scripted

Volume 10, Issue 1, April 2013

ENHANCING DATA PROTECTION AND DATA PROCESSING IN THE PUBLIC SECTOR: THE CRITICAL ROLE OF PROPORTIONALITY AND THE PUBLIC INTEREST

Dr Gillian Black and Leslie Stevens [*]

Abstract

Data protection in the public sector has suffered from a number of high profile breaches over the last decade, revealing a culture of weak compliance, especially in comparison with that in the private sector. This article examines certain factors which make public sector data processing distinct, and how the lack of clarity regarding the routes to legitimate processing may be exacerbating these problems. By closely examining the jurisprudence regarding Schedule 2 of the Data Protection Act 1998, which provides the legitimate bases for data processing, we reveal the current problems public sector data controllers face in determining whether their processing is "necessary" and therefore legitimate. We determine that the test of necessity is reliant on proportionality, requiring the interest in processing the personal data to be balanced against the data subjects' data protection and privacy interests. This in turn requires a detailed consideration of the public interests at stake, in providing the public services and respecting the personal data involved. We conclude by providing a structured and coherent three-step test for data controllers to apply in reaching their decision. This test focuses on the critical issues in balancing the competing interests, enabling data controllers to take a principle-based decision as to whether or not their processing is indeed in the public interest, proportionate and necessary – and therefore ultimately legitimate. This three-step test offers greater clarity for data controllers, which in turn should enhance the rigour of their data processing, thereby strengthening the data protection culture and benefiting data controllers, data subjects, and the public at large.

---

[*] Dr Gillian Black is a Senior Lecturer at Edinburgh Law School, University of Edinburgh, and Leslie Stevens is a California-licensed attorney and PhD student at Edinburgh Law School, University of Edinburgh. The authors would like to thank Professor Graeme Laurie, University of Edinburgh, and two anonymous reviewers, for very helpful comments on an earlier version of this article.

DOI: 10.2966/scrip.100113.93

1. Introduction

This article will examine the serious difficulties facing public sector organisations in the United Kingdom (UK) when determining whether there is a legitimate basis for their processing of personal data. Concepts such as the tests of "necessity" and "proportionality" will be examined, in order to expose the fundamental weaknesses in the jurisprudence of this area. These weaknesses will in turn allow us to suggest what changes are needed to secure the legitimate processing of personal data by the public sector – for the consequent benefit of the organisations, the individuals, and of society as a whole.

Such a review is essential. Ensuring that the processing of personal data is legitimate can be a challenge for any organisation, and the consequences of getting it wrong can adversely affect all parties involved. For the data controller, processing personal data without a legitimate basis can incur consequences ranging from damaging publicity[1] to monetary penalties.[2] Additionally, illegitimate data processing can result in potentially intangible damage, such as a chilling effect on processing more generally. For individuals, unauthorised processing of their personal data is an infringement of their fundamental right to data protection, guaranteed by article 8 of the European Charter of Fundamental Rights. It may lead to the wrongful denial of services, or other harmful social consequences,[3] and could ultimately be a breach of their right to private life under Article 8 of the European Convention on Human Rights (ECHR).

Thus, while data processing and data sharing are inevitable functions in today's society, it is essential that the body carrying out the processing complies with the law. In the UK, this requires compliance with the eight data protection principles set out in Schedule 1 of the Data Protection Act 1998 (DPA) including, critically, that the processing is lawful[4] and has a legitimate basis. The legitimate bases for processing

---

[1] The highest profile case to date in the UK remains the (alleged) loss of 25 million child benefit records by HMRC in 2007, resulting in the Poynter Report of 2008 (The *Review of Information Security at HM Revenue and Customs*). The Information Commissioner served an enforcement notice on HMRC requiring it to comply with the recommendations in that report: Enforcement Notice of 14 July 2008 (available at www.ico.gov.uk). Other examples abound in the media and on the Information Commissioner's Office website: www.ico.gov.uk.

[2] Since April 2010, the Information Commissioner has been able to impose monetary penalties of up to £500,000 for breaches of the data protection principles, under s 55A of the Data Protection Act 1998 (inserted by the Criminal Justice and Immigration Act 2008 (c 4), s 144(1)). See further G Black, *Data Protection Reissue*, in The Laws of Scotland Stair Memorial Encyclopedia (2010) (hereafter "Black, *Data Protection*, SME"), at para 338 *et seq*.

[3] The recent unfounded allegations of child abuse made against Lord McAlpine being one example: see BBC Online coverage in November 2012, including http://www.bbc.co.uk/news/uk-20348978 (accessed 25 March 13) .

[4] Lawfulness under the first data protection principle extends to compliance with all relevant laws, not just data protection laws: see Black, *Data Protection*, SME, at para 103 and *Murray v Express Newspapers and Big Pictures* [2007] EWHC 1908 (Ch) at 72.

are set out in Schedule 2 (for personal data) and Schedule 3 (for sensitive personal data).[5]

In addressing these issues, we will focus on the particular challenges faced by public sector organisations. Given this emphasis, the first section sets out the specific challenges they face and why they merit separate treatment from private sector data controllers. This is put sharply into focus with the recent disclosure that the UK Government processes over one billion transactions every year in its provision of public services, and each transaction involves personal or sensitive personal data.[6] We will outline briefly the current grounds which legitimise the processing of personal data, as set out in Schedule 2 of the DPA.

Having identified the grounds of legitimate processing, we will explore the problems of determining when processing will be "necessary" in terms of the Act, which also introduces the test of proportionality. In particular, the problem of establishing when processing is in the public interest will be reviewed, with reference to the conflicting interpretations of "public interest": Does data protection always place an individualist right to privacy in competition with a communitarian interest in permitting processing? By advocating a broader understanding of the value of data protection, we propose how public services can serve the public interest without jeopardising informational privacy rights.

The article concludes with some key recommendations for future reform and guidance, to ensure that public sector processing is not unnecessarily stifled – but that the rights and interests of individuals cannot be overruled by unsubstantiated and politicised claims of processing in the public interest. To achieve this, we advocate the adoption of a three-step test which takes data controllers through the key issues in turn: the legitimate basis for which processing is required; the identification of the personal data required; and the basis on which to balance these two elements, with reference to the public interest. In doing so, a more nuanced and appropriate understanding of the test of necessity under Schedule 2 will emerge: something which has otherwise remained elusive. The end result is to provide a more coherent approach to striking the correct balance between processing and protection, especially in the public sector.

2. Data Processing and the Public Sector: Schedule 2 Conditions

---

[5] This article will focus primarily on Schedule 2, as the primary gateway to processing personal data.

[6] Charlotte Jee, "Government announces cost per transaction for major services - Government Computing Network", 17 January 2013: http://central-government.governmentcomputing.com/news/government-announces-cost-per-transaction-for-major-services (accessed 25 March 13). Such "transactions" include the Government's processing of HMRC inquiries, Stamp Duty, Child Benefit Claims, Visa Applications, Vehicle Excise Duties, Job Seekers Allowance, and Statutory Off Road Notifications. All of these transactions would involve the processing of personal and/or sensitive personal data and thus would need to be justified under a Schedule 2 (and possibly also a Schedule 3) condition to processing.

All data processing requires the data controller to balance the need for that processing against the individuals' rights not to have their personal data processed excessively or unnecessarily. In order to demonstrate that the processing is indeed legitimate, the data controller must be able to point to a fulfilled condition in Schedule 2. In brief (and in slightly abridged form) the Schedule 2 conditions[7] are as follows:

1. The data subject has given his consent to the processing;

2. The processing is necessary for the performance of a contract to which the data subject is a party, or as a preliminary to entering into such a contract;

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract;

4. The processing is necessary in order to protect the vital interests of the data subject;

5. The processing is necessary:—

   (a) for the administration of justice;

   (aa) for the exercise of any functions of either House of Parliament;

   (b) for the exercise of any functions conferred on any person by or under any enactment;

   (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department; or

   (d) for the exercise of any other functions of a public nature exercised in the public interest by any person;

6. The processing is necessary for the purposes of legitimate interests pursued by the data controller, unless unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the data subject (and the Secretary of State may specify particular circumstances in which this condition is, or is not, to be taken to be satisfied).

