

# CONTENTS

Annex A - The legal framework	2
Annex B - International comparisons	18
Annex C - Public attitudes research – a brief literature survey	27
Annex D - The analytical framework and privacy impact assessments	34
Annex E - The role of the PIU	42
Annex F - The Advisory Group and organisations consulted	43
Annex G - Selected bibliography	46

## ANNEX A: THE LEGAL FRAMEWORK

### Introduction<sup>1</sup>

A.01. English law does not set forth any coherent statement of a right to privacy. However, recent developments, notably the enactment of the Human Rights Act 1998 and the Data Protection Act 1998 – both now in force – represent significant advances in this area.

### Defining privacy

A.02. Problems of definition have been cited as one of the reasons why there is no coherent law of privacy in this country. Definition of ‘privacy’ is most often attempted by reference to the opposite, distinguishing that which is rightfully private from that which is public. When such a definition is applied in a human context, matters falling within the private sphere are distinguished from those in the public one; such matters may include a person’s home, family, religion, health or sexuality. However, even these most personal of matters may still be subject to legitimate intrusion.

### Defining data-sharing

A.03. If finding a working definition of privacy is elusive, the phrase ‘data-sharing’ may also be seen to cover a variety of different practices. The term is used in this PIU study to mean the disclosure of personal information within the public sector. It should be noted that while the term ‘data-sharing’ is

most often used in connection with the exchange of electronic records, the rules surveyed apply to both electronic data and relevant paper files.

A.04. Data-sharing may be undertaken on a single information item basis or on a block data-set basis. For the purposes of this review, no distinction is drawn between the various techniques involved in data-processing and data-matching. However, the nature of the data-sharing process, as well as the purpose of the action and the parties involved, needs to be considered in applying the law relating to data-sharing. For example, while the comparison of a single information item may be lawful in certain circumstances, a broad data-matching exercise between the same public authorities may not.

A.05. In this regard, while diverse emanations of the state are for certain legal purposes considered one entity, this doctrine of the ‘indivisibility of the Crown’ does not appear to apply in the data-sharing arena.<sup>2</sup> Government departments, agencies and other public bodies are each viewed as separate entities for the purpose of data-sharing and for privacy concerns. Moreover, the laws surveyed reveal that personal data collected by public bodies are regulated according to the specific purpose for which they were provided. Thus, even comparison of two sets of data collected by the same public authority for different purposes will be

<sup>1</sup> This review of the legal environment focuses on obligations applicable to authorities in the public sector (for the purposes of this paper ‘public authorities’).

<sup>2</sup> The existence of legislative ‘gateway powers’ authorising the disclosure of information between departments implies the necessity of such powers, contrary to the indivisibility doctrine (see Chapter 4). The Strasbourg Case of *MS v Sweden* concerning the interaction between a Swedish Health Service doctor and the Swedish Government reinforces that for the purposes of data-sharing, public authorities are treated as distinct.



subject to compliance with applicable data-sharing laws.

## Human rights and the right to respect for private life

### *The European Convention on Human Rights*

A.06. The European Convention on Human Rights ('the Convention') is a convention of the Council of Europe which was adopted in 1950 and ratified by the United Kingdom in 1951. It was designed to give binding effect to the guarantee of various rights and freedoms in the United Nations Declaration on Human Rights, adopted in 1948. Article 8 of the Convention provides that:

8.1 *“Everyone has the right to respect for his private and family life, his home and his correspondence.*

8.2 *“There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”*

A.07. The Convention thus enshrines a right to respect for individuals' private lives and prescribes the circumstances in which it is legitimate for a public authority to interfere with the enjoyment of this right. The Convention provides a qualified right – interference with the enjoyment of the right is expressly foreseen in certain circumstances. It is recognised that public authorities in pursuit of legitimate aims will have just cause

in a democratic society for intervening in individuals' private spheres.

A.08. Since the adoption of the Convention, citizens of Council of Europe member states have had the right to present cases to the European Commission and Court of Human Rights ('commission' and 'court'), established in Strasbourg. An international body of case law therefore exists which informs the extent to which the fundamental rights and freedoms enshrined in the Convention may find practical application. Applying general principles of international law, the Strasbourg court interprets the Convention in such a way as to give *practical effect to its objects and purpose*. Hence, in the case of Soering v UK<sup>3</sup> the court noted:

*In interpreting the Convention regard must be had to its special character as a treaty for the collective enforcement of human rights and fundamental freedoms ... Thus, the object and purpose of the Convention as an instrument for the protection of individual human beings require that its provisions be interpreted and applied so as to make its safeguards practical and effective.”*

A.09. As well as interpreting the Convention in such a way as to give practical effects to its objects and purpose, the court also recognises that the Convention is a *living instrument* that should be interpreted in a dynamic manner. This notion means that the court is not bound by precedent and instead recognises that the conditions prevailing at the time a case is considered may properly affect the outcome of a particular decision. Hence, the approach of the Strasbourg court, particularly when considering cases touched on by societal mores (e.g. corporal punishment, legitimacy of offspring and the rights of transsexuals),

<sup>3</sup> (1989) 11 EHRR 439.



has not remained fixed but rather has adapted to reflect prevailing conditions. With regard to Article 8 rights, developments in information and communication technologies have presented evolving challenges for judicial interpretation.

### **Restrictions of rights**

A.10. Article 8(2) specifically envisages circumstances in which interference with the rights contained in Article 8(1) is permitted. However, such interference is subject to the satisfaction of strict requirements to prevent abuse and compromise of personal rights. A number of principles have been adopted by the Strasbourg court when considering the extent of restrictions on the fundamental rights and freedoms set forth in the Convention.

A.11. **The principle of legality** is relevant in this context since interference with the Article 8 right is expressly limited to that which is “in accordance with the law”. The Strasbourg court has elucidated three rules applicable to satisfying this principle:

- The legal basis for any restriction on Convention rights must be identified and established. In essence this is determined by reference to domestic law. Legislation, delegated legislation, the common law and even the rules of a professional body may suffice.
- The law or rule must be *accessible*, i.e. persons likely to be affected must be able to find out what the law is that restricts their Convention right.
- The law or rule must be sufficiently certain that those likely to be affected must be able to understand its effect and thereby be able to order their conduct so as to avoid breaking the law.

A.12. The second key principle is **the principle of proportionality**. This principle is the mechanism by which the Strasbourg court seeks to determine whether a fair balance has been struck between the protection of the rights and freedoms of the individual and the interests of the community or society as a whole. In determining whether a restriction is *proportionate*, the court will consider the following questions:

- Have ‘relevant and sufficient reasons’ supporting the restriction been advanced?
- Is there a less restrictive alternative?<sup>4</sup>
- Is the decision-making process procedurally fair?
- Are there any safeguards against abuse?
- Does the restriction destroy the very essence of the Convention right?

A.13. The principle of proportionality has been held by the Strasbourg court to be particularly relevant in determining whether or not a restriction under Article 8(2) is “necessary in a democratic society”.<sup>5</sup> Thus the notion of necessity is not synonymous with ‘indispensability’ but rather implies a ‘pressing social need’.

A.14. In determining the extent to which contracting states may be under a positive obligation to promote “respect for private ... life”, the Strasbourg court has applied a wide **margin of appreciation**. This doctrine recognises that different contracting states have different cultural and societal standards. In view of this, the Strasbourg court considers that the domestic authorities of those states are better placed than an international court to determine the propriety of particular measures.

<sup>4</sup> [Campbell v UK](#) (1993) 15 EHRR 137 – the blanket opening of prisoners’ mail to establish whether any of it contained any prohibited material was not proportionate since a lesser measure of opening mail only where there was a reasonable ground to suspect that it contained such material would have sufficed.

<sup>5</sup> [Handyside v UK](#) (1979–80) 1 EHRR 711.



## **Rights included within Article 8 – a survey of relevant case law**

A.15. The cases of Gaskin v UK<sup>6</sup> concerned the rights of access to the files of social services concerning an individual's childhood in care. The court recognised that rights of access to such data must be tempered with the rights of contributors of such data, and the necessity for certain information to remain confidential to ensure reliable and objective contributions. A number of cases have considered the extent to which concerns of national security may temper rights regarding the collection, recording and access to personal data.<sup>7</sup>

A.16. *The recording of personal information for purposes of criminal investigation* falls with the scope of Article 8 but may be justified. The court accepted that information obtained by the police for the prevention and investigation of terrorism, in ways that represented prima facie interference with Article 8 rights, could be justified even when no criminal charges were brought and where there was no reasonable suspicion in relation to such an offence.<sup>8</sup> The action of the police authorities was capable of being justified in the interests of public safety and the prevention of crime, since the fight against terrorism was a pressing social need and the interference with the applicants' rights in those cases was relatively minor.

A.17. *Recording and storage of personal data in the medical field*, particularly data concerning treatment, will generally be justified unless there are failures in the safeguards on the use or disclosure of such data.<sup>9</sup>

A.18. *The provision of information to various other public authorities* has also been considered in Strasbourg. For instance, the compulsory provision of information to a national census, though prima facie an infringement, could nonetheless be justified if the individual's privacy was sufficiently protected since the aim of the economic well-being of the country was pursued.<sup>10</sup> Similarly, compulsion by the tax authorities to divulge details of private expenditure was an interference that could be justified in circumstances where the tax authorities legitimately required evidence concerning the disposition of substantial personal assets, although broad use of such powers was likely to be considered disproportionate.<sup>11</sup>

A.19. More particularly, the Strasbourg court has considered a number of cases in which the issue at question was *the disclosure of personal data between different public authorities*. It is clear that disclosure of personal information to third parties or the public constitutes interference with an individual's enjoyment of his private and family life to which the protection of personal data is of fundamental importance (e.g. Z v Finland<sup>12</sup>). For such interference to be justified, the public interest in disclosure must outweigh the individual's right to privacy, and consideration must be paid to the aim pursued in the disclosure and the safeguards employed in doing so.

<sup>6</sup> [1989] 12 EHRR 36.

<sup>7</sup> Martin v Switzerland 25099/94 (Dec.) 28 February 1996, Harman and Hewitt v UK (1989) 67 DR 88.

<sup>8</sup> McVeigh v UK 8022/77 (Rep) 18 March 1981, Murray v UK 19 EHRR 193.

<sup>9</sup> 14461/88 (Dec.) 9/7/91 71 DR 141 The retention of information concerning a patient's psychiatric confinement after their release was justified since strict rules of confidentiality applied even though the patient's confinement had been unlawful.

<sup>10</sup> 9702/82 (Dec.) 6/10/82 30 DR 239.

<sup>11</sup> 9804/82 (Dec.) 7 December 1982 31 DR 231.

<sup>12</sup> 25 February 1997, R. J. D., 1997-1, 31 at paragraph no. 95 "the Court will take into account that the protection of personal data, not least medical 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 Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general."



A.20. In *M. S. v Sweden*<sup>13</sup> the applicant contested the disclosure by her clinic of her medical history to the Social Insurance Office (SIO) to whom she had submitted a compensation claim in respect of an industrial injury. The Swedish Industrial Injury Insurance Act obliged the SIO to request the information in question and obliged public authorities (such as the applicant's health clinic) to submit information of importance to the application of the Act on named individuals to the SIO. The court found that the disclosure by the clinic in connection with the benefit application was legitimate. There was a basis in law for the disclosure, the disclosure pursued a legitimate aim (economic well-being of the country – directing public funds to deserving cases) and could be considered 'necessary in a democratic society'. In this final regard, the measure could be considered 'relevant and sufficient' in establishing the cause and existence of the applicant's back injury. Further, there were sufficient safeguards inherent in the system of disclosure since there was a duty of confidentiality, and abuse was punishable as a criminal offence. The measure was therefore not disproportionate to the legitimate aim pursued.

### **Human Rights Act 1998**

A.21. The Human Rights Act 1998 (HRA) allows UK citizens to assert their rights under the Convention in UK courts and tribunals – although they may ultimately continue to take cases to Strasbourg. Furthermore, Section 3(1) of the HRA provides that "so far as possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with Convention rights".<sup>14</sup> Section 6 provides

that "it is unlawful for a public authority to act in a way which is incompatible with a Convention right". Accordingly, legislation is to be given effect and public authorities will be obliged to act in a way which is compatible with an individual's right to respect for their private life. If individuals feel that public authorities have failed to do so, they may challenge this through the courts.

A.22. The HRA provides that "a court or tribunal in determining a decision which has arisen in connection with a Convention right must take into account the [Strasbourg jurisprudence]". That courts and tribunals should "take into account", rather than "be bound by" the Strasbourg jurisprudence, was justified in the Parliamentary passage of the HRA as reflecting both the living nature of the Convention and the doctrine of the 'margin of appreciation'. The Strasbourg case law was thus considered inappropriate for strict precedent purposes in the UK. Having noted as much, commentators on the new HRA have, not surprisingly, suggested that the UK courts are "generally unlikely to depart from Strasbourg Jurisprudence".<sup>15</sup>

### **Application of the HRA with regard to data-sharing by public authorities**

A.23. The courts in this country have yet to establish their own body of HRA case law in this area. However, from the Strasbourg jurisprudence it is clear that the legitimacy of any interference with this right will depend upon three factors:

- Is it in accordance with law?
- Does it pursue a legitimate aim?
- Can it be considered necessary in a democratic society?

<sup>13</sup> 74/1996/693/885.

<sup>14</sup> 'Convention right' defined in Section 1 of the HRA means the rights and fundamental freedoms set out in, *inter alia*, Articles 2–12 of the Convention.

<sup>15</sup> Grosz, Beatson and Duffy, *Human Rights The 1998 Act and the European Convention*.



