do anything...which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their statutory functions." The courts have noted the breadth of the power.[43]

4.31 This broad power should now also be read in the light of the general power conferred on local authorities by section 2(1) of the Local Government Act 2000, which provides that local authorities:

> have power to do anything which they consider is likely to achieve any one or more of the following objects—(a) the promotion or improvement of the economic well-being of their area; (b) the promotion or improvement of the social well-being of their area; (c) the promotion or improvement of the environmental well-being of their area.

4.32 These provisions provide wide powers to local authorities to share data. For example, in *R (Stanley, Marshall and Kelly)* v *Metropolitan Police Commissioner*,[44] the court accepted that this power gave local authorities a legal basis to disclose information about particular individuals who are the subjects of anti-social behaviour orders.

4.33 Although there is a broad interpretation of statutory provisions, the principle of legality requires that statutes be construed, if possible, not to infringe common law fundamental rights.[45] So, for example, the statutes could not be construed as allowing the government to override the right to confidential communication with a legal adviser protected by professional privilege, recognised as a common law right.[46]

NON STATUTORY SOURCES OF AUTHORITY TO SHARE DATA

4.34 Statute is not the only source of legal authority for data sharing. Ministers also exercise power under the prerogative or a "third source of authority".[47] This is sometimes expressed as a "residual liberty" of the government to act,[48] although prerogative powers are sometimes understood more narrowly as those powers that are unique to the Crown.

[43] *R (A) v Hertfordshire County Council* [2001] EWHC 211 (Admin) [2001] BLGR 435, by Keene J at [31].

[44] *R (Stanley, Marshall and Kelly) v Metropolitan Police Commissioner* [2004] EWHC 2229 (Admin) (2004) 168 JP 623 at [21].

[45] *R v Secretary of State for the Home Department ex parte Simms* [2000] 2 AC 115 at [131], by Lord Hoffmann. Interpretations will also have to be consistent with human rights: see Human Rights Act 1998, s 3.

[46] *R* v *Secretary of State for the Home Department, ex parte Leech* [1994] QB 198 at [211], by Steyn LJ; *R (Daly) v Secretary of State for the Home Department* [2001] UKHL 26, [2001] 2 AC 532 at [537] and [538], by Lord Bingham.

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

[48] M Elliott, quoted by B V Harris, "The 'third source' of authority for Government action revisited" [2007] *Law Quarterly Review* 225; see A V Dicey, *The Law of the Constitution* (10th ed) p 425; Wade, *Constitutional Fundamentals* (1989) pp 45 to 53 for discussion.

4.35 There is a great deal of controversy over the correct nomenclature for other sources of government power. The very use of the word "power" may conflate positive powers to act with the residual liberty of the Crown to act as a corporation sole, which are not powers but rather the absence of constraint. The term "common law powers" may obfuscate the distinction between prerogative and third source "power". De facto, residual, third source, secondary prerogative powers, pretended prerogative powers, common law discretionary powers and common law personified powers are all also used with differing shades of meaning reflecting the underlying theoretic and legal debates. In this paper, we use the phrase "non statutory sources of authority" to avoid taking a definitive view on these debates while ensuring that we are addressing all other sources of legal authority to share data.

4.36 Blackstone defined the prerogative in a highly limited way as "that special pre-eminence which the King hath, over and above all other persons, and out of the ordinary course of the common law, in right of his royal dignity". [49]

4.37 The courts have not been consistent in their approach to the precise basis of such authority.[50] In *Malone v Metropolitan Police Commissioner*, Sir Robert Megarry VC reasoned that if an activity by two public bodies can be "carried out without any breach of the law, it does not require any statutory or common law power to justify it: it can lawfully be done simply because there is nothing to make it unlawful".[51] By contrast, in *R v Somerset County Council ex parte Fewings* Laws J argued that while that was true of private individuals, who may do anything the law does not prohibit, the opposite is true for public bodies, whose action "must be justified by positive law".[52]

4.38 Reliance on the liberty of government to act to provide the non statutory authority of government has been a long standing practice in government, although it remains controversial.[53] In 1945, First Parliamentary Counsel Sir Granville Ram produced legal advice for the Government that later became known as "the Ram Doctrine":[54]

> A Minister of the Crown is not in the same position as a statutory corporation. … a Minister of the Crown, even though there may have been a statute authorising his appointment, is not a creature of

[49] Blackstone, *Commentaries* I p 239; H W R Wade and C F Forsyth, *Administrative Law* (8th ed 2000) p 222.