As can be seen, these conditions require either consent (condition 1) or, in all other cases, that the processing is *necessary*. While the individual conditions are not segregated according to whether the data controller is a public or private sector organisation, the differing nature of processing carried out in the two sectors means that some conditions will be more relevant to one sector than the other.

Private sector processing is typically carried out for a commercial aim, and is much more likely to be conducted at the behest of the data subject. Accordingly, the consent of the data subject is far more likely to justify the processing of private

[7] These conditions implement Art 7 of the Data Protection Directive 95/46/EC.

companies. Consent itself is a thorny issue,[8] yet nonetheless, there is extensive guidance about when consent will be free and informed.[9] For both private and public sector organisations, one of the most fundamental risks in relying upon consent is that it can be subsequently withdrawn by the data subject, thereby depriving the processing of its lawful basis. Thus, one of the other conditions in Schedule 2 will often provide a more robust basis for processing. Moreover, there are particular concerns with consent in the public sector. The Ministry of Justice has stated that, "In certain circumstances (such as data sharing in the context of regulatory or enforcement functions) it is unlikely that consent would be an appropriate condition and public bodies will wish to rely on other conditions".[10] The reason for this reluctance arises from the nature of the relationship between the data controller and the data subject in the public sector, where the data subject is likely to be dependent on the data controller for the provision of public services, whether health case, finance or housing, for example. As recital 34 of the draft Data Protection Regulation states:

> Consent should *not* provide a valid legal ground for the processing of personal data, *where there is a clear imbalance between the data subject and the controller*. This is especially the case where the data subject is in a situation of dependence from the controller…Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.[11][Emphasis added]

Critically, the constantly evolving nature of public services requires more than an initial acceptance via consent to foster a relationship of trust between the public and the public sector provider. If the relationship between the government and its citizens is viewed as a "continuing relational process" then justifying the use of citizens' personal data should rely upon justifications in the public interest which demonstrate

---

[8] Professor Graeme Laurie refers to "the fetishisation of consent" in respect of the "attitude prevalent among many regulators, including ethics committees, whereby the obtaining of consent has come to be seen as both necessary and sufficient to legitimate data handling and sharing when it is neither; nor, is it achievable or even desirable in some cases" in G Laurie, "SCRIPT Opinion 1:2008 Data Sharing Response to Ministry of Justice Consultation" (2008) available at http://www.law.ed.ac.uk/ahrc/Opinion_Data_Sharing_Feb_2008.pdf (accessed 25 March 13) and G Laurie and E Postan, "Rhetoric or Reality: What is the legal status of the consent form in health-related research?" (2012) 1 *Medical Law Review*. See also Ministry of Justice, "Data Sharing Protocol: Annex H, Public Sector Data Sharing: Guidance on the Law" (2012) 14, available at http://www.justice.gov.uk/information-access-rights/data-protection/data-sharing (accessed 25 March 13) (henceforth "Ministry of Justice, *Data Sharing Protocol Annex H* (2012)").

[9] For a review of this, see for example Black, *Data Protection*, SME, paras 108-118; R Jay, *Data Protection Law and Practice*, 4th ed (2012) (henceforth Jay, *Data Protection Law*), at paras 4-35 – 4-46 and paras 5-08 – 5-10 re Schedule 2 consent.

[10] Ministry of Justice, *Data Sharing Protocol Annex H* (2012) at p14, para 11.

[11] Draft Data Protection Regulation, 25 January 2012, recital 34.

a continuing obligation to process their personal data only as such processing relates to the public interest of society as a whole.[12]

For these reasons, public sector processing is likely to be justified by, and find a stronger legal basis in, one of the other conditions in Schedule 2, reflecting the broader social purposes for which it is carried out. Public sector processing will usually be provided in furtherance of legitimate objectives in the public interest, such as the provision of health care, welfare benefits, housing services, or national security and surveillance. Indeed, condition 5 is specifically addressed to the Government and local authorities, enabling them to carry out their functions. In meeting any of the non-consent conditions, data controllers must show that their processing fulfils the function specified *and* is also "necessary". The concept of "necessary" therefore plays a fundamental role in determining when data processing will be legitimate.

A further consideration for public sector organisations is that, in addition to meeting the requirements of the DPA, they are also obliged to take into account a multitude of competing factors arising from their position in the public sector. Whilst the private sector is subject to the same regulatory framework re data protection, it nevertheless "…works under different transparency frameworks to those that are operating in the public sector."[13] This includes answering to the public tribunal, not to mention Parliament and other Government Departments, as well to the ever-present budgetary pressure faced by all public bodies.

Moreover, public sector organisations are also likely to suffer different consequences to private sector controllers if they get it wrong. Whereas a private sector company may suffer adverse commercial consequences from unlawful processing such as damaging its reputation and business interests, unlawful processing in the public sector arguably harms not merely the organisation, but more widely society as a whole. At a very practical level, this harm can arise simply from the indirect cost to taxpayers from the fines incurred by public sector organisations for data breaches. Whereas such fines incurred by private organisations reduce their profit, public sector fines reduce the available funds for public use. In 2012, the Information Commissioner's Office (ICO) imposed monetary penalties on twenty different public sector bodies for data protection breaches, in marked contrast with the penalties levied against only three private companies. The total cost to the public sector of these monetary penalties was £2.56 million.[14] Clearly, such a financial burden is damaging

---

[12] See G Laurie and E Postan, "Rhetoric or Reality: What is the legal status of the consent form in health-related research?" (2012) 1 *Medical Law Review* 1at 42-43.

[13]Stewart Room, "Do fines work, or is there an alternative?" (27 October, 2012) available at http://www.stewartroom.com/?p=1519 (accessed 25 March 2013).

[14] ICO website: details of all fines imposed in 2012 are listed at the 'Monetary Penalty Notices' page available at *http://www.ico.gov.uk/enforcement/fines.aspx* (accessed 1 February 2013). The penalties of £2.56 million across 20 organisations equates to an average of £128,000 per body, while the three private sector organisations were fined a total of £640,000, or £213,000 on average. While this indicates that the penalties levied against private sector organisations are typically higher, the fact remains that public sector organisations incur far more of them.

to the wider public interest, quite irrespective of the harm caused by the individual data breaches.

In addition to the immediate harm arising from financial penalties, there can be less tangible consequences. Staff time dedicated to investigating the breach, dealing with any direct fallout, and ensuring more robust procedures are in place in future, results in a loss of efficiency, temporarily at least.[15] Significantly, public confidence in the Government and local authorities can be undermined by poor standards of data protection, leading to reduced public engagement in future. The Ministry of Justice has pointed to the importance of this public understanding and engagement:

> Research suggests that the public is willing to give out personal information to Government and allow it to be shared if there is a clear benefit to be gained by this information sharing. Improved services are seen as providing a clear benefit, but public concerns still remain about the way that information can and should be shared across Government, the wider public sector and with private organisations.[16]

This is a particular concern given that public bodies handle extensive, and often sensitive, personal data concerning large sectors of the population. It has already been noted that the Government processes over one billion transactions each year involving personal data.[17] As Baroness Nicolson noted in the House of Lords during discussion of the Data Protection Bill, the legislation should have particular importance in the UK where "the Secretary of State for Health owns the health records of all those who use the National Health Service, presumably 99% of the whole population". [18]

A weak data protection culture may also give rise to deterrent effect on the organisation or other public sector bodies. The withdrawal or reduction of services

---

[15] While the same could be true of private companies, any loss of efficiency on their part is damaging to their business interests, so is more likely to be absorbed, eg by recruiting temporary staff. This is far less likely to be an option for public sector organisations on fixed salary budgets etc.