A.24. The first element requires some legal basis to permit data-sharing. The second element, while according a broad range of legitimate aims, must nonetheless be satisfied. It is suggested that the majority of cases will turn on satisfying the third element. In determining whether any such restriction is ‘necessary in a democratic society’, courts are to look at all the facts and circumstances of the case in making this evaluation.<sup>16</sup>

A.25. In assessing whether the exercise of any power was itself proportionate, the courts will consider whether the decision-maker’s aims were legitimate and sufficiently well defined, and then whether the means chosen were necessary. Necessity of a measure will be determined by considering whether the ends could have been achieved in a less intrusive way. If the means were thus suitable as well as lawful, the final question is whether the ends sought to be achieved were properly balanced with the means chosen to achieve them. This assessment is far from straightforward, and satisfying each of these requirements will not always be possible to an objective standard. Nonetheless if public authorities can demonstrate that they have considered and attempted to adhere to these requirements, this will help ensure that the measures adopted are compliant with the requirements of the HRA.

A.26. The recent judgment by the House of Lords in the case of *ex parte Daly* set out a new test to be adopted by the courts in assessing the proportionality principle. In the judgment, Lord Steyn stated that the intensity of review is greater under the proportionality approach in three key respects:

- the court may need to consider the balance struck;

- the proportionality test may require attention to be directed to the relative weight accorded to interests and considerations; and
- the heightened scrutiny test is not necessarily appropriate to the protection of human rights.

## Data protection

### *A brief history of data protection*

A.27. In 1980 the OECD adopted ‘Guidelines on the Protection of Privacy and Transborder Flows of Personal Data’ to establish an international trade area within which personal data could be shared in a manner which protected individual privacy. This initiative was taken further by the Council of Europe which adopted a Convention in 1981, the *Convention on the Protection of Individuals with regard to the Automatic Processing of Personal Data* (Convention 108), which led to the adoption in the UK of the Data Protection Act 1984. By 1990 only six EU member states had ratified the Convention, and the Commission therefore proposed a Directive in the area to ensure that data could be transferred freely between member states.

A.28. Directive 95/46/EC “on the protection of individuals with regard to the processing of personal data and the free movement of such data” was finally adopted on 24 October 1995. This Directive required a further review of domestic data protection legislation, culminating in the Data Protection Act 1998.

### *Data Protection Acts*

A.29. The Data Protection Act 1998 (DPA), which updated the Data Protection Act 1984, regulates the processing and handling of personal data which have been lawfully

<sup>16</sup> *Sunday Times v United Kingdom* (No. 2) [1991] 14 EHRR 229.



obtained. As required by the Directive, the Act provides for a framework of notification by data controllers with an independent supervisory authority<sup>17</sup> – the Data Protection Commissioner (DPC).<sup>18</sup>

A.30. The DPA sets forth eight Data Protection Principles.<sup>19</sup> The basic purpose of the Principles is to enshrine broad formulations of acceptable processing practice. Under Schedule 1, personal data must be:

1. processed fairly and lawfully, and in particular must not be processed unless at least one of the conditions in Schedule 2 is met and, in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met;
2. data must be obtained for specified and lawful purposes and not further processed in any manner incompatible with those purposes;
3. adequate, relevant and not excessive;
4. accurate;
5. not kept longer than necessary;
6. processed in accordance with the data subject's rights;
7. secure; and
8. not transferred to countries without adequate protection.

A.31. Under the first Data Protection Principle, personal data are required to be processed not only “lawfully” in accordance with applicable law and the provisions of the Act, but also “fairly”. On each occasion that personal data are processed, the data controller must, as a requisite of fair and lawful processing, have legitimate grounds

for doing so in accordance with Schedule 2 of the Act (and with respect to sensitive personal data, Schedule 3 of the Act). Schedule 2 sets out the following possible grounds for these purposes:

1. processing with the consent of the data subject;
2. processing necessary for the performance of a contract to which the data subject is a party or which is necessary for entering into a contract;
3. processing which is necessary for compliance with a legal obligation other than one imposed by contract;
4. processing which is necessary in order to protect the vital interests<sup>20</sup> of the data subject;
5. processing which is necessary for the administration of justice, the exercise of any functions conferred by or under any enactment, the exercise of any functions of the Crown, a Minister of the Crown, or a government department, or the exercise of any other function of a public nature exercised in the public interest;
6. processing which is necessary for the purposes of the legitimate interests of the data controller or a third party to whom the data are disclosed, providing that these are not outweighed by the interests of the data subject.

A.32. When processing sensitive personal data it is necessary to satisfy both a condition from Schedule 2 and at least one from Schedule 3. The Schedule 3 conditions are:

1. processing with the explicit consent of the data subject;

<sup>17</sup> There are exemptions in the Act which mean that not all data controllers have to register with the Commissioner.

<sup>18</sup> Following the Freedom of Information Act 2000, which conferred additional responsibilities on the Data Protection Commissioner, the Office has been re-titled the Information Commissioner.

<sup>19</sup> The first five principles are drawn from the Principles set forth in Article 6 of the Directive while the remaining three reflect further provisions of the Directive set forth in the Directive.

<sup>20</sup> The approach adopted by the DPC is that reliance on this condition may only be claimed where the processing is necessary for matters of life and death.



2. processing necessary for the purpose of exercising or performing a legal right or obligation in the context of employment;
3. processing necessary to protect the vital interests of the data subject or another in cases where consent cannot be obtained;
4. processing of political, philosophical, religious or trade union data in connection with its legitimate interests by any non profit bodies;
5. processing of information made public as a result of steps deliberately taken by the data subject;
6. processing necessary in connection with legal proceedings or the seeking of legal advice;
7. processing necessary for the administration of justice, the performance of statutory functions, exercise of function of the Crown, Ministers or government departments;
8. processing of medical data by medical professionals or others owing an obligation of confidence to the data subject; and
9. ethnic monitoring.

A.33. In addition, there are further conditions created by order of the Secretary of State that allow public authorities to process sensitive personal data for certain purposes.<sup>21</sup> These fall into a number of broad categories:

- crime prevention, policing, and regulatory functions (subject to a substantial public interest test);
- insurance;
- equality monitoring in the area of disability and religious or other beliefs; and
- research.

A.34. Public authorities will normally be able to establish the legitimacy of their processing by reference to their statutory or public functions.<sup>22</sup> In some cases they may need to rely upon the final condition of Schedule 2, i.e. the pursuit of a legitimate interest not outweighed by the interests of the data subject.

A.35. Legitimate aims of public authorities are thus recognised in the grounds for fair and lawful processing, again reflecting the balance that is to be struck in protecting personal data while allowing the performance of certain functions that are necessary in a democratic society.

## *Regulation and enforcement of the Act*

### *(a) Rights given to data subjects*

A.36. The DPA provides individuals with rights by which they can take practical steps to protect their personal data from being unlawfully or unfairly processed:

- ***The right of subject access:***<sup>23</sup> Individuals are entitled to be informed by data controllers whether they are processing (directly or indirectly) personal data relating to them. If so, individuals have a right to be given a description of the personal data, the purposes for which it is being processed, the source of the data, and those (if any) to whom such data may be disclosed. Individuals also have the right to be given a copy of the information constituting the data held about them. A fee may be charged and the data controller should comply with the request promptly, and in any case within 40 days. The right of subject access is subject to certain exceptions provided for in sections 27 to 38 of, and Schedule 7 to, the DPA.
- ***The right to prevent processing likely to cause damage or distress:***<sup>24</sup> Data subjects

<sup>21</sup> The Data Protection (Processing of Personal Data) Order 2000, SI 2000 No. 417.

<sup>22</sup> See conditions 5 (Schedule 2) and 7 (Schedule 3) above.

<sup>23</sup> DPA 1998, s.7–9.

<sup>24</sup> DPA 1998, s.10.



are entitled to serve a written ‘data subject notice’ on data controllers requiring them not to begin, or to cease processing, personal data relating to them, where such processing is causing, or is likely to cause, unwarranted substantial damage distress to them or another. In case of dispute, upon application by the data subject, the court will consider the matter and, if satisfied, will order the data controller to take such steps as are necessary to comply with the notice.

- **The right to prevent processing for the purpose of direct marketing:**<sup>25</sup> Data subjects may, by written notice, require data controllers to refrain from processing personal data relating to them for the purpose of direct marketing.
- **Rights in relation to automated decision-taking:**<sup>26</sup> Data subjects are entitled to require a data controller to ensure that no decision which significantly affects them is based solely on the processing of their personal data by automatic means. Data subjects also have the right to be informed of the logic of any automated decision process taken concerning them.<sup>27</sup>
- **Rights to compensation in the event that an individual suffers damage as a result of processing by a data controller in contravention of the Act**<sup>28</sup> where the data controller is unable to prove that they have taken such care as is reasonable in all the circumstances to comply with the relevant requirement.
- **Rights to take action to rectify, block, erase or destroy data**<sup>29</sup> relating to them which is inaccurate (incorrect or misleading as to any matter of fact) or contains an expression of opinion which the court finds is based on the inaccurate data.
- **Right to request an Assessment by the Commissioner**<sup>30</sup> as to whether or not personal data have been or are being processed in accordance with the Act.

### (b) Role of the data protection commissioner

A.37. The first duty of the Data Protection Commissioner – now the Information Commissioner (IC) – is to promote good practice. In addition, the IC has the power to enforce compliance with the Data Protection Principles and to bring prosecutions for breaches of the criminal provisions in the Act. The Commissioner also has a duty to assess complaints from individuals.

A.38. The Act prohibits data controllers from processing personal data unless they are notified to the IC for the purpose of processing personal data<sup>31</sup> – although there are exemptions in the Act that enable some data controllers to process data without notifying the Commissioner. In notifying, they must inform the IC of the purposes for which they hold, use and disclose personal data, details of any actual or proposed transfers of the data outside the European Economic Area, and details of the security measures in place to protect the data. The IC maintains a register of notifications.

A.39. In addition to maintaining this register, the IC exercises certain supervisory functions:

- **Section 42 Assessments:** As noted above, data subjects may request the IC to carry out an assessment of whether any particular processing operation carried out by a data controller is likely to breach the provisions of the Act. The IC must make an assessment in such manner as appears to her to be appropriate, and must notify

<sup>25</sup> DPA 1998, s.11.

<sup>26</sup> DPA 1998, s.12.

<sup>27</sup> DPA 1998, s.7(1)(d).

<sup>28</sup> DPA 1998, s.13.

<sup>29</sup> DPA 1998, s.14.

<sup>30</sup> DPA 1998, s.42.

<sup>31</sup> DPA 1998, s.17.



the person who made the request whether she has made an assessment and any view formed or action taken as a result.

- **Information and Enforcement Notices:** Data controllers are under a duty to provide information to the IC to enable her to determine whether processing is lawful. To this end the IC may serve an *Information Notice* on data controllers requiring the supply of relevant information concerning their processing actions. If the IC is satisfied that a data controller has contravened or is contravening any of the data protection principles, she may serve an *Enforcement Notice* requiring compliance with the principle in question.<sup>32</sup> Failure to comply with an Enforcement Notice is an offence under the Act.
- The data controller has a right to appeal to the *Information Tribunal* concerning the service and extent of such notices. The Act also provides the IC with limited powers of search and entry, upon application a circuit judge.

A.40. In practice, the application of these various measures will often be sequential; Enforcement Notices may, on appeal, be upheld, withdrawn or amended by the Tribunal.

### **Application of the Act with regard to data-sharing**

A.41. The DPA regulates the use to which personal data are put each time they are processed. The Principles apply to all personal data processed by data controllers, unless the data controller is able to claim one of the exemptions listed in the Act. Controllers must comply with them, irrespective of whether they are required to notify and whether or not they are actually

notified. Notwithstanding that personal data may legitimately have been collected and held by the data controller for a particular processing purpose, if the data are subsequently processed in a manner which does not comply with the Data Protection Principles, that processing is *prima facie* unlawful.

A.42. Aside from general compliance with the Data Protection Principles, the second Data Protection Principle provides that “Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes”. The third Principle requires that “Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed”. The guidance in paragraph 5, Part II of Schedule 1 to the Act provides that:

*“the purpose or purposes for which personal data are obtained may in particular be specified in a notice given for the purposes of paragraph 2 by the data controller to the data subject, or [in the data controller’s notification to the IC].”*

A.43. In addition, paragraph 2 of Part II of Schedule 1 provides that, for the purposes of the 1st principle, personal data are not to be treated as processed fairly unless, in the case of data obtained from the data subject, the data controller ensures that certain information, including the purposes for which the data are intended to be processed, is provided to the data subject. In this manner the data subject is given an effective right to know, at the time in which his/her personal data are provided to the data controller, the purposes for which those data may be processed. It is also clear that data-sharing – the disclosure of personal data to

<sup>32</sup> DPA 1998, s. 40.



third parties by the data controller – falls within the broad definition of ‘processing’.

A.44. Paragraph 6 of Part II of Schedule 1 provides that:

*“In determining whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained, regard is to be had to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed.”*

A.45. Therefore, unless the disclosure to third parties (data-sharing) can properly be considered to be compatible with the purpose for which the data were obtained, the Act effectively prohibits data-sharing.<sup>33</sup> The Act contains certain exceptions to those of its provisions which may restrict or prohibit disclosures. Section 29(3) provides that the non-disclosure rules will be disapplied where the application of the requirements of the Act would be likely to prejudice one of the matters listed below:

- the prevention or detection of crime;
- the apprehension or prosecution of offenders; or
- the collection or assessment of any tax or duty.

A.46. Under Section 35 of the Act disclosures of personal data required by law or made in connection with legal proceedings are exempted from the non-disclosure requirement. Information disclosed for certain regulatory functions is also exempted from the non-disclosure requirement. In addition, the Secretary of State may make orders exempting from the non-disclosure provisions in the Act any disclosures of personal data made in circumstances specified in the order, “if he considers the exemption is necessary for the safeguarding

of the interests of the data subject or the rights and freedoms of any other individual”.<sup>34</sup> These exemptions again recognise the broad balance to be struck between the protection of personal data and the necessity of certain actions in exercise of the legitimate functions of public authorities.

## Limits on data-sharing imposed by administrative law

### *An introduction to administrative law*

A.47. Administrative law is the law that governs the actions of public authorities. According to well-established rules of administrative law, a public authority must possess the power to carry out what it intends to do. If not, its action will be *ultra vires*, i.e. beyond its lawful powers. For public authorities considering the lawfulness of any data-sharing they propose to undertake, a key question is therefore whether they have the power – or *vires* – to process personal data.