[50] See H W R Wade and C F Forsyth, *Administrative Law* (8th ed 2000) p 222, referring to *R v Criminal Injuries Compensation Board ex parte Lain* [1967] 2 QB 864. In this case, the compensation scheme was treated by the court as set up "under the prerogative", although the power to set up a trust is not unique to the Crown.

[51] *Malone v Metropolitan Police Commissioner* [1979] Ch 344, 367; *Malone v United Kingdom* (1985) 7 EHRR 14 (App 8691/79). That case involved phone tapping by the Post Office and the police.

[52] *R v Somerset County Council ex parte Fewings* [1995] 1 All ER 513, 524 by Laws J.

[53] A Lester and M Weait, "The use of ministerial powers without parliamentary authority: the Ram doctrine" [2003] *Public Law* 415; see also *R v Somerset County Council ex parte Fewings* [1995] 1 All ER 513, 524 by Laws J.

[54] This advice was first made public in 2003: Hansard, HC col WA12 (25 February 2003). See A Lester and M Weait, "The use of ministerial powers without parliamentary authority: the Ram doctrine" [2003] *Public Law* 415.

> statute and 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.[55]

4.39 The Crown as a corporation sole in common law has all the capacities and powers as a natural person,[56] subject to the ordinary law[57] and limited to the extent that there is express statutory provision.[58]

4.40 This approach was supported in *R v Secretary of State for Health, ex parte C*,[59] which held that the powers of the Secretary of State are not confined to those conferred by statute or prerogative. The appeal concerned the lawfulness of the Consultancy Service Index, a list maintained, without statutory basis, by the Department of Health comprising people about whom there were doubts as to their suitability to work with children.[60] After recalling the principle that neither the Crown nor a private individual may exercise their freedoms in such a way as to interfere with the rights of others without lawful authority, the Court concluded that maintaining this list was not, in itself, unlawful. This decision was followed in *R v Worcester County Council, ex parte SW*.[61]

4.41 In *R (Hooper) v. Secretary of State for Work and Pensions*,[62] the House of Lords held that the government could pay pensions to widowers on the basis of its "common law powers". This was so even though the payment of such pensions was not positively authorised by statute because the government is free, more generally, to do that which is not legally prohibited or contrary to the legal rights of others.

4.42 Although there is no comprehensive list of these powers, this third source is regarded as including a variety of powers that the government makes abundant use of on a regular basis, so that:

> to require parliamentary authority for every exercise of the common law powers exercisable by the Crown either it would impose upon Parliament an impossible burden or produce legislation in terms that simply reproduced the common law".[63]

[55] D Feldman, *English Public Law*, (2004) para 3.119.

[56] *R v Secretary of State for Health, ex parte C* [2000] 1 FLR 627; *Shrewsbury and Atcham Borough Council v Secretary of State for Communities and Local Government* [2008] EWCA Civ 148, [2008] 3 All ER 548.

[57] *Entick v Carrington* (1765) 19 St Tr 1030.

[58] *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.

[59] *R v Secretary of State for Health ex parte C* [2000] 1 FLR 627 at [13] to [21].

[60] Replaced since then by a list implemented under the Protection of Children Act 1999.

[61] *R v Worcester County Council, ex parte SW* [2000] HRLR 702, 713.

[62] *R (Hooper) v. Secretary of State for Work and Pensions* [2005] UKHL 29, [2005] 1 WLR 1681.

[63] A Lester and M Weait, "The use of ministerial powers without parliamentary authority: the Ram doctrine" [2003] *Public Law* 415.

4.43 Those powers are considered to include entering into contracts, employing staff, conveying property, settling a trust,[64] and other management functions not provided for by statute.[65] Just as making pamphlets available to the community has been seen as belonging to this non-statutory power,[66] it is possible that data may be shared by central government departments headed by a Minister of the Crown without requiring an express or implied statutory power in some cases. It is, however, controversial whether data sharing will always fall under the scope of such power and uncertainty may lead to a reluctance to rely on such powers, especially where the sharing in question is sensitive or controversial.

Ambit of non statutory powers

4.44 The prerogative or other common law powers may not be used in a "field which is already the subject of statutory regulation".[67] Where a power is inconsistent with the statutory scheme it may not be relied upon in order to avoid the requirements of a statute.[68] The existence of a statutory scheme may also impose public law duties which constrain the use of a non-statutory power.[69]

4.45 Ministers' common law powers may be limited by statute or otherwise by the requirements of public law,[70] the law of confidence or by agreement. They are subject to the legal rights of other legal persons,[71] for example the principles of judicial review and the protection conferred by the Human Rights Act.[72] In particular, if they cannot be clearly stated, they will fail to be "in accordance with the law", as demanded by the European Convention on Human Rights.[73] An additional limit is that parliamentary approval is needed where the action carried out by the Secretary of State involves the spending of public money.[74]

4.46 It can be difficult to identify whether an implied power or a common law power is relied upon. There is often uncertainty as to the precise legal basis for action.