[16] Ministry of Justice evidence to the House of Lords Select Committee on "Surveillance: Citizens and the State", (Report HL 18-I published 21 January 2009): Memorandum reported 25 June 2008, at para 23, footnote omitted.

[17] Charlotte Jee, "Government announces cost per transaction for major services - Government Computing Network", 17 January 2013:

http://central-government.governmentcomputing.com/news/government-announces-cost-per-transaction-for-major-services (accessed 25 March 13) . Such "transactions" include the Government's processing of HMRC inquiries, Stamp Duty, Child Benefit Claims, Visa Applications, Vehicle Excise Duties, Job Seekers Allowance, and Statutory Off Road Notifications. All of these transactions would involve the processing of personal and/or sensitive personal data and thus would need to be justified under a Schedule 2 (and possibly also a Schedule 3) condition to processing.

[18] Baroness Nicolson of Winterbourne, House of Lords, 2 February 1998. This demonstrates why lower levels of compliance within NHS in particular, is a strong cause for concern. HL Deb 02 February 1998 vol 305, col 451, available at

http://www.publications.parliament.uk/pa/ld199798/ldhansrd/vo980202/text/80202-06.htm (accessed 25 March 13).

provided may well appear to be a more preferable option for an organisation than the risk of breaching the DPA, with its attendant bad publicity, monetary fines, and public disengagement. In a more robust data protection culture, supported by clearer guidelines, these risks would potentially be managed successfully.

There is a further risk that a lack of definitive guidance re data protection compliance, especially for the public sector, results in a lack of joined-up thinking across different public sector organisations. With no uniform governance mechanisms or procedures in place, there is diverse practice throughout the UK, only adding to the confusion and lack of confidence in each individual organisation, and further promoting a culture of caution.[19]

All these factors illustrate why it is essential to have a rigorous data protection culture in the public sector, yet the available evidence suggests that public bodies are not complying satisfactorily with their DPA obligations. In addition to the number of monetary penalties imposed, a recent audit undertaken by the ICO has demonstrated that these bodies often have poor compliance records, especially when compared to private sector organisations. The ICO conducted data protection audits between February 2010 and July 2012, and investigated both private and public sector organisations for overall compliance with the DPA.[20] The audits assessed organisations according to an overall assurance rating,[21] which was derived from six possible areas, each individually reviewed. These results revealed a higher level of compliance by private sector organisations than their public sector counterparts –

---

[19] It is to tackle issues such as these that there have been significant efforts within the Scottish health research sector, through SHIP: the Scottish Health Informatics Programme. This is a Scotland-wide project to provide robust governance for data linkage, for research purposes, of Electronic Patient Records. The project has been advised in relation to data protection matters by Professor Graeme Laurie and Nayha Sethi of the University of Edinburgh. For further details, see: www.scot-ship.ac.uk/

[20] ICO Press Release, "Private sector leads the way on data protection compliance but 'room for improvement' elsewhere" (11 October 2012), available at *http://www.ico.gov.uk/news/latest_news/2012/private-sector-leads-the-way-on-data-protection-compliance-11102012.aspx* (accessed 25 March 13).

[21] The ICO marked the results of each audit according to an overall assurance rating, which was comprised of four possible ratings: (1) High assurance, indicating good data protection practice with room for little improvement; (2) Reasonable assurance, conveying good data protection practices with some room for improvement; (3) Limited assurance, conveying a moderate level need for improvement in data protection practice; and (4) Very limited assurance, conveying a high risk for non-compliance with the DPA and the need for immediate action. The Audits were conducted for four different sectors: Central Government; Local Authorities, NHS, and private sector:

ICO "Audit outcomes analysis: central government (February 2010 to July 2012)" (2012) 1,(henceforth ICO Audit Results: central government).

ICO "Audit outcomes analysis: Local authorities - February 2010 to July 2012" (2012) 1, (henceforth ICO Audit Results: Local Authorities).

ICO "Audit outcomes analysis: NHS (February 2010 to July 2012)" (2012) 1. (henceforth ICO Audit Results: NHS).

ICO "Audit outcomes analysis: private sector (February 2010 to July 2012)" (2012) 1. (henceforth ICO Audit Results: private sector) All available at *http://www.ico.gov.uk/news/latest_news/2012/private-sector-leads-the-way-on-data-protection-compliance-11102012.aspx*.

arguably reflecting the strong commercial and reputational drivers behind private sector compliance.[22] Moreover, these audit results are reflected in the high profile media stories concerning serious data protection breaches by public sector organisations, typically involving the loss of sensitive personal data through inappropriate data handling and retention practices.[23]

Security lapses, in breach of the seventh data protection principle, are of course distinct from failure to comply with Schedule 2 (or 3) conditions. They nevertheless point to a weak data protection culture, especially since taking practical steps to improve data security (such as encrypting laptops and securely shredding documents) is typically more straightforward than interpreting and applying the concept of "necessary" to processing under Schedule 2. Thus, security breaches can arguably be indicative of wider data protection failings within an organisation. Moreover, although difficult to establish, it could be suggested that a lack of clarity within the data protection regime is itself responsible for engendering a less robust culture, by undermining or trivialising the significance of protecting personal data.

Consequently, it is to the collective advantage of public sector organisations, their users, and the society they serve if processing is compliant with the DPA. This in turn requires that the route to legal compliance under the DPA is as clear and unambiguous as possible. Only then can we be sure that there are no unnecessary barriers to compliance with the Act.

Yet, while the ideal would be to have clarity and simplicity, a review of the Schedule 2 conditions reveals that there is considerable uncertainty surrounding the interpretation of fundamental concepts employed therein. This poses a significant challenge to the practical application of the conditions, in three different contexts. As already noted, other than consent, Schedule 2 turns on the basis that processing will only be legitimate where it is necessary. This leads to our first question: What does "necessary" entail?

3. When is data processing "necessary"?

---

[22] ICO, "Private sector leads the way on data protection compliance but 'room for improvement' elsewhere" (2012), available at *http://www.ico.gov.uk/news/latest_news/2012/private-sector-leads-the-way-on-data-protection-compliance-11102012.aspx* (accessed 25 March 13)

[23] Recent examples from 2012 include the ICO's fine of £120,000 in October 2012 to Greater Manchester Police for failing to take appropriate precautions to prevent the loss of personal data. This fine stems from the second reported loss of personal data due to the use of unencrypted memory sticks, with no passwords, which contained the sensitive personal data of individuals related to several police investigations. Despite this incidence having occurred previously in September 2010, Greater Manchester Police failed to take proper precautions by allowing police officers, until this incident, to use unencrypted memory sticks and download sensitive personal data onto them. On 11 September 2012 the Scottish Borders Council was fined £250,000 for failing to securely dispose of employee records which were discovered intact in a supermarket's recycle bin. The ICO reported that over 676 files were thrown haphazardly into this recycling bin and contained confidential information as to individuals' salaries and bank account details. The ICO has reported 18 public sector data breaches so far in 2012, but it is possible that this is only the tip of the iceberg. ICO "News releases – 2012" (2012), available at *http://www.ico.gov.uk/news/latest_news/2012.aspx* (accessed 25 March 13).