A.48. Some public bodies, such as local authorities, need to have a statutory basis for data-sharing. In addition to the necessity for a power to exist, it is also necessary that the power must be exercised for the purpose for which it was created. The case of *Hazell v Hammersmith and Fulham LBC*<sup>35</sup> makes clear that an action will be *ultra vires* notwithstanding the existence of a power, if a public authority uses the power to achieve a purpose that the power was not created to achieve. The Local Government Act 2000 invests local authorities with the power to promote “economic well-being”. Whether this new power may prove sufficiently wide to establish a gateway

<sup>33</sup> See generally DPA 1998, s. 27.

<sup>34</sup> DPA 1998, s. 38(2).

<sup>35</sup> [1992] 2 AC.1.



for data-sharing by local government is, as yet, untested.

A.49. As well as the specific powers provided to public authorities, it is clear that they may also undertake tasks “reasonably incidental” to the defined purpose. At first glance such a purposive approach might appear to create a broad power to permit public bodies to share data. Section 6 of the HRA provides that it is unlawful for a public authority to act in a way that is incompatible with a Convention right unless the use of such power is a duty required by primary legislation such that “the public authority could not have acted differently”. The Convention right in question (Article 8) foresees public authority interference in pursuit of legitimate aims. However, noting the applicability of the principle of legality, it seems fair to suggest that the HRA militates against an interpretation that data-sharing may be too readily inferred since it is apparent from the Strasbourg jurisprudence that the processing and disclosure to third parties of personal data falls within the scope of the Convention right.

### **The power of public authorities to share data**

A.50. Public authorities that wish to exchange electronic data or enter into information-sharing arrangements must have the power to do so. There is no universal statutory power permitting public authorities to disclose personal data to other such bodies in even limited circumstances.

A.51. Some public authorities are obliged to maintain public registers of what is essentially personal data, for instance the electoral register or the list of shareholders of public companies. However, there are a number of situations in which the non-disclosure

provisions of the DPA, countless other statutory provisions<sup>36</sup> and common law duties of confidence proscribe the disclosure or dissemination of personal data by public authorities.

A.52. In addition there exist a large number of specific statutory constraints that prevent the disclosure of data or its use for purposes other than that for which it was collected. For instance, Section 41 of the Education Act 1997 permits disclosure of information obtained in the course of school inspections *only* for the limited purpose of “report making or the inspection itself”.

A.53. Specific ‘gateway’ provisions apply in many statutory contexts, which may disapply criminal prohibitions where the individual consents to the disclosure of information.<sup>37</sup> However, the consent of a data subject alone will not suffice to provide a public authority with the power to share personal data. The *vires* of departments to enter into data-sharing agreements, where specific statutory constraints apply, depend in the first instance on the statutory construction and interpretation of that provision.

A.54. Without an overarching legislative gateway permitting the sharing of personal data, attention inevitably must focus on departmental statutory powers to share personal data. Perhaps the most well-publicised statutory gateway is that provided in s.122 and s.122A of the Social Security Administration Act 1992 (SSA).<sup>38</sup> This gateway provides power for the Inland Revenue and Customs & Excise to supply the Secretary of State for Work and Pensions with information for use in connection with the prevention of social security offences or for use in checking the accuracy of social security information. Specific powers are also granted under s.122B of the SSA relating to

<sup>36</sup> The 1993 White Paper *Open Government* identified more than 200 such provisions.

<sup>37</sup> See the Statistics of Trade Act 1947, Finance Act 1989 s.182(5).

<sup>38</sup> As inserted by the Social Security Administration (Fraud) Act 1997.



immigration and passport matters, and under s.122C social security information held by the Department for Work and Pensions (DWP) may be supplied to local authorities administering housing benefit or council tax benefit for the same fraud prevention purposes.

A.55. A further example of statutory gateways is that provided by s.115 of the Crime and Disorder Act 1998 (CDA). The CDA adopts an alternative broad approach by providing that:

*“any person who apart from this section would not have power to disclose information*

- (a) *to a relevant authority, or*
- (b) *to a person acting on behalf of such an authority*
- (c) *shall have the power to do so where the disclosure is necessary or expedient for the purposes of any provision of this Act.”*

A.56. The CDA requires the responsible authorities for a local government area to formulate and implement a strategy for the reduction of crime and disorder in the area. The CDA encourages the creation of so-called ‘Crime and Disorder Partnerships’, in which the “relevant authorities” (namely the chief police officer, police authority, local authority, probation committee or health authority) may enter into information-sharing arrangements in order to implement local strategies for the reduction of crime and disorder. S.115 provides public authorities with the *vires* to share personal data with the relevant authorities. Of course, any sharing of personal data must be in accordance with the provisions of the DPA.

A.57. The recent enactment of the Freedom of Information Act 2000 contains a broad exclusion<sup>39</sup> from the public access and disclosure requirements in relation to personal data as broadly defined in the DPA. The Freedom of Information Act will not therefore provide a mechanism whereby personal data may be disclosed by public authorities that would otherwise be precluded by provisions of the DPA.

A.58. The specific legislative gateway approach to data-sharing is now well established. These gateway powers have proved effective in providing a legal basis for both the processing and sharing of personal data by public authorities, since they provide the *vires* for public authorities to do so. These powers represent a lawful basis for processing of personal data under the Data Protection Principles and also seem likely to satisfy the HRA requirement of the restriction of the Article 8 Convention Right being “in accordance with law”.

## Common law

A.59. Common law jurisdictions have established torts to protect individuals’ rights to privacy. Torts are essentially civil wrongs that provide individuals with a cause of action for damages in respect of the breach of a legal duty. A number of common law torts afford protection to individuals’ private interests and their confidential information. For instance, the tort of defamation will protect individuals from certain forms of public dissemination of personal information for which there is no basis in fact; and the tort of trespass will protect individuals from intrusion on their private property. However, with regard to the use and disclosure of

<sup>39</sup> Freedom of Information Act 2000, s.40.



personal information, the tort of breach of confidence is clearly the most relevant.

### **Breach of confidence**

A.60. The common law tort of breach of confidence deals with unauthorised use or disclosure of certain types of confidential information and may protect such information on the basis of actual or deemed agreement to keep such information secret. The majority of cases have concerned trade secrets. However, the courts found no particular obstacle in accepting that personal information may be protected by a duty of confidence.<sup>40</sup> To establish that a breach of confidence has occurred, the following conditions must be satisfied:

- *the information in question must have the necessary “quality of confidence”.*<sup>41</sup> The nature of the information is relevant – the law “will not intervene to protect trivial tittle-tattle”. With regard to personal information, it should not be in the public domain or readily available from another source<sup>42</sup> and should have a certain degree of sensitivity;
- *if disclosed, the information must be communicated in circumstances giving rise to an obligation of confidence.* An obligation of confidence must exist, although this may be implied from circumstances (for instance, a photographic studio has been found to owe a duty of confidence with respect to its clients). An obligation of confidence is imposed by law if the circumstances are such that a person knew, or ought to have known, that the information is to be treated confidentially.<sup>43</sup> The duty of confidence owed by certain

persons is well established, for instance doctors, lawyers and bankers all owe duties of confidence to their clients. Further, where information is obliged to be provided to a public authority, an obligation of confidence will generally arise;<sup>44</sup> and

- *there must be an unauthorised use of the information by the party under the obligation of confidence.* Unauthorised use need not be dishonest<sup>45</sup> and it seems unnecessary to prove damage or detriment to establish a breach of confidence, although the damage or distress suffered will be relevant in determining the remedies applied by the court.

### **The duty of confidence and public authorities**

A.61. Information provided to public authorities will often, though not exclusively, be subject to an obligation of confidence. The courts have generally recognised three circumstances in which a public authority may ignore the duty of confidence it owes with regard to a particular information item:

- where there is legal requirement (either under statute or a court order) to disclose the information (for instance, notification of certain diseases to public health authorities);
- where there is an overriding duty to the public (for instance, the information concerns the commission of a criminal offence or relates to life-threatening circumstances);<sup>46</sup> or
- where the individual to whom the information relates has consented to the disclosure.

<sup>40</sup> For instance, *Stephens v Avery* [1988] 1 Ch 455 Browne-Wilkinson V-C accepted that “nothing in principle or authority... [supported] the view that information relating to sexual conduct cannot be the subject matter of a duty of confidence”.

<sup>41</sup> *Saltman Engineering Co. Ltd v Campbell Engineering Co. Ltd* (1948) RPC 203, Per Lord Greene MR. This requirement is normally satisfied by demonstrating that the information is not “public property and public knowledge”.

<sup>42</sup> *Elliott v Chief Constable of Wiltshire and others* Times Law Reports, 5 December 1996.

<sup>43</sup> *Coco v A N Clark (Engineers) Ltd* (1969) RPC 41.

<sup>44</sup> *Marcel v Commissioner of Police for the Metropolis* [1992] 1 All ER 72.

<sup>45</sup> *Seager v Copydex Ltd* [1967] 2 All ER 835.

<sup>46</sup> *Church of Scientology v Kaufman* [1972] 2 QB 84.



A.62. Furthermore, while there is an obligation on the part of the recipient of the information “not to take unfair advantage of it”, the purpose for which the information may be used need not necessarily be that for which it was provided. A breach of confidence will only occur where the disclosure of information is an abuse or unconscionable to a reasonable man.

A.63. The recent Court of Appeal judgment in the Source Informatics case<sup>47</sup> cited with approval the following passage from an Australian case<sup>48</sup>: “the courts should not be too ready to import an equitable obligation in a marginal case ... [else] the administration of business and government... might be unduly obstructed by use of too narrow a test”. Notwithstanding such a view, there can be no *carte blanche* for the broad dissemination of confidential information by public authorities. As stated by Lord Keith in Spycatcher (No 2)<sup>49</sup>: “as a general rule, it is in the public interest that confidences should be respected, and the encouragement of such respect may in itself constitute a sufficient ground for recognising and enforcing the obligation of confidence”.

### **Citizen’s Charter and privacy statements**

A.64. While not essential to establishing that a public authority owes a duty of confidence to an individual, statements in Citizen’s Charters of a vast range of public authorities contain commitments with regard to confidential information. For instance, the Inland Revenue *Taxpayers’ Charter* states:

*“In handling your affairs, we will:*

- *deal with them on a strictly confidential basis, within the law*
- *respect your privacy*
- *find a private room or space for you if you visit us to discuss your affairs, should you prefer it.”*

A.65. Such statements should leave citizens in no doubt that when they impart information to these public bodies they are owed a duty of confidence with respect to the use to which that information is put. It has also been suggested that statements such as these in Citizen’s Charter documents may give rise to a legitimate expectation on the part of the public to be consulted prior to any change in the use to which confidential information is put.<sup>50</sup>

### **Applying the duty of confidence in the context of privacy and data-sharing**

A.66. As noted in earlier chapters, the strictures of the DPA and HRA, at least in regard to personal information, are now pre-eminent in this area. However, as evidenced by the Source Informatics case, the common law tort of breach of confidence still applies today, not least in the way that public authorities handle confidential information. That case concerned the collection and sale of anonymised data from pharmacists revealing GPs’ prescribing patterns to Source Informatics for marketing purposes. The ruling at first instance suggested that the sale of such anonymised data represented a breach of the pharmacists’ duty of patient confidentiality. However, the Court of Appeal, overturning the initial judgment, held that the disclosure of information by pharmacists

<sup>47</sup> R v Department of Health, ex parte Source Informatics Ltd [2000] 1 All ER 793.

<sup>48</sup> SmithKline & French Laboratories (Australia) Ltd v Secretary to the Department of Community Services and Health (1991) 99 ALR 679.

<sup>49</sup> [1990] 1 AC 256.

<sup>50</sup> *Private lives and public powers: A guide to the law on the use and disclosure of information about living individuals by public bodies*, Data Protection Registrar p.26. The administrative law doctrine of legitimate expectations, although well developed in European case law, is in its infancy in English law. If applicable, the doctrine would act in such a way as to require a public authority which had given an express promise to treat information in a particular way to be held to its promise until such time as it had undergone a process of public consultation on the proposed change in practice.



did not constitute a breach of confidence, provided the identity of the patients was protected.

A.67. While it is clear that the common law remedy for breach of confidence may have a broad application to personal information collected by public authorities, its precise application will depend on a range of circumstances. The circumstances in which information subject to a duty of confidence may nonetheless be disclosed would certainly allow public authorities to share data, recognising as they do that a legal requirement or an overriding duty to the public could permit data-sharing notwithstanding a duty of confidence. However, since the action for breach of confidence has a broad application to personal information provided to public authorities, public authorities must be mindful of the extent of the duty they owe in considering whether to take part in data-sharing exercises or whether they are precluded from so doing.

## Concluding comments

A.68. There is no single body of law that circumscribes the action of public authorities with regard to privacy and the sharing of personal data. Instead, diverse strands of law converge in this area and lay down a tapestry of legal regulation. However, the HRA is clearly of prime significance. Not only does it effectively establish a right to the respect for individuals' private lives, but also it provides an obligation on public authorities to act in a way that is not incompatible with the Convention right. Moreover, since the HRA requires that, so far as possible, primary legislation and subordinate legislation must be read and given effect in a way that is compatible with Convention rights, its impact will be felt in the realms of data

protection and administrative law. It is equally clear from the wording of the Article 8 Convention right that certain action by public authorities which impinges on individuals' private spheres is legitimate in the broader interests of democratic society as a whole.

A.69. From the Strasbourg case law it is clear that the protection of personal data is an important aspect of respect for private life. Any interference with that right by means of data-sharing must: (1) be in accordance with law; (2) pursue a legitimate aim; and (3) be considered "necessary in a democratic society".<sup>51</sup> Compliance with these elements is essential, since in doing so a public authority satisfies not only the demands of the HRA but also the requirements of administrative law (*vires* for data-sharing), any duty of confidence it may owe, and many elements of the DPA. However, despite its wide scope, the HRA does not sweep away the requirements of the other elements of legal regulation. Public authorities must therefore be mindful to satisfy each of the DPA, HRA, administrative law and the common law in their treatment of personal data and in particular in the development of new data-sharing initiatives.