The distinction between the Crown (through a Department of State)

64 See H W R Wade and C F Forsyth, *Administrative Law*, (8th ed 2000) p 222.

65 A Lester and M Weait, "The use of ministerial powers without parliamentary authority: the Ram doctrine" [2003] *Public Law* 415.

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

67 *Shrewsbury and Atcham BC v Secretary of State for Communities and Local Government* [2008] EWCA Civ 148, [2008] 3 All ER 548 at [23]. See also *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.

68 *Shrewsbury and Atcham Borough Council v Secretary of State for Communities and Local Government* [2008] EWCA Civ 148, [2008] 3 All ER 548 at [50].

69 *R v Home Secretary ex parte Fire Brigades Union* [1995] 2 AC 513.

70 It is not uncontroversial that instances of the third source of authority that are not prerogative powers but rather liberties of the Crown are subject to judicial review. See H W R Wade "Procedure and Prerogative in Public Law" (1985) 101 *Law Quarterly Review* 180 pp 190-194; Wade, letter to *The Times*, May 18, 1989; M Elliott, *The Constitutional Foundations of Judicial Review* (2001) pp 191 and 192.

71 *R v Secretary of State for Health ex parte C* [2000] 1 FLR 627, by Hale LJ.

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

73 *Malone v United Kingdom* (1985) 7 EHRR 14 (App 8691/79).

74 D Feldman, *English Public Law* (2004) para 3.120.

> exercising the same capacities as are held by a private person and a Secretary of State exercising powers not expressly conferred but ancillary to an express power is a fine one.[75]

4.47 *Shrewsbury and Atcham Borough Council* v *Secretary of State for Communities and Local Government* shows the diversity of the judicial views on this point.[76] Two borough councils sought judicial review of various decisions of the Secretary of State in preparation for legislative reform in respect of local government structures. Carnwath LJ observed that the Secretary of State's actions were governmental, undertaken for the public benefit and that it was not disputed that she could lawfully take preparatory steps in advance of promoting new legislation. He stated:

> I do not see that it is necessary to invoke a "third source" category for that purpose. I see it as simply a necessary and incidental part of the ordinary business of central government, part of which is the promotion of new policies through legislation.[77]

4.48 However, in a dissenting opinion, Richards LJ disagreed:

> it is still necessary to explain the basis on which that ordinary business of government is conducted, and the simple and satisfactory explanation is that it depends heavily on the "third source" of powers.[78]

4.49 The limits of this common law power are not clear.[79] Some judges such as Carnwath in the *Shrewsbury* case, consider that these powers should be qualified and only be exercised "for the public benefit" or for "identifiably 'governmental' purposes". Others reject such a qualification.[80]

4.50 Recently, in *R (New London College Limited)* v *Secretary of State for the Home Department*, Lord Sumption endorsed the third source concept but questioned how far the logic of the Crown acting as a natural person could go:

[75] *R v Worcester City Council ex parte SW* [2000] HRLR 702 QBD, 713.

[76] *Shrewsbury and Atcham BC v Secretary of State for Communities and Local Government* [2008] EWCA Civ 148, [2008] 3 All ER 548.

[77] *Shrewsbury and Atcham BC v Secretary of State for Communities and Local Government* [2008] EWCA Civ 148, [2008] 3 All ER 548 at [49].

[78] *Shrewsbury and Atcham BC v Secretary of State for Communities and Local Government* [2008] EWCA Civ 148, [2008] 3 All ER 548 at [73].

[79] See M Elliott, "Muddled thinking in the supreme court on the 'third source' of governmental authority", *Public law for everyone blog*, at http://publiclawforeveryone.wordpress.com/2013/07/23/muddled-thinking-in-the-supreme-court-on-the-third-source-of-governmental-authority (last visited 30 August 2013).

[80] See Richards LJ in *Shrewsbury and Atcham BC v Secretary of State for Communities and Local Government* [2008] EWCA Civ 148, [2008] 3 All ER 548 at [73].