3.1 Assessing the UK approaches to "necessary"

The DPA has been in force for over a decade, and in that time there have been numerous attempts to provide clarity on the meaning of "necessary" as it applies under the Act. Among those who have provided guidance are the ICO, the Government, the Scottish Government, and of course the courts. While this produces a range of definitions and interpretations, the most serious issue is a continuing lack of definitive guidance – again leading to a lack of consistency between data controllers. This is especially problematic as the test has to be applied in the first instance by the organisation with a vested interest in processing. (It may of course be subsequently interpreted by a court, if the decision leads to litigation). There is therefore a likelihood that any uncertainty will be interpreted in favour of enabling data processing, and thus the outcome may be biased from the outset.

A further concern is that the lack of a single definition applied in the UK fails to take account of the European jurisprudence, which recognises that necessary is "a concept which has its own independent meaning in Community law and… must be interpreted in a manner which fully reflects the objective of that directive [ie 95/46/EC]".[24] This ensures that harmonisation is not minimal in this area, but is "generally complete".[25] The necessity test as interpreted by the European Court of Justice in *Huber* imported the concept of proportionality,[26] but while reference to European jurisprudence should be an important starting point, this does not always seem to be the case in the UK, as revealed by a review of the leading approaches.

Broadly speaking, guidance produced in the UK on the test of "necessary" tends to focus on two issues: (i) whether "necessary" means the processing must be "essential" or "indispensable" to meet the processing aims, or a lesser standard of being merely one appropriate route out of several; and (ii) whether there is any need for the processing to be proportionate.

The earliest guidance was published by the ICO in 2001. This stated that the term "necessary" should be interpreted *objectively* by data controllers, who must assess whether:

- The purposes for which the data are being processed are valid;
- Such purposes can *only* be achieved by the processing of personal data; and

---

[24] *Huber v Bundesrepulick Deutschland* (C-524/06) [2009] 1 CMLR 49, at para 52. After giving general guidance as to the importance of "necessary", the Court of Justice of the European Communities then restricted its opinion in this case to a very fact-specific decision, which provides little guidance other than that the processing must be necessary in terms of Art 7 of the Data Protection Directive 95/46/EC. It held in this case that the processing was not necessary, since the objective could have been achieved through anonymisation: at paras 53-68.

[25] *Huber v Bundesrepulick Deutschland* (C-524/06) [2009] 1 CMLR 49, at para 51, with reference to *Lindqvist* (C-101/01).

[26] Jay comments that in fact the test applied in *Huber* is "perhaps a rather stricter approach" than that taken in the UK: Jay, *Data Protection Law* at para 5-03.

- The processing is proportionate to the aim pursued.[27][Emphasis added]

Thus, as early as 2001, "necessity" was being given a strict interpretation requiring it to be essential, that is the only means to achieve the processing purpose. Moreover, despite no reference in the DPA to proportionality, the ICO's guidance was clear that this was a relevant test in determining necessity – a direct reference to the jurisprudence surrounding Article 8 ECHR. In contrast, the ICO's subsequent guidance, published in 2010, revised the test. Here, the term "necessary":

> Imposes a strict requirement, because the condition will not be met if the organisation can achieve the purpose by some other reasonable means or if the processing is necessary only because the organisation has decided to operate its business in a particular way.[28]

Both versions consider that "necessary" should be interpreted objectively, rather than subjectively according to the considerations of the data controller. However the 2010 guidance does not take into account the concept of "proportionality" present in the 2001 version. It is not clear why this has been dropped. Indeed, much of the other guidance considered below continues to refer to proportionality, as will be seen. Further, the 2010 guidance muddies the water as regards the essential nature of the processing. It no longer emphasises that the processing must be the *only* way to achieve the aims, but seems to indicate that the processing will be deemed necessary (and therefore legitimate) if there would be other means to achieve the end, but they would not be reasonable. Of the two approaches, it appears to be the earlier version which meets the proposals currently under discussion in the draft Data Protection Regulation 2012. Recital 30 states: "Personal data should only be processed if the purpose of the processing could not be fulfilled by other means". The concept of necessity in the UK may therefore be clarified if and when this version of the Regulation is in force.

Although the ICO has dropped the requirement for proportionality, most other attempts to define necessity emphasise its importance. In *Michael Stone v SE Coast Strategic Health Authority*, the English High Court considered "necessary" in reference to the Freedom of Information Act 2000 (FOIA).[29] Mr Justice Davis stated that:

---

[27] ICO, *Data Protection Act 1998 Legal Guidance*, Version 1 (2001) at para 3.1.6: available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf (accessed 25 March 13).

[28] The ICO discusses the term "necessary" both in terms of its use in Schedule 2 as to personal data, and also to its use in Schedule 3 as to sensitive personal data. ICO, *The Guide to Data Protection*, (2010) 114, available at

https://www.ico.gov.uk/tools_and_resources/~/media/documents/library/Data_Protection/Practical_application/THE_GUIDE_TO_DATA_PROTECTION.ashx (henceforth ICO, 'Guide to Data Protection 2010') (accessed 25 March 13).

[29] *Stone v South East Coast Strategic Health Authority* [2006] EWHC 1668 (Admin).

> It is common ground that the word "necessary", as used in the Schedules to the 1998 Act, carries with it the connotations of the European Convention on Human Rights: those include the proposition that a pressing social need is involved and that the measure employed is proportionate to the legitimate aim being pursued.[30]

This approach was upheld in a data protection context in *Corporate Officer of the House of Commons* v *The Information Commissioner and Others*, where the Information Tribunal made specific reference to *Stone*, and echoed the wording of Mr Justice Davis.[31]

Other cases where the data protection question in this context was answered by reference to the Article 8 concept of proportionality include *R (Ellis) v Chief Constable of Essex Police*[32] and *R v Secretary of State for the Home Department (ex parte Daly)*, where Lord Steyn set forth a test for proportionality that directly referenced Article 8 jurisprudence.[33] A recent Scottish decision of the Court of Session, *South Lanarkshire Council v The Scottish Information Commissioner*, acknowledged the importance of these decisions, but the Court ultimately reserved its opinion as to whether to follow the test of necessity set out in the English jurisprudence or apply the "ordinary" meaning of the word.[34]

The consequences of incorporating proportionality within the test of necessity will be explored below. At this stage, it should be noted that regardless of which approach is ultimately followed, one essential step forward would be to ensure harmonisation *within* the UK. Absent definitive guidance from the legislature or the ICO, the English and Scottish courts should adopt the same approach to determining necessary. Failure to do so may result in different tests for necessity north and south of the border. In extreme cases, this could mean that a public body in Scotland might meet the test of necessity, thereby legitimately processing personal data, whereas its counterpart in England would not, and would be unable to process the personal data to provide the equivalent services – or vice versa.

Thus, despite the lack of explicit reference to Article 8 ECHR, or indeed to proportionality in the DPA, the courts have typically taken a purposive approach to interpreting the Schedule 2 conditions, giving due credit to the privacy rationale underlying the DPA. The most recent decision of the UK Supreme Court has,

---

[30] *Stone v South East Coast Strategic Health Authority* [2006] EWHC 1668 (Admin), at para 60 per Mr Justice Davis. Note however that, although Jay accepts the use of proportionality, she queries the use of pressing social need as being "somewhat misleading", since the social need is already required by the Schedule 2 condition for processing: Jay, *Data Protection Law* at para 5-03.

[31] [2009] 3 All ER 403 at para 59, citing *Stone v South East Coast Strategic Health Authority* [2006] EWHC 1668 (Admin), at para 60 per Mr Justice Davis.

[32] *R (Ellis) v Chief Constable of Essex Police* [2003] EWHC 1321 (Admin) per Mr Justice Goldring, at paras 1-3.

[33] *R (Ellis)* at para 29 citing *R v Secretary of State for the Home Department (ex parte Daly)* [2001] UKHL 26, per Lord Steyn, at paras 26-27.