<sup>51</sup> From the ECHR Article 8 right (cf. paragraph A.06).

## ANNEX B: INTERNATIONAL COMPARISONS

### Introduction

B.01. It would be dangerous to translate directly the experiences of other countries, which may be similar to the UK in some respects but differ in others. For instance, key areas of divergence may include:

- the legal framework and the protection afforded to privacy in law;
- cultural attitudes to openness and privacy and the role of government;
- historical events, which may have left an indelible impression on public attitudes to privacy; and
- population size, which has an impact on the ease with which projects can be implemented.

### *Legal environment*

B.02. While EU States share certain overarching legal frameworks for privacy (the European Convention on Human Rights and the Data Protection Directive), there may nevertheless be important differences, including those derived from the fact that the UK is a common law jurisdiction, as opposed to civil law elsewhere.

B.03. For example, while the Directive – and the UK Data Protection Act based on it – requires data-processing to be lawful, different governments have taken different approaches to providing this legal basis. So while the UK has specific legislation covering bulk data-sharing between the Department for Work and Pensions and the Inland

Revenue, it might be that similar legislation does not exist in another EU country. In addition, in federal countries laws, standards or targets at the national level may differ from those covering provinces or regions.

B.04. Non-EU states may have completely different overall frameworks from the EU and yet display legal and cultural similarities (such as the common law and a less interventionist approach to markets). For example, the original Australian data protection legislation did not generally cover the private sector, but it is in the process of being extended, whereupon it will be reasonably similar to the UK's. Similarly, while US data protection law gives less protection to the citizen than EU laws, there is a specific tort of privacy, through which US citizens are able to sue in respect of breach of their privacy.

### *Cultural attitudes*

B.05. Certain countries appear to have attitudes radically different from those of the UK in this area. For example, in Sweden it is accepted that everyone's tax return can be inspected by anyone who cares to do so. Similarly, in many countries it is accepted that drivers should carry their licence with them at all times when driving.

B.06. However, a country which has a generally accepting attitude to increased use of computers and data-sharing may nevertheless have concerns over particular proposals because of historical resonance. For example, Dutch government files listing



religious affiliation were used by the Nazis to identify Jews. So a reasonably anodyne proposal concerning information on religion may touch a nerve there. There are other countries, notably certain states in Eastern Europe, which are wary about increased data-sharing because of recent historical experiences.

B.07. Another key question is the balance between market forces and direct state action to deliver e-commerce or a privacy infrastructure. This is likely to be based on political culture and the traditional role of the state, while the strength of the private sector in information and communication technology may also be relevant. A range of government responses can be considered. For instance, government could issue every citizen with an ID card containing a chip with a digital signature capability and insist on its use in all government–citizen interactions. Alternatively, the state could provide the infrastructure such as card readers in post offices and benefits agencies, while leaving citizens and the private sector the choice as to whether or not to use them for non-government-related activity.

### Infrastructure

B.08. If a country already has a national ID card, it is relatively straightforward to issue a smartcard version with functionality for public key cryptography. In the absence of such a pre-existing framework, however, options are more limited. The infrastructure question, then, is a major consideration when assessing whether a project can be ‘imported’ into the UK.

## Australia

### Background

B.09. The initial Australian data protection legislation, the Privacy Act 1988, did not generally cover the private sector, but is currently being updated. There is a Federal Privacy Commissioner, with a broadly similar remit to the UK Information Commissioner; the Privacy Act allows him to rule that a breach of an ‘information privacy principle’ is acceptable on public interest grounds, and he has published guidelines for departments wishing to apply for such a ruling.

B.10. The 1990 Data-matching Program (Assistance and Tax) Act is an example of a specific piece of legislation enabling data-matching to identify incorrect benefit payments. It enables the use of Tax File Numbers to match Tax Office data with information held by welfare agencies. More generally, in 1998 the Privacy Commissioner produced guidelines on the federal use of data-matching.

### The Australia card

B.11. A government proposal in the mid-1980s for a national ID card (the ‘Australia card’), the motivation for which seemed mainly to be to reduce tax evasion and social security fraud, was withdrawn after public protest, having originally received a reasonable level of public support. Press reports<sup>52</sup> suggest that concerns about privacy were reinforced by the realisation in certain industries that tax evasion was so widespread that if the card worked it would have very wide implications.<sup>53</sup>

<sup>52</sup> See, for example, *The Economist*, 3 October 1987.

<sup>53</sup> Similarities can be seen with the UK, where many police officers have refused to give DNA samples to a database designed to eliminate them from crime scenes, partly due to fears that their DNA may be used by the Child Support Agency for paternity tests (see e.g. *The Times*, 17 August 2000).



## Centrelink

B.12. Australia set up a one-stop shop for many government services, called Centrelink, in late 1997. It is based on 400 social security offices which have been adapted to provide services from other departments, plus 600 other outlets (visiting offices for remote areas, etc.). Centrelink is planning to allow electronic access to its services via multiple methods. In August 2000 there was a major breach of privacy rules when clients' personal identification numbers were printed on the *outside* of envelopes in a mailshot.

## Belgium

B.13. In mid-November 2000, Belgium announced plans to replace existing compulsory paper-based ID cards with cryptographic smart cards. It appears that these cards will include social security and driver's licence information as well as being ID cards, and they will be compulsory. At present, Belgians have an 'SIS' card for social security purposes, which has a small data storage capacity (name, etc.) but no cryptographic functions, and is used for identification at hospitals, pharmacies, etc.

B.14. Certification service providers (i.e. issuers of digital signatures) will be drawn from the private sector, and the citizen will be able to choose which authority he/she uses, and indeed whether to use the digital signature capacity of the card or not. It is possible that banking functions will also be placed on the card, and local authorities may extend it to include, for example, student data. The plan is for the compulsory functions to be available in three years' time; at present, the focus is on rolling out the technology infrastructure.

## Canada

### Background

B.15. Canada has a number of different privacy laws. At a federal level, there has been a Privacy Act since 1983, which is based on the OECD Guidelines and is thus broadly similar to EU data protection legislation except that it only applies to the public sector. However, the Personal Information Protection and Electronic Documents Act extended data protection to the private sector from 1 January 2001. In addition to federal law, the Canadian provinces also have data protection legislation, enforced by independent commissioners. There is also a Canadian Human Rights Act, broadly comparable to the European Convention on Human Rights (ECHR).

B.16. Many of the socio-political developments in Canada over the last two decades are similar to those in the UK, with significant parts of the public sector being privatised, which had the effect of taking sets of data, e.g. on employees, out of the scope of the 1983 data protection legislation as enterprises transferred from the public to the private sector.

B.17. In some instances, Canada seems further advanced than the UK, including in the deployment of certain privacy enhancing technologies. However, in other areas it seems significantly behind – for example, the issue of whether genetic data are actually covered by data protection legislation at all.

### Social Insurance Number

B.18. Canada does not have a formal national identification number, but the Social Insurance Number (SIN) is used beyond its original scope (in the absence of any legislative or other controls). The government's 1994 *Blueprint for Renewing Government Services Using Information*



*Technology* envisaged a ‘horizontally integrated’ public service supported by the building of a data warehouse to be indexed by some kind of national identification number, which would also bring significant efficiency gains for the government; the SIN was considered an obvious candidate.

B.19. However, the Canadian Auditor General questioned whether these benefits would actually materialise. Human Resource Development Canada (HRDC) echoed these concerns and those of the Federal Privacy Commissioner regarding the proposal. Public disquiet about the developments of a ‘big brother’ state has been present throughout this debate. These issues have not yet been resolved; those in favour of a national identification number appear to have failed to persuade the other stakeholders, while those opposed have failed to persuade the government to introduce statutory safeguards concerning the use of the SIN.

### ***HRDC Longitudinal Labour Force File***

B.20. Human Resource Development Canada was created out of a number of former federal departments and agencies, including the Departments of Employment, Immigration, Health & Welfare, Labour, and Citizenship & Immigration. The motivation for the merger was to improve services to the citizen. In 1997 the Federal Privacy Commissioner began a study of data held by the HRDC, which was by far the largest repository of personal data on Canadian citizens. The Commissioner discovered the existence of extensive longitudinal records containing up to 2,000 items of data on each individual, which had been compiled from data gathered by HRDC predecessor departments as well as information gathered subsequently by its various agencies and operational arms. The records included tax

returns, benefit information, immigration files, welfare files from provincial and municipal levels, training information and employment and social insurance master files.

B.21. The Privacy Commissioner expressed concern about the size of the individual files, their comprehensiveness and the lack of statutory safeguards, the absence of any retention or destruction policy and, above all, the fact that the database had been compiled largely without the knowledge of Canadian citizens. Publication of the Commissioner’s report appears to have resulted in a public outcry, the upshot of which was an announcement (on 29 May 2000) by the HRDC that it was dismantling the longitudinal file and was scrapping the software that allowed sharing with other agencies and returning the information which it had received from them.

### ***Social security benefits – use of smart cards***

B.22. Social security benefit recipients in Toronto have been issued with smart cards into which are programmed a biometric identifier, namely a fingerprint. The fingerprint is stored on the card and not in a central database and is encrypted using a non-reversible algorithm. The card is used both as a means of receiving payment and as a stored-value (smart money or ‘e-purse’) card. It is said to have had a major impact on social security fraud, as it makes it difficult to make multiple benefit claims. However, it has been criticised by the Privacy Commissioner because it subjects claimants to checks that other citizens do not have to tolerate and also it may allow spending profiles of claimants to be drawn up by researchers.



## Finland

### *Background*

B.23. A unique identifier (ID) is used as a key for all government information about individuals (social security, etc.). It is also used in banks, hospitals, etc., and the 1990 census was conducted simply by collating information from various databases using the unique ID. The unique ID begins with the person's date of birth followed by a three-digit number (even numbers for women, odd numbers for men) and a letter. The entire population and all buildings are registered with the Population Register Centre, whose database is used by government departments to avoid repeated requests for information and for verification of information supplied. The register can also be used by private sector companies, for example to ensure the accuracy of their mailing lists. Citizens can opt out of that use and a number of others.

B.24. Banks and employers provide the taxation authorities with electronic information about individuals, which allows the authorities to compile tax returns automatically as 'proposals'. Taxpayers can either accept or amend the proposal. Apparently, about two-thirds are accepted unchanged. The Finnish Government has replaced general departmental authorities to gather data by a more restrictive system, with the aim of increasing efficiency but also of not gathering unnecessary data.

### *FINEID (Finnish Electronic ID) Card*

B.25. It is not compulsory to have a national ID card in Finland, and many people use driving licences and passports as means of identification instead. Nevertheless, many people have one, the vast majority having an older version (i.e. not the FINEID card). They are issued by local police stations for a fee.

The newer FINEID version can either have a digital chip on it or not. They are still issued by the police, but the chip comes from the Government's Population Register Centre (PRC). The chip contains the bearer's private key for use in creating digital signatures, thus unambiguously identifying the bearer. The chip also contains a second, separate, private key that the bearer uses to decrypt messages. The Government set standards for this chip, and is installing card readers in public libraries and municipal service centres, so that card-holders can identify themselves, including over the Internet. Services have been made available since December 1999.

B.26. The standards are open and the Finnish Government encourages other uses of the card. For example, ICL (which is the contractor for parts of the project) uses it instead of a company ID card, including for access to the company's computers. Banks and insurance companies are also using it – for example, OKO Bank uses it to control access to bank accounts. The card can also be used to provide proof of identity over mobile phones, for access to WAP bank accounts, etc., if appropriate hardware is in place.

B.27. An electronic health data smart card using similar technology is also planned, again using chips supplied by the PRC. Similarly, local authorities will issue cards for various purposes, using chips supplied by the PRC but with no cross-certification/mutual recognition with the FINEID. The plan is to issue 50,000 FINEID cards initially; at the start of 2001, 7,000 had been issued with a chip and 7,000 without.



## France

### *Background*

B.28. The French constitution has always had a strong human rights aspect. A right to privacy is not explicitly mentioned, but a court ruling in 1994 decided that it was implicitly covered. The Commission Nationale de l'Informatique et des Libertés (CNIL) is larger and has greater scope than typical data protection authorities in other countries. National ID cards are compulsory, and in theory must be carried at all times.<sup>54</sup>

### *SESAM-Vital*

B.29. Since 1995 the Government has required doctors to use computers to transact with health insurance organisations as part of the SESAM-Vital project. Under the French social insurance system, someone needing medical treatment from their GP pays fees and then reclaims the sum concerned from the social security fund. This system has a significant administrative cost with large numbers of forms to be completed and processed. The French sought to replace this paper-based system with an electronic system based on smart cards, which were issued to everyone in the country. They contain people's medical files and, in principle, allow them to notify the social security fund of their treatment and reclaim fees electronically.

B.30. However, the system failed to realise the expected benefits. Doctors initially refused to invest in the PCs, smart card readers and other technology that would allow the smart cards to be used. This was because it is common practice in France for patients to consult several doctors about an ailment and to reclaim fees for each consultation, and doctors feared the new smart card technology would reveal the extent of over-treatment and so reduce their income.

<sup>54</sup> Some French sources dispute that the card is compulsory, but it is generally thought of as such.

## Ireland

### *Reach*

B.31. Reach is an agency established by the Irish Government to develop a strategy for the integration of public services and to develop and implement a framework for e-government. The basic objectives of Reach are:

- to radically improve the quality of service to personal and business customers of the Irish public service; and
- to develop a model for the electronic delivery of public services, known as the Public Services Broker, to help achieve that improvement.

B.32. Reach aims to provide a one-stop service for public service customers – enabling them to access related services at a single point of contact and to give their information, and prove their identity, once only, instead of having to go through the same procedure separately for each related service. To improve services in this way, internal business processes need to be integrated. Data-sharing is a key to facilitating the seamless delivery of public services – it promotes customer service and efficiency and reduces the need to call for physical documents. However, there is also the requirement of meeting customers' expectations that data are kept securely and that their privacy is respected.