> it is open to question whether the analogy with a natural person is really apt in the case of public or governmental action, as opposed 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.[81]

4.51 The observation is a non-binding comment, as Lord Sumption resolved the case on the basis of the proper interpretation of the Secretary of State's statutory powers, which covered a "range of ancillary and incidental administrative powers", including the power in question: a power to vet visa sponsors.[82]

4.52 However, data sharing will not always be a purely managerial act. Lord Sumption calls into question whether the third source covers all capacities of a natural person or merely consists of an ability to enter into private law transactions, such as contract, property and employment, to further general managerial objects. Managerial requirements would cover some forms of data sharing, for instance the acquisition, use and retention of data about government employees required for the general management of departments and in compliance with the general law and applicable statutory provisions. A data sharing scheme that goes beyond the managerial and approaches the governmental may fall outside the third source of authority. The distinction between purely managerial and governmental acts will often be difficult, especially where the desire to share data arises from a desire to improve the functioning and efficiency of government.

4.53 Lord Carnwath, in a concurring judgment, by contrast, expressed a strong opinion against the third source concept:

> I cannot accept Mr Swift's submission (if I understood it correctly) that there is some alternative, unidentified source of such powers, derived neither from the prerogative nor from any specific provision in the Act, but from the general responsibilities of the Secretary of State in this field. No authority was cited for that proposition and to my knowledge none exists. Mr Swift did not seek to rely on a possible "third source" of powers, by reference to the "controversial" line of authority mentioned by Lord Sumption (para 28). In my view he was wise not to do so.[83]

4.54 It is possible that this rejection reflects differences in the definition of the prerogative, which subjects claims to the definition and control of the common law rather than being a permission to act as a natural person. Nevertheless, it further reflects the controversy and uncertainty in the area. Reliance on non-statutory sources of authority in relation to data sharing might expose public bodies to an element of risk.

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

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

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

4.55 Although the power of a Minister of the Crown lawfully to share information with another public body may be derived from its public functions or common law powers, it is greatly constrained. It may only be exercised when statutory instruments do not require any other statutory intervention,[84] are not inconsistent with statute and do not impinge on individuals' rights, including the right to privacy as protected by article 8 of the European Convention on Human Rights. Therefore, for example, where a statute requires that an individual's consent is necessary, it will not be possible for a Secretary of State, on the basis of common law power, lawfully to share information with another government department without seeking consent as well.

4.56 The existence of non statutory authority to share information will often be a fact-specific question. In particular, the nature of the information to be collected and disclosed, the purposes for which it was to be collected and disclosed and the identity of the bodies acting as recipients will be relevant.[85]

4.57 Statutory vehicles have a number of advantages compared to common law powers:

(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) Ministers of the Crown often share the same powers as another entity which does not have any extra-statutory powers, so that they cannot rely on common law powers.

[84] See, for a compulsory statutory framework which imposes criminal sanctions on officials for non-compliance, Finance Act 1989, s 182.

[85] See *R v Secretary of State for Health, ex parte C* [2000] 1 FLR 627: this data collection and sharing was considered lawful on a number of grounds, in particular "the Index should only be consulted at the stage when the decision has been reached to offer employment. …It does not disclose what those relevant events were, unless there is a conviction. It leaves the decision as to whether to pursue the matter and what to make of those events to the prospective employer."

4.58 The relationships between express and implied powers and other non-statutory sources of authority can be complex. Uncertainty about whether the necessary powers to share data can be implied from statute or whether non-statutory sources of authority can be relied upon as a basis for data sharing in different contexts has encouraged a tendency to multiply detailed express statutory gateways.

4.59 It is not clear whether the reports of significant obstacles to data sharing are the result of inadequacies in the legal regime or the result of practical or cultural barriers to data sharing. The law is detailed and complex, reflecting the various principle and policy concerns underlying data sharing, which may create unnecessary obstacles to that sharing.

CHAPTER 5
CONSULTATION QUESTIONS

5.1 In this chapter, we set out our consultation questions. It would assist us if you answer the questions that are appropriate to you in this chapter. We would also be grateful to receive any other comments or observations you may have on the subject matter of this consultation paper. It may be that the way in which we have framed the questions does not reflect your understanding or experience. If so, please tell us, and explain why.

5.2 It would help us to analyse the responses if you set out briefly whether you are responding as an individual or on behalf of an organisation. If you are an individual, please indicate what particular expertise you have, or why you are particularly interested in data sharing. If you are responding for an organisation, please briefly explain the nature of the organisation and what it does.

Clarity and certainty of the law

5.3 The law surrounding data sharing is complex. It has been suggested that complexity and lack of clarity are hindrances to data sharing.

5.4 Question 1: Do you think that the current law on data sharing is sufficiently clear and certain? If not, please explain which parts of the law you find unclear or uncertain, and if possible please give examples of any problems that the lack of clarity or certainty causes.