[34] *South Lanarkshire Council v The Scottish Information Commissioner* [2012] CSIH 30, at para 10.

however, moved away from reliance upon the ECHR – while still endorsing a test of proportionality. In *The Rugby Football Union (RFU) v Consolidated Information Services Ltd (Viagogo)*,[35] the claimants sought to enforce their data protection rights not by reference to the DPA or Article 8 ECHR, but instead under the Charter of Fundamental Rights of the European Union of 7 December 2000 (CFR). The Treaty of Lisbon 2009 gives direct effect to the CFR, and thus *its* Article 8, which enshrines the protection of personal data as a fundamental right in all Member States.[36] The Supreme Court therefore applied the CFR and upheld the RFU's claim to access personal data. It remains to be seen whether the specific data protection right under the CFR will now take precedence in cases involving data protection rights, instead of the previous reliance on Article 8 ECHR jurisprudence.

Both the Scottish and UK Governments provide interpretations of the word "necessary" as it is used in Schedule 2 of the DPA. The Scottish Government considers "necessary" in this context to encompass:

> Matters which are 'reasonably required or legally ancillary' to the accomplishment of the specified purposes, it is not limited to those matters which are 'absolutely essential' to the accomplishment of those purposes.[37]

This interpretation is noticeably broader than those offered by the ICO and the Scottish and English Courts, yet it is perhaps open to challenge on the basis that the primary reference is a non-data protection specific case, dating from 1849.[38] This same guidance immediately follows with reference to *R (Ellis)*, which, as noted above, interpreted "necessary" in Schedule 2 with direct reference to Article 8 ECHR.[39] Thus the Scottish Government appears to adopt a combined interpretation of "necessary", referring to the Article 8 ECHR requirement of a "pressing social need" in terms of proportionality, while accepting that the processing need not be strictly necessary. Again, leaving aside the wider question of proportionality at this stage, this is unsatisfactory at a very practical level: the lack of consistency with other Scottish or English interpretations leads to yet another possible regime for data controllers to follow and is evidence of the non-uniform approach to data protection in the public sector.

The UK's Ministry of Justice, which is responsible for domestic data protection and representing the UK's interests internationally,[40] published data sharing guidelines in

---

[35] [2012] UKSC 55 (21 November 2012).

[36] Confusingly, Article 8 in the Charter concerns the right to data protection, and Article 9 protects privacy, whereas under the ECHR, Article 8 protects privacy and there is no specific protection for personal data above and beyond the Article 8 right to private life.

[37] Scottish Executive, "Data Sharing: Legal Guidance for the Scottish Public Sector" (2004) at 29, available at http://www.scotland.gov.uk/Publications/2004/10/20158/45768 (accessed 25 March 13) (henceforth, Scottish Executive, "Data Sharing"), citing *A.G. v Walker* 154 E.R. 833; [1849] 3 Ex. 242.

[38] *A.G. v Walker* 154 E.R. 833; [1849] 3 Ex. 242.

[39] Scottish Executive, "Data Sharing" at 29.

[40] Ministry of Justice, "Ministry of Justice responsibilities" (2012), available at http://www.justice.gov.uk/about/moj/what-we-do/our-responsibilities#def.

2012. These state that data sharing under Schedule 2 may be considered necessary "if it is a proportionate method of achieving a legitimate objective: it need not be absolutely essential to the achievement of that objective". [41] As with the Scottish Government guidance, this rejects the ordinary meaning of the word "necessary" which connotes a strict interpretation of being absolutely essential, but also incorporates Article 8 language by referencing proportionality and the need for a legitimate objective (which is akin to a "pressing social need"). Thus both the Scottish and UK Governments continue the trend of blurring the line between the DPA on the one hand and the right to privacy under Article 8 ECHR on the other, by choosing to embed Article 8's interpretation of proportionality into DPA jurisprudence. Whether or not this is inevitable is considered in section 4 below ("Establishing the basis for Proportionality"), where we will assess if, in fact, this approach is merited.

3.2 Developing a meaningful approach to necessity

Two things are clear from the various interpretations of necessary which are currently on offer in the UK. The first is the lack of definitive guidance. From a practical perspective, it is not obvious how a data protection officer should go about assessing whether processing in his/her organisation is necessary. Does necessity mean "essential", or just "one reasonable means"? What role should be played by proportionality, if any? Accordingly, whether or not the proposed processing is legitimate in terms of Schedule 2 will remain uncertain, potentially pending litigation. This is entirely unsatisfactory.

The second observation is that the majority of the guidance (the exception being the revised ICO guidance from 2010) employs the concept of proportionality, although the language of proportionality is not used in Schedule 2 to the DPA. This leads to the further question: is proportionality a necessary part of the test of necessity?

In fact, a standard which looks only to necessity in the strict sense of meaning "essential" fails to reflect the competing interests at stake, namely how important is the processing when set against the consequences of using personal data? The critical factor which should be reflected in any definition of necessary is the balance between the personal data sought to be used and the aims sought to be achieved. The question therefore becomes "is the processing proportionate"? Only where the legitimate purposes of the data controller can be met by *proportionate* use of the personal data should the processing be deemed necessary. This sets a high standard for the data controller, while not requiring the processing to be deemed essential in artificial and unhelpful ways.

Of the definitions reviewed above, the one that comes closest to this standard is the recent guidance from the Ministry of Justice in 2012, which indicates that data processing (specifically data sharing) will be necessary "if it is a proportionate method of achieving a legitimate objective".[42] This reflects a rigorous standard, while

---

[41] Ministry of Justice, *Data Sharing Protocol Annex H* (2012) at 13 citing *Stone* at para 60, *R (Ellis)* at para 29, and *R (Daly) v Secretary of State for the Home Department* at paras 27-28.

[42] Ministry of Justice, *Data Sharing Protocol Annex H* (2012) at 13.

avoiding the rigidity and potentially arbitrary nature of a test which relies solely on whether the processing is "essential".

This definition also addresses the second question posed above: what role is there for proportionality? A definition of necessity which requires the data controller to establish that its processing is valid when weighed against the use of personal data, does require a balancing test, thereby requiring an examination of proportionality.

4. Establishing the basis for Proportionality

While the above definition appears to indicate that a test of proportionality is a vital part of the Schedule 2 conditions, this is nevertheless a challenging position since there is no mention whatsoever of "proportionality" in Schedule 2, or indeed elsewhere in the DPA or the Data Protection Directive 95/46/EC.[43] A balancing test *is* envisaged in condition 6 of Schedule 2, which stipulates that the processing must be necessary for legitimate interests pursued by the data controller "except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject". This reflects recital 30 and article 7 of the Data Protection Directive, and clearly imposes a duty to balance the legitimate interests of the data controller in the processing against the legitimate interests of the data subject, albeit not couched in the language of proportionality. It could be argued that the fact that condition 6 expressly requires a form of balancing exercise means that one cannot be implied in conditions 2-5.[44] Similarly, one could argue that if the proportionality test itself was intended to be part of the test of necessity, then it could have been explicitly incorporated into the Data Protection Directive and hence to the DPA. Instead, proportionality flows from jurisprudence developed under the Article 8 ECHR privacy right, and it is not immediately obvious that this can or should be translated into the data protection arena. This is because the DPA, while drawing on concepts of privacy, in fact provides a discrete legal right for data subjects, separate from their right to private life under the ECHR.[45] The question then becomes whether there is a legal basis for requiring proportionality as part of the necessity test. This section will explore that question.

The DPA regulates the processing of personal data, being any data which identifies a living individual.[46] There is no requirement for that personal data to be "private" or

---

[43] Albeit the latter does refer on occasion to acts which are "disproportionate" – but not specifically the test of proportionality.

[44] Condition 1 is where the data subject consents to the processing, and this does not turn upon necessity.