B.33. In response to this, Reach is developing the Public Services Broker. The model seeks to balance the need for the maximum availability of data to public service agencies while ensuring the highest level of privacy and respect for data protection principles. The Public Services Broker model involves an integrated approach on three levels:



- a single access point to related services (integration across agencies, services and transactions);
- updated data available in real-time and data available for repeat transactions (integration across time); and
- the same data and experience available across the three main access channels – counter, telephone and the Internet (integration across channels).

B.34. The Public Services Broker model will be based on a hub architecture. Hubs at central, sectoral or local levels can be used to exchange data to support common services at the appropriate level and sectoral data stores can be supported by central authentication and security services. This means that data captured once can be reused by other agencies and on other occasions. The individual's right to privacy will be protected by enabling them to know, and exercise control over, how their personal information is used.

---

## The Netherlands

### *Background*

B.35. The Netherlands data protection authority strongly supports the use of privacy enhancing technologies to allow certain transactions to take place electronically without leaving a trail of identifying information when it is not necessary. Academic work has been done in the Netherlands on verifiable but untraceable transactions using public key cryptography. There are plans for a Privacy Incorporated Software Agent demonstrator to go live in 2003.

### *e-Government*

B.36. The Dutch Government is considering the wider introduction of smart cards for identification as part of its Electronic

Government Action Programme, but the study is in its preliminary stages. A pilot is being run on a voluntary contract between citizens and government for proactive service delivery. In this, the citizen chooses which services he/she would like (for example, automatic reminder that a passport needs renewing, having a tax return completed on their behalf – 1.2 million people in the Netherlands *file* their tax returns electronically – notification of eligibility for social security benefits, notification of proposed local traffic schemes) on the understanding that data-sharing will be required to deliver them. The citizen can cancel the contract at any time.

---

## Sweden

### *Background*

B.37. Sweden has a very open culture: for instance, anyone can look at anyone else's tax return. It has long-established and strong freedom of information legislation. In addition, there is a right to roam which allows anyone access to anyone else's land, without permission being needed.

B.38. There is no Government-issued ID card. ID cards are issued by the Post Office and banks. Drivers licences and passports are also accepted as proof of identity for daily transactions. The system is voluntary: applicants must be accompanied by a witness who already holds a valid ID card and have to provide an identity certificate from the National Tax Board. The Board produce these certificates on the basis of an individual's personal number, which is allocated on registration of birth. Almost 100% of Swedish adults carry a valid ID card.

### *Controlling access to government data*

B.39. In Sweden, police, tax, social security and some health and other government staff use cryptographic smart cards to gain access



to their respective computer systems. Combined with a password, this can authenticate that the person has the right to access the computer (or parts of it) and can in principle also provide an audit trail which cannot be repudiated (i.e. the employee cannot claim that someone else used his login). The cards carry different keys for signature and authentication, as this guards against security compromises. They also often carry a third key for 'confidentiality' uses. Fifty thousand smart cards are used in this way.

## USA

### *Background*

B.40. The US constitution does not explicitly mention privacy, but a number of Supreme Court decisions have developed legal doctrine concerning privacy protection, reading a right to it as being implicit in the constitution. In addition, there are specific laws, including one from 1988 on government data-matching, government codes of practice and industry self-regulatory codes.

B.41. In the USA, driver's licences, which must be presented on demand to the police without any need for reasonable cause, usually carry social security numbers too, thus giving police the key to private information such as tax details even though they are unrelated to crime or the vehicle. In fact, social security numbers are ubiquitous in the USA, often appearing on bank statements and so on, and sometimes even being used as personnel numbers by firms. In addition, a number of state Departments of Motor Vehicles sell driver's licence information for commercial use.

B.42. Freedom from government interference extends to businesses to a greater extent

than in the EU. For example, private sector use of personal data is much less regulated, as is genetic research. This appears to be leading to increased public concern, especially when the Internet is involved.

### *ACES and 'pay.gov'*

B.43. A number of departments of the federal government are developing on-line services related to education, based on ACES (Access Certificates for Electronic Services), trialling of which began in September 2000. More generally, the federal government is aiming at interoperability of its certificates with those used by state governments. The US Treasury Department is also developing 'pay.gov' as a central service for other Government agencies that receive money from the public. It is still in development, but the Government is looking at authenticating individuals by asking questions whose answers are only likely to be known by the people themselves (what is sometimes referred to as 'shared knowledge'). Confidence ratings will be used, i.e. if the consequences of a false claim to be somebody are small, fewer or less sensitive questions will be asked. It is possible that cryptographic smartcards will eventually be used for authentication, but there is concern that to date there have not been any large-scale deployments of public key infrastructure (PKI) technology.

### *The Freedom network*

B.44. The Freedom network is an overlay network that runs on top of the Internet. It uses layers of encryption to allow an end-user to engage in a wide variety of pseudonymous activity by hiding the user's real Internet provider address, e-mail address and other identifying information from counter-parties, eavesdroppers and active attempts to violate the user's privacy. Users are encouraged to create pseudonyms for each area in which



they want to preserve privacy. The various pseudonyms that someone uses cannot be associated with each other. Individual nodes in the network are operated by a number of commercial firms (the idea comes from a Canadian company called Zero Knowledge), so that no single operator has comprehensive knowledge of what data are flowing through the network. Similar products are available from anonymizer.com, SurfSecret, PrivadaProxy and others.

## Conclusions – lessons for the UK

B.45. An important caveat is that the majority of the electronic government initiatives described above are recent and have yet to be formally evaluated. Nevertheless, it is still possible to draw some broad conclusions from these examples that are relevant to the UK.

B.46. The experiences of the Australia Card, the HRDC Longitudinal Labour Force File and the French SESAM-Vital project all demonstrate the necessity of securing public buy-in to new initiatives. Public reaction to these initiatives varied with the degree of knowledge of the project and the potential impact on personal privacy, but full knowledge of the proposals, particularly in the Australian and Canadian examples, gave rise to strong opposition. By contrast, the voluntary nature of other proposals, such as the Dutch e-government proposals, have secured greater buy-in.

B.47. The examples cited also show that several governments around the world are looking to PKI as a key e-government enabler, providing solutions to identification and authentication issues. In the case of Belgium and Finland, PKI has been tacked onto an ID card, which has facilitated the

development of each initiative. The FINEID card's interoperability also demonstrates the extent to which technology can enable governments to provide key services with benefits for citizens.

B.48. While public attitudes in the majority of instances have demonstrated growing awareness of technology and of the potential impact on privacy, public and private sectors are in some cases lagging behind in responding to these concerns. Indeed, the response of governments to privacy concerns is varied, although there appears to be a general trend towards providing greater security for personal information in law.

B.49. Overall, the lessons for the UK can be summarised as:

- the importance of open and transparent consultative processes – particularly when considering large-scale information and data-related projects – to ensure that government is able to demonstrate the benefit to citizens of individual proposals and the safeguards and security measures in place to protect misuse of data;
- the developing use of PKI as a solution to identification and authentication issues and as an enabler for e-government; and
- technology's potential to enable the creation of new and innovative solutions – such as joined-up services and one-stop shops – and to deliver effective protection to personal privacy.

## ANNEX C: PUBLIC ATTITUDES RESEARCH – A BRIEF LITERATURE SURVEY

### Introduction

C.01. This is a selection of UK consumer attitudes surveys which shed some light on the question of the public's views of the potential for more intelligent data use in both the public and private sector and its impact on their privacy. There is a considerable amount of material covering the many different aspects of this complex question and many interpretations of its implications. Views on related, but in many ways significantly different, questions of the security of new information technologies, the competence of public services and the ethics of 'big business' and the media all overlie what are often summarised simply as 'privacy' attitudes. Furthermore, as discussed below, responses to privacy questions are highly sensitive to the form and context in which the questions are put. However, some clear general conclusions can be drawn about the factors that influence public attitudes to privacy and the conditions necessary to secure trust in public sector data-sharing.

#### What's new?

C.02. Concerns about privacy are not new. They have emerged before when the public has perceived a threat from the arrival of new information technologies. 'The right to be left alone' was most famously first articulated in 1890 in reaction to the spread of photography and cheap (newspaper) printing which threatened that "what is whispered in the closet shall be proclaimed from the housetops".<sup>55</sup> Threats to privacy

came to the public's attention again in the 1960s, with the introduction of computerised record-keeping systems; and again in the 1980s, with the arrival of database marketing and telemarketing. Each wave of concern was followed by legislation aimed at restoring a level of personal privacy.

C.03. Privacy as a public policy issue is not only a reaction to technology, however. Indeed, it is argued<sup>56</sup> that it is wrong to regard information technology as a driver of privacy concerns. Rather, new technologies provide occasional prompts to express consistently and deeply held views of the personal and social value of private life. The role of privacy in democracies and in the reconstruction of civil society after the Second World War was acknowledged in the Human Rights Convention of 1950 and has influenced the evolution of the legal landscape for the protection of privacy in the UK and Europe.<sup>57</sup>

### What recent surveys tell us ...

#### ... about general attitudes to privacy and data-sharing

C.04. Data protection is not an area that provokes strong *spontaneous* feelings. When invited to think explicitly about the issues involved in the use of their personal information, people can express sophisticated views, but in general, context-free surveys aimed at ranking concerns and attitudes to current public policies, few people identify

<sup>55</sup> M. J. Culnan, ' "How did they get my name?": An exploratory investigation of consumer attitudes towards secondary information use', *MIS Quarterly*, September 1993.

<sup>56</sup> Private communication, Perri 6, 8 March 2001.

<sup>57</sup> See Annex A for a fuller discussion of the legal aspects.



privacy and data-sharing issues, nor do they admit to having thought deeply about them to date.<sup>58</sup>

C.05. Once prompted, however, privacy is revealed as an important concern for most people.<sup>59</sup> Data protection surveys regularly show that protecting people's rights to privacy is a top public concern, beaten only by crime prevention and improving standards of education.<sup>60</sup> This is replicated internationally: Australian, Canadian and US surveys suggest that there has been a recent notable increase in the number of people very concerned about privacy intrusions of all kinds.<sup>61</sup> Rising trends in the proportion of landline telephone subscribers taking up privacy protection options (e.g. going ex-directory) also support this conclusion.<sup>62</sup>

### ... about knowledge of current data-sharing practices

C.06. People usually associate private companies with passing on information. Consumer perceptions of data-using organisations are largely based on popular media, personal stories and their own experiences of the Internet and direct marketing.<sup>63</sup> When asked to reflect on the use currently made of their personal data by *government*, many people have a less clear idea of what is actually being done with it.<sup>64</sup> They are divided about the extent to which the public bodies are allowed to – and

actually do – share information. Many people assume that the police and the courts in particular have access to a wide variety of data. Others quote their own experiences of public services to support their views that little data-sharing occurs.<sup>65</sup>

C.07. Lack of awareness about how personal information is shared is linked to a feeling that individuals have little control over it. This in turn often leads to a degree of suspicion and fear.<sup>66</sup> Findings suggest that if consumers do not know what information an organisation holds, they may create their own version of events. Consumers react to each organisation according to their feelings of trust and control.<sup>67</sup>

### ... and perceptions of the law on data and privacy protection

C.08. It is generally felt that if more people were aware of how to challenge the use of their personal information, they might do so. While there is relatively high awareness of the existence of data protection legislation, especially among the holders of data ('data controllers'),<sup>68</sup> there is much less knowledge of the detail of what that protection consists of. People tend to be confused about the precise purpose and application of the Data Protection Act.<sup>69</sup> Furthermore, few are optimistic that complaining would have a positive effect. Several pieces of research,<sup>70, 71</sup> show that consumers place little confidence

<sup>58</sup> *Consumer Privacy in the Information Age: a report from the National Consumer Council*, 1999.

<sup>59</sup> *Op cit.*

<sup>60</sup> *Data Protection Registrar's 14th Annual Report*, 1998.

<sup>61</sup> *Community Attitudes to Privacy*, Information Paper no 3, Australian Privacy Commissioner, August 1995.

<sup>62</sup> "In 1993 nineteen percent of people surveyed said they'd had an unlisted telephone number; this rose to 22% a year later", *Community Attitudes to Privacy*.

<sup>63</sup> *Proactive Online Privacy: scripting an informed dialogue to allay consumer fears*, Jupiter Communications, June 1999.

<sup>64</sup> *Attitudes towards confidentiality and survey research: some results from qualitative research*, ONS, November 2000.

<sup>65</sup> *Strategies for Reassurance*, Perri 6 for Cabinet Office, 2001.

<sup>66</sup> National Consumer Council, 1999

<sup>67</sup> *Privacy in the Marketplace*, CRICT, Brunel University, 1997.

<sup>68</sup> See annual tracking surveys in annual reports of the Office of the Information Commissioner.

<sup>69</sup> National Consumer Council, 1999.

<sup>70</sup> *The Future of Privacy*, Demos, 1998.

<sup>71</sup> Brunel University, 1997.



in the law. Proving that data has been misused and harm caused is seen as a major hurdle.<sup>72</sup>

### *The distinctions between private and public sector use of personal information*

C.09. A clear area of consensus in the survey literature is that the British public draws a clear distinction between the private and the public sectors in information-sharing matters. Public bodies are generally viewed with less suspicion than the commercial sector (although commercial banks consistently rank highly on trust scales).<sup>73</sup> Doctors and civil servants still command trust with confidential information and there is a perception of both the personal convenience and wider social benefits of shared information within the public sector.

C.10. Some research, however, makes the point that trust in an organisation is *not* determined simplistically by whether it is in the public or private sector; rather it is determined by a more discerning assessment of the values, controls and incentives on the organisation and its staff: “[thus,] while GPs and the NHS score highly, local councils score poorly in the various trust leagues”.<sup>74</sup> The distinction made between the public and private sector seems to be influenced by views about the tendency of the commercial sector to extract uncompensated financial gain from the use of individual information.