Knowledge and application of the law

5.5 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?

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

Balancing data sharing and the rights of individuals

5.7 Some public bodies may feel that sharing information is too onerous and should be streamlined. However, there are also potential risks of data sharing alongside its benefits.

5.8 Question 4: If you think that there are inappropriate obstacles to data sharing between public bodies, please say what these are and where you have encountered them.

5.9 Question 5: If you think there should be more checks on data sharing, please say why (and indicate what those checks should be). If possible, please provide examples of sharing that is currently allowed that you think should not be.

5.10 Question 6: 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? If not, please say why.

Public attitudes to data sharing

5.11 Public bodies may encounter difficulties when collecting or sharing data about individuals due to the reluctance of individuals to allow their data to be shared. Public bodies themselves may also be reluctant to share data due to a lack of public trust in the ability of public bodies to handle their data.

5.12 Question 7: Does the reluctance of individuals to have their data shared by public bodies have an effect on data sharing? If possible, please provide examples.

5.13 Question 8: Do you think that there is a lack of public trust in public bodies which has an effect on data sharing? If so, is this because the public have a poor understanding of data sharing, or are they right to question sharing?

Availability of powers to share data

5.14 Question 9: Do you think that you, or your organisation, have sufficient powers to share the information you want to share with other organisations? If possible, please provide examples

5.15 Question 10: Do you think that others, who you think should disclose data to you, have sufficient powers to do so? If possible, please provide examples.

Misuse of data

5.16 There have been a number of high profile examples of data loss or the unauthorised disclosure of data.

5.17 Question 11: Do you think that the adverse consequences of unauthorised disclosure, including reputational damage or formal sanctioning, have an adverse effect on data sharing? If so, what sorts of consequences are most significant? If possible, please provide examples of each.

Other legal restrictions on the use of data

5.18 Public bodies' use of data can also be subject to private law rights, such as contractual, employment and intellectual property rights.

5.19 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.

5.20 Question 13: What benefits, if any, to data collection and sharing do these rights afford? If possible, please give examples.

5.21 Question 14: Do you use strategies to manage the effect, if any, of private law rights on data sharing? If possible, please give examples.

Lack of incentives or motivation to share

5.22 Data collection and sharing can require a large investment in terms of resources and time. A public body able to collect and share data may not consider data sharing to be a high priority to allow it to carry out its functions. Other public bodies may lack the resources to share data that would improve their ability to carry out their public functions. A public body may fail to share information because it does not have the necessary resources, in terms of staff, finance or time. We are interested in learning whether the distribution of those resources creates a lack of incentives to share data and what role managerial and organisational priorities and attitudes have on motivation to share data.

5.23 Question 15: Do you think that data sharing is prevented because public bodies lack the practical capacity or resources (lack of staff, money, time) to process and share data? If possible, please provide examples.

5.24 Question 16: What role does a lack of incentives or motivation play in failure to share appropriately? If possible, please provide examples.

Concerns about security

5.25 Public bodies holding relevant information may not be willing to share it due to concerns about their own security systems, the security system of the prospective recipient body or the security of the process of communicating data. A number of cases of data loss have resulted from security issues and have increased security concerns.

5.26 Question 17: What role do you think security concerns play in public bodies' reluctance to share data? If possible, please provide examples.

Quality issues

5.27 Problems with the quality of data, such as incomplete, out of date or inconsistent data, may be an obstacle to the transfer and linkage of data.

5.28 Question 18: What role do you think quality concerns play in public bodies' ability to share data? If possible, please provide examples.

Other possible causes

5.29 Question 19: Do you, or your organisation, find it difficult to secure the data you want because the holder of the information is unwilling to divulge it for other reasons? If so, what are the reasons? If possible, please provide examples.

5.30 Question 20: Are you, or your organisation, unwilling to divulge information for other reasons? If so, what are the reasons? If possible, please provide examples.

The use of shared data by public bodies

5.31 We are interested in the use of shared data by public bodies. This includes what information public bodies require and disclose, and from which and to which other public bodies. It also includes the purpose of sharing that data and the types of data that are shared, such as personal, sensitive personal, anonymised or de-identified data. We are also interested in consultees' views on the magnitude of the problems encountered in data sharing, for example, whether any difficulties in data sharing affect the possibility of sharing, cause delay or render sharing more onerous.

5.32 Question 21: Please describe the information you want or disclose, and the other public bodies concerned. For what purposes is the data required or disclosed? What types of data are concerned by this sharing? Through what process is it shared?

5.33 Question 22: Please describe the magnitude of any problem encountered in data sharing and the effects of such problems on data sharing.