[45] Although Data Protection Directive 95/46/EC upon which the DPA is based, does make specific reference to the need to protect individuals' privacy, this is only one of the principles underlying the Directive: see Recital 2 and Article 1. The distinction between private life and data protection gains further strength from the CFR which, as noted above, contains two separate fundamental rights: one for data protection and one for private life.

[46] Or which would be capable of identifying a living individual when taken with other information in the possession of, or likely to come into the possession of, the data controller. See the definition of "personal data" in section 1 of the DPA. See also section 1 for definitions of the "data controller" and "data subject".

give rise to a reasonable expectation of privacy.[47] The protection of personal data is therefore not synonymous with privacy in its broad sense.[48] There is a consequent danger that reliance on proportionality here risks conflating two separate rights: privacy and data protection. It is not axiomatic that the test of necessity under Schedule 2 should be interpreted in light of Article 8 ECHR – or at least, not on every occasion. Where there is a privacy interest as well as a data protection interest, then Article 8 ECHR jurisprudence will be relevant, and the case is clear in relation to *sensitive* personal data, since recital 34 of the Data Protection Directive does specifically require member states to protect the privacy of individuals.[49] If privacy is only relevant in certain data protection situations, then we may end up with a two-tier system, whereby data protection claims are treated differently depending on whether there is also a reasonable expectation of privacy. This would be manifestly inappropriate, in that it would be unfair to data subjects and lead to yet further uncertainty and confusion for data controllers in applying the DPA.

The first data protection principle, however, ensures that there is no need for a two tier "privacy/no privacy" approach to data protection. Since the first data protection principle in the DPA requires *all* processing to be lawful, and lawfulness requires, inter alia, compliance with Article 8 ECHR, then a breach of the right to privacy would render any associated processing of personal data unlawful.[50] It is therefore essential that Schedule 2 is applied robustly and with reference to the balance of interests between processing and privacy protection, via data protection: proportionality is the essential element of this.

5. The test of Proportionality

If proportionality is indeed an essential element in balancing processing against data protection in order to determine if the processing is necessary, then it too must be defined. Since the term is not set out in the DPA, we are again left with examining

---

[47] While Auld LJ in *Durant v FSA* [2003] EWCA Civ 1746 did require a privacy focus, through his analysis that the personal data should be "biographical" and have the data subject as its focus – "In short, it is information that affects his privacy" (at para 28) – this decision has of course been subject to widespread criticism, and is potentially part of the reason for the European Commission's concerns regarding the UK's deficient implementation of the Data Protection Directive (for updates on FOI proceedings to access the Commission's letters, see Dr Chris Pounder's blog "hawktalk" at http://amberhawk.typepad.com/amberhawk/.) Moreover, this interpretation is not supported by the DPA, which does not stipulate any need for the personal data to be private. See further Black, *Data Protection*, SME, at paras 410-413.

[48] For example, the right to privacy could be infringed by strip-searching, but there would be no data protection implications here: *Wainwright v Home Office* [2004] 2 AC 406, although note the lack of privacy dimension as the Human Rights Act 1998 did not apply retrospectively in this case.

[49] Recital 34 Data Protection Directive 95/46/EC states: "Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection… whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals".

[50] *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446 at [62]; *Douglas v Hello!* [2003] EWHC 786 (Ch) at [234].

other sources to determine how it should operate. Here, the picture is both enhanced and complicated by the fact that proportionality plays a role in many areas of law, not just in information governance. There is therefore much material upon which to draw. However, two key sources in this field are a 2008 report co-authored by the then Information Commission, Richard Thomas, and a Supreme Court decision from 2012.

In 2008, the Thomas/Walport Report on Data Sharing explained:

> There is no simple answer to the question of when it might be appropriate to share personal information for enforcement and protection purposes. In each case a proportionality test is the most appropriate consideration… *We mean by this the application of objective judgment as to whether the benefits outweigh the risks, using what some might call the test of reasonableness or common sense.* Proportionality involves making a considered and high-quality decision based on the circumstances of the case, including the consequence of not sharing. Decisions must flow especially from the principles of relevance and necessity and the need to avoid an excessive approach.[51][Emphasis added]

At first sight, an objective judgment as to whether the benefits outweigh the risks appears a straightforward and attractive account of "proportionality". Yet there are a number of problems with this, not least the lack of reference to any statutory or judicial authority. This lack of authority is both surprising and disappointing. Further, although initially stated to rely on "reasonableness or common sense", the test then goes on to require "high-quality" decision making, which takes account of the principles of relevance and necessity. How these are to be assessed objectively remains unclear, as does the need to assess what the benefits and risks are in the first place. Formulating the test in these terms places a high burden on the individual decision-maker, while providing little to assist in the practical task of determining whether the processing of personal data is proportionate to the aims sought by the data controller.

Further, since proportionality is in all cases a decision to be taken by the data controller, there is a risk that the test can become meaningless if the decision-maker's approach remains unquestioned: "If one were to adopt… a more deferential view to the question of proportionality and treat with considerable respect the view of the original decision-maker as to whether the interference was justified and proportionate, that would be a much less useful protection".[52]

With this caveat in mind, the most recent and authoritative guidance on proportionality in the context of disclosure of personal data (by way of a *Norwich Phamacal* order) can be found in *The Rugby Football Union (RFU) v Consolidated*

---

[51] Thomas/Walport Data Sharing Review, July 2008, at para 2.8.

[52] Prof David Feldman in evidence to the House of Lords Select Committee on "Surveillance: Citizens and the State", (Report HL 18-I published 21 January 2009): evidence reported 2 April 2008, at para 314.

Information Services Ltd (Viagogo).[53] Here the Supreme Court approved the recent test of proportionality outlined by Mr Justice Arnold in a copyright and disclosure dispute, *Goldeneye v Telfonica*:[54]

> That approach [to balancing] is as follows: (i) neither Article as such has precedence over the other; (ii) where the values under the two Articles are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary; (iii) the justifications for interfering with or restricting each right must be taken into account; (iv) finally, the proportionality test – or 'ultimate balancing test' – must be applied to each.[55]

Despite having senior judicial approval, much remains left to the judgment of the individual decision-maker under this formulation,[56] not least determining the justifications for restricting each right and how to conduct the "ultimate balancing test" between the two rights. Secondary literature may help fill the gap, but such material is likely to fall into one of two categories, both of which present their own challenges. In the first place, academic articles (such as this) may be unknown to the data protection officers operating at the "front line" of data protection. Even if not inaccessible per se, academic commentary is likely to be perceived as too theoretical or abstract, or simply too voluminous, to provide practical assistance, particularly in a time-pressured situation. In contrast, the second type of supporting material would comprise the data controller's own information governance policies. These will certainly be accessible to the decision-maker and, one would hope, practical and relevant. However, they may be out of date and fail to take account of the latest developments, especially European or judicial ones. Perhaps an even more serious concern is that they will also be organisation-specific, thereby adding to the multiplicity of approaches to determining necessity and proportionality. Their efficacy is likely to be tested only in litigation, which is of course is too late for both the data controller and the data subject. Thus, only statutory or definitive judicial guidance can seek to harmonise the test of proportionality in data protection.

While a definitive test as to "proportionality" would be fundamental in assisting data controllers determine whether their processing is legitimate under Schedule 2, such a goal is arguably unattainable – the very nature of the exercise means that there must always be an element of discretion in the decision making. The facts of every case will need to be considered, to ascertain whether the nature and the extent of the processing is necessary and proportionate to the purposes sought to be achieved. If necessity and proportionality under Schedule 2 turn on balancing the value of the

---

[53] [2012] UKSC 55 (21 November 2012).

[54] [2012] EWHC 723 (Ch).

[55] [2012] UKSC 55 at para 44, citing [2012] EWHC 723 (Ch) at para 117.