C.11. Where the private sector is involved in jointly providing a key public service and the controls and values are shared, the

distinction fades. For example, little concern is expressed about records passing around different parts of the National Health Service or shared with private hospitals: “the benefits are clear and doctors are trusted to respect the privacy of medical records. There is less approval for the idea of private contractors processing medical records for health care providers. Again, however, the benefits are seen to outweigh the concerns.”<sup>75</sup>

### *Generational differences in attitudes*

C.12. Among all groups, there seems to be little objection to providing personal data when the benefits, choices and avenues of redress are clear,<sup>76</sup> though there are some interesting generational differences. Younger groups tend to be less concerned about privacy, possibly because many surveys focus on *web* privacy and the young have a greater facility with, and understanding of, Internet and privacy enhancing technologies. Adults under 30 are also the most enthusiastic about the advantages of consumer-based information services and are more willing to engage in trade-offs involving consumer information uses than other segments of the population.<sup>77</sup> Positive attitudes towards the use of personal information for direct marketing result from an understanding of the benefits to the consumer, of the type of information used, and of the ability to control the use of personal information.<sup>78</sup>

C.13. Younger groups tend to be less convinced of the benefits of *public sector* data-sharing than older groups. Older people tend to see greater potential benefit from public sector data-sharing, often as a result of

<sup>72</sup> National Consumer Council, 1999.

<sup>73</sup> *British Social Attitudes Survey, 1997–98*, National Centre for Social Research [see [www.natcen.ac.uk](http://www.natcen.ac.uk)].

<sup>74</sup> *The Future of Privacy, Demos*, 1998.

<sup>75</sup> National Consumer Council, 1999.

<sup>76</sup> *IBM Multi-national Consumer Privacy Survey*, Louis Harris & Associates, October 1999.

<sup>77</sup> National Consumer Council, 1999.

<sup>78</sup> *Equifax Survey, 1990*, Louis Harris and Associates Inc.



their accumulated experience of interacting with public services.<sup>79</sup> However, they tend to feel less able to control or influence its conduct.

### *The influence of education and information*

C.14. People's ideas about data protection are set against a backdrop of conceptions about technology. Ignorance about technology and its possible developments create a sense of the unknown, as well as fears about lack of control. The majority's "privacy equilibrium" can easily be upset by unease about the future and technology.<sup>80</sup>

C.15. There is evidence of an information failure in privacy enhancing technology that may have implications for privacy attitudes: 86 per cent of on-line users surveyed were concerned about others accessing their personal information, but only 10 per cent of all users set their web browsers to reject cookies.<sup>81</sup> Fifty-six per cent did not know what cookies are. Of users with less than six months' experience, 62 per cent were very concerned, compared with 50 per cent of users who have been on-line for three or more years.<sup>82</sup> It may be deduced from this that better understanding of, and familiarity with, technology will reduce privacy concerns over time. But other evidence suggests that information and education may be a double-edged sword.

C.16 Surveys of public attitudes to biotechnology and human genetic information are useful for inferring attitudes to public sector data-sharing and privacy more generally because of similarities in:

- the asserted potential individual benefits they offer;

- the way questions of information, education and trust in institutions read across issues; and
- the constant evolution of technology, and the consequent implications for individual knowledge and uncertainty.

C.17. There are some significant differences, however, which make inferences from one subject field to another imperfect: biotechnology and human genetic information carry more moral and ethical concerns, while data-sharing concerns tend to have a more limited social and political content. Individual attitudes to data-sharing and privacy tend to be based on a balance of benefits and costs which are more personal and immediate, while in the field of biotechnology the balance of concerns tend to be global and longer term. Finally, knowledge in the field of privacy and data-sharing is more likely to be information about administrative processes; whereas in biotechnology, knowledge entails wider education about the science and its potential.

C.18. Nevertheless, it is instructive to examine the formation of public attitudes by looking at specifically interested sub-groups. In the field of biotechnology, those who claim they are informed are those who are most likely to see the benefits. But they are not less critical; they are more likely to see the disadvantages and to show lower confidence in controls over the application of the technology.<sup>83</sup> Knowledge of biotechnology encourages people to have more clear-cut opinions.<sup>84</sup> Those with low levels of scientific understanding show less consistent and less discriminatory attitudes to science. Groups with an identifiable interest in biotechnology have fairly stable attitudes about it which are difficult to change.<sup>85</sup>

<sup>79</sup> *Strategies for Reassurance*, Perri 6 for Cabinet Office, 2002.

<sup>80</sup> The Future Foundation, 1997.

<sup>81</sup> Put simply, cookies enable websites to trace a user's Internet browsing, enabling the site to recognise when a user returns.

<sup>82</sup> *Pew Internet Survey on FT.com Community*, September 2000.

<sup>83</sup> *Food Future*, The Food and Drink Federation, 1995.

<sup>84</sup> *The Europeans and Modern Biotechnology*, Eurobarometer, 1997.

<sup>85</sup> Martin S. and Tait J. *Attitudes of selected public groups in the UK to biotechnology for the European Federation of Biotechnology*, 1992.



C.19. A general wariness of big business has led to strong negative views of use and possible abuse of genetic tests in work and insurance. The right to privacy is a key issue. Genetic databases are regarded positively if they advance medical research but there are strong concerns over anonymity and consent.

### *'Privacy pragmatism'?*

C.20. A theory of 'privacy pragmatism' emerges from most survey work. Views on both the private consumer value of personalised marketing and the social value of shared knowledge for such things as research and crime prevention support this, as does the clear evidence that the existence of effective choices and controls qualifies seemingly absolute privacy values.

C.21. Evidence from the commercial world is that consumers prefer to give out personal information when they receive specific benefits for sharing it, including the chance to win free goods through sweepstakes and promotions. Thirty per cent of on-line shoppers will give out some data to their favourite retailers even when they are not buying. Access to members-only sections of a site get approximately one-fifth of web-users to share private information.<sup>86</sup> The demand for personalisation of web content continues to grow; the number of personalised websites has increased tenfold over the past two years: "Today's cybercitizens are significantly more likely to share private demographic information in return for personalisation ... but 49 per cent feel that a site that shares their information is invading their privacy".<sup>87</sup>

C.22. There is evidence that a significant proportion of the population is fatalistic about information-sharing, particularly in the private sector: one survey indicates that 70 per cent felt that they could not avoid giving their personal details to companies.<sup>88</sup> This has led some to conclude that personal privacy concerns are pragmatically conceding to a new world (or a return to an old one) of open information. Others have argued that this "fatalism"<sup>89</sup> warrants attention by policy makers because it is in fact not a result of temperament and technology but a response to a sense of lack of control and choice. More importantly, the evidence from other fields is that fatalism is not a stable position and that events may flip it into a fundamentalist backlash.<sup>90</sup>

C.23. The critical point is the existence of practical measures for reassurance, control and security. In both the public and the private sectors they clearly reduce 'privacy protectionism'. Individuals who believe they can exert more control over events are less likely to perceive that their privacy is being invaded.<sup>91</sup> Research suggests that, in general, individuals are less likely to perceive information practices as privacy invasive when:

- information is collected in the context of an existing relationship;
- there is a perceived ability to control future use of the information;
- the information collected is relevant to the transaction; and
- it is believed that the information will be used to draw reliable and valid inferences.<sup>92</sup>

<sup>86</sup> Forrester Research Inc, 2000.

<sup>87</sup> *Privacy vs. Personalisation*, Cyber Dialogue, 2000.

<sup>88</sup> *The New Information Trade*, The Future Foundation, 1997.

<sup>89</sup> *The Future of Privacy*, Perri 6, Demos, 1998.

<sup>90</sup> *Ibid.*

<sup>91</sup> *Ibid.*

<sup>92</sup> Culnan, 1993.

## The results of research commissioned by the Cabinet Office

C.24. The literature survey sheds useful light on the work of the project team. But it leaves some important gaps. Much of the survey material relates to commercial data use, to web privacy and security issues especially or to quite specific examples of sensitive, confidential information. Some of the important research on public sector data use and privacy is already somewhat dated. The existing literature does not investigate in the necessary depth the supposed ‘risk-benefit trade-off’ that the public appears to make nor test their opinion of the protections in principle on offer to them.

C.25. It was therefore decided to commission a focus group study<sup>93</sup> to explore more deeply how far people are aware of the sharing of data about them across public services; what risks and benefits they recognise; how they think about the relationship between the two; and their views about the solutions and safeguards that might enable an increase in public trust around data-sharing. The following is a summary of the conclusions of that study.

### Understanding

C.26. Different groups of people probably under- and over-estimate the extent of sharing of personal information about them by public bodies. Some proximate factors that seem to predict how people are biased in these respects are the extent to which they are frequent or infrequent users of public services, and the extent to which they are voluntary or involuntary consumers of those services. Most groups are not typically persuaded that widespread data-sharing is now inevitable, still less resigned to it.

### Benefits

C.27. Few groups felt very positively about the benefits, although some of those who saw themselves as taxpayers first felt that fraud control and crime detection were of real importance. However, most of the benefits that people could identify were ones that they thought were essentially benefits for public services rather than ones they would personally gain from. Even exercises and prompts to elicit benefit perception sometimes tended to elicit risk perception instead. People nearly always found themselves unable to concentrate on benefits without also calling for safeguards against risks. Even those who lamented the lack of data-sharing thought in this way.

C.28. The group that was most committed to the argument that the advantages outweighed the disadvantages still demanded safeguards against risks. Even the benefit from data-sharing of eliminating or reducing multiple requests for the same information failed to attract much excitement and interest. Some participants were doubtful that it would materialise. Such benefits as targeting of proactive service offering or personalisation were regarded with some scepticism. Those focus groups in which people attached greatest weight to the benefits to public services were the ones whose members used public services least frequently. The converse is also true, namely, that those who attached the least weight to the benefits were those who used public services most frequently and intensively.

<sup>93</sup> *Strategies for Reassurance: Public concerns about privacy and data-sharing in government.* Perri 6 for the Cabinet Office, March 2002.



## Risks

C.29. The following risks were identified by the focus groups:

- errors in data-handling;
- infection with inaccurate data;
- misidentification;
- rigidity in data structure and handling, rigid services;
- malicious provision of data from anonymous sources;
- reversal of the presumption of innocence;
- unjust inference (e.g. jumping to conclusions, decisions to deny entitlement unfairly based on inferences from matched data, where each of the elements matched might have been correct in its original context but where the combination is misleading);
- 'soft' data (e.g. professionals' opinions or assessments of individuals as clients);
- unauthorised access to personal information;
- unauthorised informal disclosure of personal information;
- arbitrary use of power;
- failure to identify criminals, people not entitled to services but claiming or using them, etc.; and
- being subject to physical oversight (e.g. being seen to be a user of certain stigmatised public services).

C.30. By contrast with the perceived benefits, significantly more categories of perceived risk were elicited without prompting in almost every group, and in every group, the emotional charge attached to the risks was greater than that attached to the benefits.

## Principles

C.31. Although in several groups the principle was invoked that 'If you have nothing to hide, you should not be concerned about privacy', no one used it consistently, and even its toughest advocates dropped it when the discussion turned to information that even they thought 'personal'. All the groups agreed that some things were personal, but struggled to define this with lists of categories of information or with exceptions. Most resorted therefore to some way of trying to decide when information might be shared, depending on the purpose for which agencies might want the information. That information should only be collected, used and disclosed for a purpose of which the data subject is aware is, of course, the first data protection principle. Participants had a rich vocabulary for discussing the idea of *purpose*, ranging from terms such as 'use' through 'relevance' to the idea of a 'need to know' principle.

C.32. All the groups attached much more importance than had been expected to a 'forgiveness' principle whereby, after a certain point, and with the obvious exception of serious crimes, information about misdemeanours sufficiently far in the past should be deleted from records.

C.33. All the focus groups insisted upon the principle that there should be complete transparency from public services about what data-sharing is, or will be, carried out, for what purpose, which categories of data will be involved, what procedures will be used, what safeguards will be in place, and how those constraints will be enforced. Meeting this standard is probably a precondition of achieving public trust in data-sharing.

## ANNEX D: THE ANALYTICAL FRAMEWORK AND PRIVACY IMPACT ASSESSMENTS

### The analytical framework

#### What is it?

D.01. A strategy for advancing both data-sharing and privacy needs to be supported by a clear framework for decision-making. Whenever the costs, risks and benefits of a policy approach are unfamiliar, diffuse, indirect or occur over different timescales, they are neither easily quantifiable nor comparable. Standard cost-benefit techniques are incomplete for the purpose. It is important, therefore, to have a clear process by which the costs and benefits can be identified and described.

D.02. An analytical framework<sup>94</sup> has been designed to aid this process. It aims to condense the decision process into its basic steps. At each step, it attempts to define, by grouping into discrete types, the different benefits, risks and costs that may arise. By giving conceptual clarity to each of the different costs and benefits, the framework helps in developing ways of describing, measuring and adducing evidence to each. It will also help in identifying where the particular gaps are in knowledge and methods and where more research and guidance would be useful.

D.03. The analytical framework reflects the privacy principles that have been developed in this report and ensures that they influence public bodies' decision-making processes. Those principles are:

- data-sharing by public bodies must be justified;
- the process of justification should be transparent;
- safeguards should be in place; and
- public trust and confidence must be nurtured.

D.04. The framework, by making explicit and emphasising the balancing question, "how large are the benefits of increased data-sharing *in relation* to the costs and risks", and indicating how evidence for each may be gathered, aims to give genuine significance to this moment in the decision-making process. The framework also asks the question about the practical measures to put in place that will ensure that the net benefits identified at appraisal do indeed materialise.

D.05. The aim of the framework is to assist organisations in considering the important questions surrounding better use of information in order to improve delivery of their objectives. The Lord Chancellor's Department should provide guidance and support, and should further develop both the analytical framework and related tools (such as privacy impact assessments, discussed below). But the decisions as to when to use the framework and other diagnostic aides will remain with individual organisations.