[56] The individual decision-maker will always be the data controller in the first instance, but may be superseded by the judiciary if the decision is litigated. However, in many cases, the data subject will have neither the means nor the inclination to litigate, although a complaint to the ICO remains an option.

services with the potential detriment to the data subject, then it is essential to examine how these competing interests can be weighed.

Doing so in fact brings in a third element, and it is arguably this element which is the decisive factor: Where does the public interest lie? This involves the identification of a public interest served by the proposed processing, and then determining the extent to which that public interest would actually be met by the processing in question. Our final section will therefore examine the role of the public interest in legitimising (or not legitimising) data processing: What is the role of the public interest, and what value and weight should be assigned to protecting personal data?

6. Identifying the Public Interest

6.1 Introducing the Public Interest

In the context of data protection, there is no single or statutory definition of the public interest. As in any field where the concept is employed, it is a "notoriously uncertain idea".[57] Although there is no definition of "public interest" in the DPA, it has been described by the ICO in relation to freedom of information as covering:

> A wide range of values and principles relating to the public good, or what is in the best interests of society. Thus, for example, there is a public interest in transparency and accountability, to promote public understanding and to safeguard democratic processes. There is a public interest in good decision-making by public bodies, in upholding standards of integrity, in ensuring justice and fair treatment for all, in securing the best use of public resources and in ensuring fair commercial competition in a mixed economy.[58]

The guidance further provides that "in each case, the public interest test involves identifying the appropriate public interests and assessing the extent to which they are served by disclosure or by maintaining an exemption".[59] Although this provides detailed (arguably overly detailed) guidance, Laurie notes that "the devil is in the detail of determining what is mean by *public interest* in each case".[60] In fact, in many cases the public interest will be determined on a case-by-case basis, frequently with appeal to political values or judgements. This typically results in a "definition of

---

[57] M Taylor, *Genetic Data and the Law* (Cambridge: CUP, 2012), at 29.

[58] The ICO, "The public interest test – Freedom of Information Act" at para 9, available at *http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/awareness_guidance_3_public_interest_test.pdf* (accessed 25 March 13).

[59] The ICO, "The public interest test – Freedom of Information Act" at para 10, available at *http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/awareness_guidance_3_public_interest_test.pdf* (accessed 25 March 13).

[60] G Laurie, *Genetic Privacy* (Cambridge: CUP, 2002), at 279. For a recent examination of the public interest in the context of privacy, see C. D Raab, "Privacy, Social Values and the Public Interest" in A Busch and J Hofmann (eds), *Politik und die Regulierung von Information*, Politische Vierteljahresschrift Sonderheft 46, (Baden-Baden: Nomos Verlagsgesellschaft, 2012), at 129-151 (hereafter C Raab, 'Privacy, Social Values and the Public Interest').

'public interest' [which] is very unclear and yet… is the heart of the overriding of the individual's rights".[61]

6.2 An Individual Right vs the Collective Public Good?

While the public interest under Schedule 2 will typically depend on the nature of the public services provided, the debate about the value of protecting personal data, and privacy, is harder to assess. Typically, personal data and privacy can be categorised as individualistic rights (especially by "opponents" who wish to play down the significance of privacy in society).[62] Where this is the case, and privacy is seen as protecting only individual interests, then it can be difficult to envisage many situations where the individual rights of the data subject would outweigh the wider public interest in permitting the processing to go ahead. This is especially the case where the processing is carried out by public sector organisations for the provision of services which benefit the community more widely – not least those related to surveillance and national security. It is all too easy for the proponents of certain public sector data processing, especially regarding surveillance and national security, to seek to down-play the importance of privacy for the community, and even to advance claims about the damage caused by privacy protection, such as "the common good is being systematically neglected out of excessive deference to privacy".[63] On one level this demonstrates the scope for confusion, with the public interest being adopted to support opposing positions, thereby leaving data controllers in urgent need of clarity and guidance. At a deeper level, however, an approach to privacy and data protection which focuses exclusively on an individualist conception of privacy and balances it against the communitarian interests of society, will always fare badly. This bias can be seen even in less emotive spheres than national security, as a recent case concerning the English Rugby Football Union demonstrates.

In *The Rugby Football Union (RFU) v Consolidated Information Services Ltd (Viagogo)*,[64] the Supreme Court had little difficulty in concluding that the test of proportionality was satisfied and that the personal data should be released. In granting the *Norwich Pharamacal* order to require Viagogo to release the identity of certain of its website users, the Supreme Court asserted that:

---

[61] D Townend, "Overriding Data Subjects' Rights in the Public Interest" in D Beyleveld et al (eds), *The Data Protection Directive and Medical Research Across Europe* (Ashgate, 2004), at 97. (hereafter D Townend, "Overriding Data Subjects' Rights in the Public Interest").

[62] Raab sets out (but does not endorse) this approach: Raab, "Privacy, Social Values and the Public Interest" note 60 above at 131. These tensions are also explored by D Beyleveld, "Data Protection and Genetics: Medical Research and the Public Good" (2007) 18 *King's Law Journal* 275. Even those not evidently opposed to privacy tend to conceptualise it as a purely individual right: see for example the evidence given by Michael Wills MP, a Minister in the Ministry of Justice, reported in the House of Lords Select Committee on "Surveillance: Citizens and the State", Report HL 18-I (published 21 January 2009), at para 264.

[63] Raab summarises the arguments made by Amitai Etzioni amongst others: see Raab, "Privacy, Social Values and the Public Interest" note 60 above at 135, citing A Etzioni, *The Limits of Privacy* (1999).

[64] [2012] UKSC 55.

> All that will be revealed is that identity of those who have, apparently, engaged in the sale and purchase of tickets in stark breach of the terms on which those tickets have been supplied by the RFU.[65]

This disclosure of otherwise anonymous information (and the Viagogo website was apparently deliberately set up to preserve anonymity), was outweighed by the interests of the RFU in having that personal data disclosed to it:

> The entirely worthy motive of the RFU in seeking to maintain the price of tickets at a reasonable level not only promotes the sport of rugby, it is in the interests of all those members of the public who wish to avail of the chance to attend international matches. The only possible outcome of the weighing exercise in this case, in my view, is in favour of the grant of the order sought.[66]

While this may very well be the correct decision on the facts in this case, it is disappointing that the Court did not consider wider issues of privacy and data protection. Although it was willing to countenance the bigger picture when it came to the motives of the RFU in seeking disclosure,[67] this was not balanced by a reciprocal consideration of the potential damage caused to *society* through the disclosure of *individuals'* identifiable personal data.

Professor Charles Raab has explored the conflict between communitarian views of privacy and individualistic views. He poses the critical question "Is it possible to escape an 'individual privacy v. public interest' formulation of the relationship between these two values"?[68] With reference to Solove, he notes that "In the discourse around 'balancing', the individual right of privacy is too often trumped by a concern for the greater social good".[69] From the outset, the attempt to balance a range of interests (collectively labelled as the public interest) against the fundamental rights and freedoms of an individual is unsatisfactory and unequal.[70]

A further imbalance arises when the rights of the individual are balanced against the rights of the many: "The inevitable imbalance in favour of the majority can immediately be understood: a substantial damage to the particular individual is soon

---

[65] [2012] UKSC 55, at para 45.

[66] [2012] UKSC 55, at para 45.

[67] The Supreme Court rejected Viagogo's argument that the RFU's case should be made entirely on the need to access the data of a named individual – instead, the Court was willing to take into account the benefits to the RFU more widely.

[68] See C Raab, "Privacy, Social Values and the Public Interest" note 60 above at 129.

[69] See C Raab, "Privacy, Social Values and the Public Interest" note 60 above at 130, citing D Solove, *Understanding Privacy* (2008), at 78-79.