#### Why is it needed?

D.06. The analytical framework developed during the course of this report has been

<sup>94</sup> See pp.126–133 of the report.



tested on three case studies, and modified as a result. Overall, the three departments concerned said that they found it an extremely useful tool. More generally, there is a demand amongst public services for analytical assistance of the sort provided by the framework: according to a MORI survey commissioned for this report, three-quarters of civil servants with data-related responsibilities agreed that there were privacy implications in their departments' plans for increased data-sharing, but they were divided on whether those implications would be positive or negative.<sup>95</sup>

D.07. A systematic checklist approach helps with the appraisal of any new policy where quantitative evidence is lacking. It is particularly valuable at this stage in the data-sharing and privacy debate because it will:

- **ensure consistency of approach across the public sector when considering privacy impacts.** This is important in itself, for reasons of analytical rigour and clarity. It is also important for reasons of public confidence and acceptability that public services are seen to require consistency;
- **integrate the consideration of privacy costs and risks into a wider cost-benefit analysis.** This signals the intention to give to privacy considerations a weight in the appraisal process equal to that of traditionally more quantifiable measures. In practical project terms, it should also encourage IT systems to be designed with privacy in mind;
- **ensure an opportunity for unfamiliar, unanticipated and indirect costs and benefits of data-sharing to be identified.** By requiring these measures to be considered at an early stage, the framework provides a discipline that will discourage the natural tendency to avoid

taking the measure of new and difficult cost issues. It should thereby help to stimulate the collection of evidence of benefits, costs and risks and contribute to a more fully developed appraisal methodology for information management in the longer term;

- **contribute to transparency.** The systematic approach of the framework aims to facilitate understanding by all of the decision-making process; by making clear how an overall decision is reached, on what evidence, and with what qualifications, it can better be challenged – or more comfortably accepted;
- **constitute something of a systematic assessment of need which compliance with the proportionality requirement of the Human Rights Act implies.** The experience of challenges by the ECHR to date suggests that weight is given to evidence of genuine attempts by governments to assess the appropriateness of their actions. The risk of adverse comment or enforcement by the Information Commissioner or by private litigation by data subjects should also be reduced.

### *When should the analytical framework be used?*

D.08. The analytical framework covers the questions that need to be asked when a policy initiative, a business re-engineering process or an IT project encompasses any element of storing and using a citizen's data electronically, even if only as a minor part of the proposal. The question which should be kept in mind when considering **any** new initiative is: *Does this policy imply the use of personal data – either new or old data – for a new purpose?*

<sup>95</sup> *Attitudes towards data-sharing: a survey among civil servants*, MORI research study conducted for the Performance and Innovation Unit, November 2000–January 2001.



D.09. The question can be unpacked further:

- *Is the data being used for the original aim but in a different context?* E.g. where a patient's GP notes are passed on to a hospital when there is a referral;
- *Is the data being used across organisations to create a new service?* E.g. where an applicant for exemption from vehicle road tax on the grounds of disability grants DTLR permission to approach the Benefits Agency for confirmation of the disability and therefore does not need to apply for and present a certificate from the Agency; and
- *Is the data being used for a completely different purpose from the original intention?* E.g. where Inland Revenue data on incomes, collected for taxation purposes, is used when considering the seizure of criminal assets.

D.10. It will be important for public sector bodies to examine privacy issues as soon as a policy initiative is mooted. This will be the moment when there will be the fullest appraisal of implementation options for the policy. Options are very quickly narrowed down, so it is important that the key privacy questions form part of this early, wide-ranging appraisal. A full privacy impact assessment (PIA) is a comprehensive assessment that could require substantial resources; it is therefore recommended only for larger projects, with more significant implications for privacy. A process which is less resource-intensive than a full PIA, but based on considering the same key questions, should be used to identify the significant implications at the options appraisal stage. At subsequent stages of the project, the framework should be reused whenever one of the factors it considers has changed.

D.11. Public services should consider how use of the analytical framework can complement the PRINCE (Projects in Controlled Environments) project management methodology.

### *How should departments use the framework?*

D.12. The framework should be used to guide the work of the proposed Chief Knowledge Officers (CKOs). It indicates the questions that these CKOs should ask their department in relation to all policy initiatives with data-sharing intentions. A CKO should be able to draw on detailed guidance on how to quantify and assess the specific questions in detail, if a broad test against the framework suggests that the privacy implications are significant. Answers to these questions would indicate when a full privacy impact assessment is called for. The framework asks six basic questions:

- i. What is the policy objective?
- ii. What are the benefits of the proposed data-sharing?
- iii. What kind of data-sharing is proposed and what are the alternatives?
- iv. What are the costs and risks of data-sharing?
- v. How large are the benefits in relation to the risks?
- vi. What is being done to maximise the benefits and minimise the costs and risks?

### *What is the policy objective?*

D.13. Specifying the overarching goal to which it is proposed data-sharing will contribute is the first step in clarifying the organisation's thinking, and should be borne in mind throughout the stages that follow. It



is also a first step in challenging any prejudices or presumptions about the data-sharing solution. Early clarity about the policy objective will prompt early consideration of alternative solutions.

### ***What are the benefits of the proposed data-sharing?***

D.14. It is a generally accepted truism that more knowledge is a good thing. It is often assumed that data-sharing is synonymous with more knowledge and therefore needs little justification. This is unhelpful for our purposes, since it takes us no further in specifying and ultimately balancing the benefit against the costs. This report specifies three distinct areas of benefit: better services to citizens; better targeted services; and better value for money.

D.15. Being able to define these three distinct types of benefit not only enables us to move onto another level of specificity and take another step towards quantification, but it clarifies that some types of benefit will be felt directly by citizens as individuals, others will be felt indirectly by them as taxpayers or as the beneficiaries of public services. This is important because where benefits fall affects how risks are perceived.

### ***What kind of data-sharing is proposed and what are the alternatives?***

D.16. Data-sharing is increasingly a shorthand for 'more intelligent use of data', encouraged by the ambition of joined-up government and by cross-boundary working. It is, however, an unhelpful portmanteau term which needs to be unpacked for analysis. Firstly, there are different kinds of data-sharing. Of the pure data-sharing *between* organisations there are two kinds: case-by-

case sharing and batch database matching; these have quite different cost, privacy and procedural implications and this needs to be made clear and understood. Secondly, data-sharing may involve anonymised data or be compulsory or voluntary. There are other approaches to more and better use of data that are not exactly data-sharing, but they are alternative ways of combining and improving data use that should be considered, again because they have different costs, benefits and legal implications.

D.17. An important alternative is the better use of a public body's own data through sharing *within* the organisation but across sections or units. It is clear that many public bodies are not aware of the extent of the data held within their own borders, nor have they given proper consideration to the opportunities of rationalising and combining the databases they already have. While consent and compliance with the Data Protection Act remain an issue, statutory facility to share and combine data may already exist; and there may be added administrative efficiencies in taking this approach. There are also likely to be added costs, and data-sharing with another body may be a rational alternative to the internal organisational changes that are entailed. For rational decision-making, this needs to be made explicit.

D.18. Other alternatives to organisational data-sharing are: collection of new data; use of publicly available data such as the electoral register,<sup>96</sup> lists of postal codes or the land ownership registers; and use of private sector data such as might be purchasable or accessible from credit reference agencies and direct marketing companies. The costs, benefits and privacy risks of each of these options need to be compared.

<sup>96</sup> Use of the electoral register is now regulated under the Representation of the People Act 2000.



### What are the costs and risks of data-sharing?

D.19. This is an important area for information managers to focus on. The technical, organisational and legal costs of more information use are relatively new and unfamiliar territory for public bodies. Even the private sector still has a long way to go in defining and quantifying them. Assistance in defining and measuring costs and risks will be an important contribution to identifying the most effective policies. We have broken down the costs specific to data-sharing as:

- **Legal costs:** any new use of personal data must comply with the Data Protection Act, but there may be combinations of alternative data sets which already have consents that do not have to be repeated. The first data protection principle requires that any processing of personal information must be legal and public bodies must have the power to share information. The costs – mainly in the seeking of legal advice and awaiting a legislative slot – of gaining statutory permission for new data-sharing powers should be weighed up against alternative approaches to acquiring the same information from other sources.
- **Sharing costs:** again, as a new activity for many organisations, the costs of sharing data may not be obvious, nor direct. But they can be substantial, and so need to be signalled and efforts made to quantify them at an early stage. The sharing costs we have identified so far include the necessary minimum standardisations to permit effective sharing, measures necessary to counteract any expected deterioration in data quality as a result of the sharing, possible changes in voluntary compliance levels by the public as a result of awareness of more data-sharing by public services,

and any sharing by one public body of the uncompensated costs of another.

- **Safeguard costs:** in the rest of the report we argue that public concerns about increased data-sharing by public bodies are likely to require data-sharing to be accompanied by special privacy safeguards. These may be either technical – privacy enhancing technologies – or staff-based. These staff costs may be new general staff training or specific arrangements to limit staff access that may be necessary to ensure safe handling.

D.20. Risk and perception of, and response to, risk are of increasing interest to policy makers. How to assess risk, how to incorporate it into project and policy appraisal, how to weight and factor in public perceptions of risk are still inexact sciences. The project's public attitudes research<sup>97</sup> confirms existing research on privacy attitudes that risk is an important determinant of public perceptions. The public tends to be sceptical that it will see the theoretical benefits, either because it has understood the well-publicised difficulties around large public sector IT projects or because it believes benefits to be extracted elsewhere in the system.

D.21. The public may also have a different understanding of the risks around such privacy-related issues as security and confidentiality from that of public services themselves. It is important for organisations, when proposing to increase data-sharing, to check whether their perceptions of risk are in line with the public's and to understand the implications of these differences. They could be significant – for instance, a slower take-up of on-line services or a decline in voluntary compliance. Many recommendations in this report aim at a public sector-wide response to this issue of the public perception of

<sup>97</sup> *Strategies for Reassurance*, Perri 6, March 2002. See also *The future of privacy*, Perri 6, Demos, 1998.



privacy risk and how to improve communication about privacy and risk. However, public services should also consider how best to manage any perception differences for their specific projects.

### *How large are the benefits in relation to the costs and risks? The balance*

D.22. It may seem simplistic to ask that benefits be balanced against costs and risks. It is difficult to quantify each of these three aspects separately, and it is even harder to compare them against each other. Nevertheless, this aspect of the framework is intended both to emphasise this process and to support public services in undertaking it. It breaks the process down into a number of more manageable considerations:

- How large are the barriers to data-sharing?
- What are the attitudes of consumers and citizens? What do they want from the proposed development, and do they think they will benefit?
- What can be learnt from similar projects which may already have been undertaken, whether in the public or private sector?
- What are the consequences of failing to communicate the risks properly?
- What are the consequences of unauthorised access, poor data quality, etc?
- How vulnerable is the IT to technical failure, security breaches, etc? Is the IT unproven or has it been tried and tested?

### *What is being done to maximise the benefits and minimise the costs and risks?*

D.23. If it has been concluded that the balance between costs and benefits is in

favour of going ahead with the proposal, there remains one more step in the analytical framework: when the proposal is implemented, efforts to minimise the risks and costs and maximise the benefits should continue. The previous stages of the framework will have been conducted on paper – a desk-based analysis. This stage makes privacy promotion real. The detailed design of the processes and systems to support the proposal must deliver the organisation's privacy commitments as well as achieving service-related objectives. By asking this final question, the framework requires specific answers about safeguards to be put in place to protect privacy, such as privacy enhancing technologies and more generally designing privacy in from the start; and about actions to build confidence in data-sharing arrangements – such as data quality assurance mechanisms, redress systems, information and public awareness campaigns and external scrutiny.

### *The role of a privacy impact assessment (PIA) in the analytical framework*

D.24. The analytical framework considers the balance between the benefits arising from greater use of data, the costs of the proposal and the risks, including privacy risks. There are well-established methodologies for assessing financial impacts and technical risks, which can be used to feed information into the relevant sections of the analytical framework. Until recently, there have been no equivalent methods to assess privacy impacts and risks. This report demonstrates how complex and broad-ranging those privacy issues and risks can be, and how important an equivalent methodology will be in giving privacy issues a fair weight in the balancing process. PIAs have been developed elsewhere to fill this gap.



### Privacy impact assessments (PIAs)<sup>98</sup>

D.25. An increasing number of countries are using PIAs as a tool to consider the privacy implications of major projects. Impact assessments are already being used in a number of other areas in the UK public sector, and a full PIA may be resource-intensive – in the longer term, the Lord Chancellor’s Department should consider the feasibility of combining the core elements of the PIA into an amalgamated, rationalised Single Impact Assessment. In the meantime, the key is for those using PIAs to find them useful, rather than an imposition.

### Why should a PIA be undertaken?

D.26. While it will be for organisations to decide when a PIA is called for, some triggers can be suggested. The PIA should primarily answer two headline questions:

- Does the project face an insuperable regulatory problem? For instance, is it incompatible with the requirements of the Human Rights Act (HRA)?
- Is it necessary to deploy a privacy enhancing technology or incorporate any other particular kind of privacy safeguard?

D.27. A PIA takes CKOs step by step through the detailed second-order questions needed to answer these headline questions. Like the analytical framework, it breaks down a complex question into manageable, answerable and, wherever possible, quantifiable components. Unlike the framework, it aims only to identify privacy impacts; but it does not attempt to balance these with other impacts.

### An outline PIA

1. Introduction
2. Description of the project/proposal
3. Risk management issues
4. Legal/statutory authorities for the collection, use and disclosure of personal data
5. Privacy standards and concerns
6. Information collected (from existing databases)
7. Consent issues
8. Access rights for individuals to their own personal data, i.e. ‘subject access rights’
9. Users of personal information
10. Security safeguards
11. Methods to restore level of privacy
12. Conclusions about the privacy impact
13. Sources of information for this PIA

<sup>98</sup> Sources in this section:

– *Privacy Impact Assessments for Justice Information Systems*, US Department of Justice Working Paper, August 2000 – also available at [www.ojp.usdoj.gov/integratedjustice/piajis.htm](http://www.ojp.usdoj.gov/integratedjustice/piajis.htm)  
– [www.privacy.org.nz/media/pia.html](http://www.privacy.org.nz/media/pia.html) for a lecture on PIAs  
– Privacy Impact Assessments – Stewart, Blair in *Privacy Law and Policy Reporter*, volume 3, number 61, 1996. Available at [www.austlii.edu.au/au/other/plpr/vol3/vol3No04/v03n04a.html](http://www.austlii.edu.au/au/other/plpr/vol3/vol3No04/v03n04a.html)  
– [www.oipcbc.org/publications/pia](http://www.oipcbc.org/publications/pia) for an example model PIA from British Columbia;  
– [www.gov.on.ca/MBS/english/fip/pia](http://www.gov.on.ca/MBS/english/fip/pia) for Ontario’s guidelines; and  
– [www.anu.edu.au/people/Roger.Clarke/DV/PIA.html](http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html)



### *When should a PIA be done? – triggers*

D.28. The triggers that lead to the decision to undertake a PIA should be more specific than those for the analytical framework. They should include consideration of the risks arising from technology,<sup>99</sup> or the scale or purpose of a system, or the particular data being collected and its relationship with existing data sets. Wider factors, such as changing public attitudes towards a particular organisation or an area of public sector work, may also be relevant.

### *Further development of the framework and PIA*

D.29. The outline of the checklists, framework, triggers and PIAs suggested here provides a structure on which CKOs can build. Experience of using these tools should lead to improvements. If the processes prove too burdensome, or inappropriate in some cases, they should be modified and developed.

#### *The analytical framework and PIAs: when to use them*

- All officials (not just information management specialists) to have the **data use questions** in mind at all times.
- Use these questions when considering policy options, re-engineering projects, IT changes.
- If the checklist suggests it is appropriate, use the **analytical framework**.
- If the project or proposal changes, use the framework again.
- Whenever the framework is used, check if the proposal has significant privacy implications by considering the **triggers**.
- If the triggers suggest it is appropriate, undertake a full **PIA**.

<sup>99</sup> From 'Privacy Impact Assessments' by Blair Stewart, cited earlier.

## ANNEX E: THE ROLE OF THE PIU

E.01 The Prime Minister announced the creation of the Performance and Innovation Unit (PIU) on 28 July 1998. The PIU's aim is to improve the capacity of government to address strategic, cross-cutting issues and promote innovation in the development of policy and in the delivery of the government's objectives. The PIU is part of the drive for better, more joined-up government. It acts as a resource for the whole of government, tackling issues that cross public sector institutional boundaries on a project basis.

E.02 The Unit's Director is Geoff Mulgan, and it reports direct to the Prime Minister through Sir Richard Wilson. A small central team helps recommend project subjects and manages the Unit's work. Work on projects is carried out by small teams assembled both from inside and outside government. About half of the current project team staff are drawn from outside Whitehall, including from private sector consultancies, think tanks, NGOs, academia and local government.

E.03 Comprehensive information about other PIU projects can be found on the PIU's website at [www.piu.gov.uk/](http://www.piu.gov.uk/)

## ANNEX F: THE ADVISORY GROUP AND ORGANISATIONS CONSULTED

F.01 This report was prepared by a multi-disciplinary team guided by a Ministerial Sponsor and an Advisory Group with government and non-government representation.

### *The team*

F.02 The team comprised:

- Jeremy Booker – on secondment from the European Bank of Regeneration and Development;
- Phil Boyd – on secondment from the Information Commissioner’s Office;
- Michael Jampel – on secondment from the Department of Trade and Industry;
- Rob Lloyd Jones – permanent member of the PIU;
- Yvette Meftah – team leader, permanent member of the PIU; and
- Rachel Phillipson – government economist, PIU.

F.03 The team was assisted by Peter Dare of IBM, who contributed valuable technical expertise, and Perri 6 of Strathclyde University, who led focus group research on behalf of the team. The team was also assisted by Tasnim Zavery – PIU, Atit Patel – PIU, Stephen Hale – PIU, Roopak Radia – PIU and Bernadette Makena-Wanjiku – PIU.

### *Sponsor Minister*

F.04 The work of all PIU teams is overseen by a Sponsor Minister, in this case Lord

Falconer of Thoroton QC, Minister of State at the Cabinet Office, now Minister for Housing, Planning and Regeneration in the Department for Transport, Local Government and the Regions.

### *Advisory Group*

F.05 In addition, the team was greatly assisted by being able to draw on the experience and advice of its Advisory Group, benefiting from an extensive process of consultation and review throughout the project. The Group, chaired by Lord Falconer, comprised:

- Anna Bradley – National Consumer Council;
- Jonathan Duke-Evans – Home Office;
- Elizabeth France – Data Protection Commissioner (now Information Commissioner);
- William Jordan – Economic and Domestic Affairs Secretariat, Cabinet Office;
- Ian McCartney MP – e-Government Minister, Cabinet Office (now Minister of State, Department for Work and Pensions);
- Jude McLaggan – Inland Revenue;
- Simon Norbury – Department for Transport, Local Government and the Regions (formerly with Newham LBC and now with Westminster LBC);
- John Pullinger – Office for National Statistics;
- James Purnell – No. 10 Policy Unit;



- Professor Charles Raab – Edinburgh University;
- Jamie Rentoul – PIU;
- Ian Roberts – Experian;
- Ann Steward – Office of the e-Envoy, Cabinet Office; and
- John Wadham – Liberty.

F.06 The team gratefully acknowledges the advice and time given by each Advisory Group member.

### *Organisations consulted*

F.07 The project team also consulted a range of organisations, and acknowledges the contributions of all who offered advice, participated in meetings or working groups, or assisted in any other way:

Audit Commission  
Business change  
Business Development and Strategy  
Cabinet Office, Better Regulation Task Force  
Cabinet Office, Centre for Management and Policy Studies  
Cabinet Office, Civil Service Corporate Management  
Cabinet Office, Modernising Public Services Group  
Cabinet Office, Office of the e-Envoy  
Cabinet Office, Regulatory Impact Unit  
Cabinet Office, Social Exclusion Unit  
Cabinet Office, UK Anti Drugs Co-ordination Unit  
Cambridge Health Informatics Ltd  
Castle Vale Housing Action Trust (HAT)  
Child Support Agency  
Civil Aviation Authority  
Consult Hyperion

Credit Industry Fraud Avoidance System  
Criminal Records Bureau  
Data Protection Authority, Netherlands  
Department for Culture, Media and Sport  
Department for Education and Skills  
Department for Environment, Food and Rural Affairs  
Department for Transport, Local Government and the Regions  
Department of Health  
Department of Trade and Industry  
Department for Work and Pensions  
Driver and Vehicle Licensing Agency  
Edentity  
Employment Service  
Experian  
Financial Services Authority  
FirstDirect  
Food Standards Agency  
Foreign and Commonwealth Office  
Foundation for Information Policy Research  
Groundwork (North Kent)  
Health and Safety Executive  
Hill & Knowlton  
HM Customs & Excise  
HM Stationery Office  
HM Treasury  
HM Treasury, Competition and Regulation Policy  
HM Treasury, Electronic Payment Systems  
HM Treasury, Enterprise and Growth Team  
HM Treasury, New Working Age Agency  
HM Treasury, Police and Criminal Justice Bill Team



Home Office  
Human Genetics Commission  
IBM  
IDeA  
Information Commission  
Inland Revenue  
Liberty  
Local Government Association  
London Borough of Newham Council  
London School of Economics  
Lord Chancellor's Department  
Matrix Chambers  
Medical Ethics Unit  
Meerkanten Psychiatric Hospital,  
Holland  
Metropolitan Police  
Microsoft Research Ltd  
Ministry of Defence  
National Association of Citizens  
Advice Bureaux  
National Audit Office  
National Consumer Council  
National Criminal Intelligence Service  
National Health Service Executive  
Office for National Statistics  
Office for National Statistics, General  
Register Office  
Office for National Statistics, Comprehensive  
Business Directory study project  
Office of Science and Technology  
Organisation Consulting Partners  
Philippsohn Crawfords Berwald Solicitors  
Privacy International  
Public Record Office  
Public Trust Office  
Registry Trust  
Scottish Executive, Development  
Department

Scottish Executive, Education, IAG and  
Modernising Government initiatives  
Scottish Executive, Executive Secretariat  
Scottish Executive, Health Department  
Scottish Executive, Justice Department  
Small Business Service  
Surrey Community Safety Unit  
Treasury Solicitors  
UK Passport Agency  
University College London  
University of Edinburgh  
University of Strathclyde  
Valuation Office Agency  
Youth Justice Board

## ANNEX G: SELECTED BIBLIOGRAPHY

**Accenture** – *eGovernment Leadership: Rhetoric vs Reality – Closing the Gap*, April 2001

**Brands, Stefan A.** – *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*, MIT Press, London, 2000

**BRMB International** – *Staff Attitudes to Security in the Benefits Agency*, 1999

**Cabinet Office** – *E-Government Metadata Framework, Issue: 1.0 For open consultation*, January 2001

**Cabinet Office** – *Electronic Government: the view from the queue*, October 1998

**Cabinet Office** – *Review of the Public Sector Ombudsmen in England*, April 2000

**Cabinet Office, Office of the e-Envoy** – *Electronic Service Delivery – Autumn 2001 Report*, December 2001

**Cabinet Office, Office of the e-Envoy** – *UK online Annual Report 2001*, November 2001

**Cyber Dialogue** – *Privacy v Personalisation*, 2000

**Data Protection Commission** – *First Report of the Data Protection Commissioner*, June 2000

**Data Protection Registrar** – *Private lives and public powers: A guide to the law on the use and disclosure of information about living individuals by public bodies*

**Department for Education and Skills** – *The Connexions Service: Prospectus and Specification*, 2000

**Department for Work and Pensions** – *Protection of Customer Information Guide*, April 2000

**Department for Work and Pensions** – *Safeguarding Social Security: Getting the Information we Need*, July 2000

**Department for Work and Pensions** – *Social Security Fraud Act 2001: Code of Practice on Obtaining Information*, July 2001

**Department of Health** – *Outline Internal Business Strategy: Painting the Big Picture*, October 2000

**Department of Health** – *Reforming the Mental Health Act*, December 2000

**Foresight Panel** – *Just Around the Corner*, March 2000

**Hedges, Alan** – *Confidentiality: The Public View*, Department for Work and Pensions Research Report No. 56, 1996

**Home Affairs** – *Select Committee Report on Border Controls*, Parliament, January 2001

**Home Office** – *Casework Information Needs Within the Criminal Justice System*. See [www.homeoffice.gov.uk/hmiprob/infoneeds.htm](http://www.homeoffice.gov.uk/hmiprob/infoneeds.htm)

**Home Office** – *Criminal Justice: The Way Ahead*, February 2001



**Home Office** – *Medium Term Strategic Plan for Information Systems in the Criminal Justice System*, October 1999

**Home Office** – *Review of Crime Statistics: A Discussion Document*, July 2000

**IBM** – *Multinational Consumer Privacy Survey*, October 1999

**Information Commissioner** – *Annual Report and Accounts for the Year Ending 31 March 2001*, HMSO, June 2001

**Jupiter Communications** – *European Online Privacy*, 1999

**Lord Grabiner QC** – *The Informal Economy*, HM Treasury, April 2000

**MORI** – *Attitudes towards data-sharing: A survey among civil servants*, survey conducted on behalf of the PIU, November 2000 to January 2001

**NAO** – *Government on the Web*, 2000

**NAO** – *Measuring the Performance of Government Departments*, March 2001

**National Consumer Council** – *Consumer Privacy in the Information Age*, December 1999

**National Consumer Council** – *Protecting Personal Privacy: Guidelines for collecting and using people's personal data*, June 2001

**National Criminal Intelligence Service** – *The National Intelligence Model*, 2000

**NHS** – *Building the Information Core: Implementing the NHS Plan*, January 2001

**NHS** – *Information for Health: An Information Strategy for the Modern NHS 1998–2005*, September 1998. See also [www.doh.gov.uk/ipu/strategy/update/index.htm](http://www.doh.gov.uk/ipu/strategy/update/index.htm)

**Ofcom** – *Effective competition review: dial-up Internet access*, 29 January 2002

**ONS** – *Attitudes towards confidentiality and survey research: some results from qualitative research*, unpublished paper, November 2000

**ONS** – *Business information in government – legal and privacy research*, autumn 2001

**ONS** – *Census Metadata Strategy*, Advisory Group Paper 2000

**ONS** – *Internet Access*, 18 December 2001

**ONS** – *Methods for Automatic Record Matching and Linkage and their Use in National Statistics*, National Statistics Methodological Series No. 25, July 2001

**People's Panel First Wave Research**; see [www.servicefirst.gov.uk/index/pphome.htm](http://www.servicefirst.gov.uk/index/pphome.htm)

**Perri 6** – *The future of privacy*, Demos, 1998

**Perri 6** – *Strategies for Reassurance: Lessons from Focus-Group Research on Allaying Public Concerns about Privacy and Data-Sharing in Government*, 2002

**Radburn, Stephen** – *Data Exchange and Crime Mapping: A Guide for Crime and Disorder Partnerships*, Home Office

**RSGB & Taylor Nelson Sofres** – *Data Protection Tracking Research 2000*, for Information Commissioner, July 2000

**Social Exclusion Unit** – *National Strategy for Neighbourhood Renewal – Report of Policy Action Team 18: Better information*, April 2000

**Stewart, Blair** – 'Privacy Impact Assessments' in *Privacy Law and Policy Reporter*, volume 3, number 61, 1996



**Swedish Association of Local Authorities  
and Swedish Federation of County  
Councils and Regions** – *E-Democracy in  
Practice: Swedish Experiences of a New Political  
Tool*, 2001 (see also  
[www.svekom.se/skvad/indexeng.htm](http://www.svekom.se/skvad/indexeng.htm))

**Turnbull & King** – *Review of ONS*

**University of Cambridge, Judge Institute of  
Management Studies** – *Deployment of  
NHSNet in Acute and Community Trusts*, April  
2000

**US Department of Justice** – *Privacy Impact  
Assessments for Justice Information Systems*,  
Working Paper, August 2000

**US Government Accounting Office** –  
*Identity Fraud: Information on Prevalence, Cost  
and Internet Impact is Limited*, May 1998,  
GAO/GCD – 98 – 100BR, cited in *Identity  
Theft: Authentication as a Solution*, National  
Fraud Centre, March 2000;  
available from [www.nationalfraud.com](http://www.nationalfraud.com)

**Which?** – *Are you being served: The growth of  
an e-nation*, 1999