[70] See generally Townend, "Overriding Data Subjects' Rights in the Public Interest" note 61 above, and especially at 98-101; also Julie E Cohen, *Configuring the Networked Self: Law, Code and the Play of Everyday Practice* (Yale, 2012), at 115-120.

outweighed by the sum of the individually negligible benefits to the other individuals within the collective".[71]

6.3 Data Protection and Privacy as a Facet of the Public Interest

This does not need to be the case, however: protecting personal information can have benefits to society more widely. As Raab says, "Privacy has a long-standing, and valuable, normative and humanistic affinity with individual autonomy and dignity".[72] Respecting privacy not only avoids harm to specific individuals, but respects them as individuals,[73] and thereby respects society as a whole. It can therefore be seen as a benefit to society in its own right – and consequently, its protection is very much in the public interest.[74] Privacy, understood in this sense, moves away from a stark individualist view to one which recognises and accepts it as a communitarian interest in its own right.

On this analysis, data protection may be a private right, but there is a cogent public interest in maintaining it. This is very clearly expressed in *W v Edgell*, a case involving breach of confidence rather than data protection, but otherwise very much in line with the "individualist vs communitarian" debate. In this case, W, a patient detained in a special hospital after he shot seven people, five of whom died of their injuries, engaged the services of Dr Edgell as a consultant psychiatrist to produce a report for use by W at his Mental Health Review Tribunal hearing. The question that arose was, when W decided that the report was prejudicial and that he would therefore not disclose it, could Dr Edgell nevertheless send it to the hospital authorities and to the Home Office? Was such disclosure an unjustified breach of confidence,[75] or was it justified by the wider public interest?

The Court of Appeal upheld the trial judge's conclusion that disclosure was justified, even against W's wishes. Critically, however, Lord Justice Bingham disagreed with the judge's approach that W only had a private interest in maintaining confidentiality, but no wider public interest in doing so:

> Here, as I think, the trial judge fell into error. W… had a personal interest in restricting the report's circulation. But these private considerations should not be allowed to obscure the public interest in maintaining professional confidences.[76]

---

[71] See D Townend, "Overriding Data Subjects' Rights in the Public Interest" note 61 above, at 99.

[72] Raab, "Privacy, Social Values and the Public Interest"note 60 above at 131.

[73] G Laurie, *Genetic Privacy* (Cambridge: CUP, 2002), at 255.

[74] See C Raab, "Privacy, Social Values and the Public Interest" note 60 above at 135; G Laurie, *Genetic Privacy* (CUP, 2002), at 279 *et seq*; D Beyleveld, "Data Protection and Genetics: Medical Research and the Public Good" (2007) 18 *King's Law Journal* 275, at 283.

[75] The question was not whether Dr Edgell's disclosure was a breach of confidence: it clearly was. The only issue for debate was whether the breach was justified: *W v Edgell* [1990] 1 All ER 835 at 842, with reference to the trial judge's decision at [1989] 2 WLR 689 at 710D.

[76] *W v Edgell* [1990] 1 All ER 835 at 849.

He continued that:

> The crucial question in the present case was how, on the special facts of the case, the balance should be struck between the public interest in maintaining professional confidences and the public interest in protecting the public against possible violence.[77]

Thus, a right should not be seen solely as an individual right simply because it is advanced by an individual: it may still have wider implications, and benefits, for society as a whole. This applies to data protection and privacy as much as to confidentiality. As JUSTICE has explained:

> In our view, privacy is best understood as a public good. By this we mean that there is a collective interest in maintaining a society in which personal privacy is protected. There are a number of reasons for this, not the least of which is that a free society is one that respects individual freedom to live a life without undue interference or scrutiny. Another reason is the belief that individuals are more likely to be contribute [sic] to the maintenance of a good society where they recognise that that society is concerned to protect their own rights, including the right to privacy.[78]

Dr David Townend has argued that this approach is especially important in the European Union, where "the purposes of the Union are themselves matters of the public interest and not matters of private interests against public interests. It is in the public interest to create a single market and to ensure that individual rights and freedoms flourish through its ever more effective operation".[79]

These arguments strongly support Laurie's analysis that the starting point should be upholding the fundamental rights of privacy and autonomy, and liberty:

> If we wish to move from that then the obligation and the onus is on the state to show that it is necessary and proportionate in the particular circumstances, and

---

[77] *W v Edgell* [1990] 1 All ER 835 at 851.

[78] Memorandum submitted by JUSTICE to the House of Lords Select Committee on "Surveillance: Citizens and the State", (Report HL 18-I published 21 January 2009): reported 6 February 2008, at para 1.

[79] See D Townend, "Overriding Data Subjects' Rights in the Public Interest", note 61 above at 99. In fact, this is part of Townend's alternative analysis. He argues that the public interest can be reframed as a series of individual interests: the balance to be struck then becomes one of competing *individual* interests, in privacy versus the benefit to an individual to be gained through the processing. This approach is not followed here, in part because it removes the emphasis from the core purpose of public sector service provision: serving the community, and improving conditions for all, even those not individually benefited by the services. (For example, the provision of health care by the state benefits me even if I am never ill, or have private health care, since it is of benefit to live in a healthier society, with reduced social and economic consequences arising from ill-health.) See Townend at 98-101.

> the circumstances obviously depend on what are the social ends that you are trying to achieve.[80]

6.4 Public Sector data processing and the Public Interest

If this approach is not taken, and the predominant approach is to focus on privacy and data protection as a right solely to protect individual interests, it will almost always be possible for public sector data controllers to legitimise their processing under one of the heads in Schedule 2, since it will always be regarded as "necessary" and proportionate. On this analysis, Schedule 2 is weighted from the outset in favour of processing by public sector bodies. This is because the purpose of the processing by a public sector body will, by definition, almost always be a purpose in the wider public interest – in contrast to private sector processing, where the purpose may well be a private, commercial gain.[81] Thus, the application of Schedule 2 potentially raises very different issues in the public and private sectors.

A further risk is that the public interest in this context can be abused, where it is measured against an individualist conception of privacy. As the House of Lords Select Committee on *Surveillance: Citizens and the State* noted with concern, the guaranteed right to privacy under Article 8 ECHR was "too easily overridden by governments' unsubstantiated assertions about the necessity of, for example, an anti-crime measure".[82] In such a situation, the balancing exercise is heavily predisposed from the outset, in favour of public sector processing.[83]

Conversely, where privacy and the protection of personal data is seen as a value to be upheld for the benefit of society as a whole, and not just the individual, then the balancing exercise may end up being almost impossible to resolve. Adopting a communitarian interpretation of the value of privacy means that upholding privacy and protecting personal data is seen as being in the public interest in its own right, ie that there is a public value in respecting personal data per se. When a public body therefore has to decide between processing and not processing, the conflict can be expressed as follows:

> Provisional of [valuable] public services **vs** protection of personal data/ privacy

---

[80] Prof Graeme Laurie in evidence to the House of Lords Select Committee on "Surveillance: Citizens and the State", (Report HL 18-I published 21 January 2009): evidence reported 30 January 2008, at para 309.

[81] Although the public interest test was satisfied in *The Rugby Football Union v Consolidated Information Services Ltd (Viagogo)* case, where a private organisation's alleged need for the personal data was held by the Supreme Court to be in the wider public interest in facilitating access to rugby: [2012] UKSC 55. The RFU's role in encouraging grass roots engagement with rugby does, however, cross the private/ public threshold. For the majority of private organisations, the balance in question is more likely to be between protecting privacy vs commercial interests: it therefore requires a different balance to be struck.

[82] House of Lords Select Committee on "Surveillance: Citizens and the State", Report HL 18-I (published 21 January 2009), at para 313.

[83] See also the arguments referred to above, by Townend and others.

On a communitarian understanding of the value of privacy, this equates to:

> Protection of public interest **vs** protection of public interest

There is thus no clear way to resolve the conflict. In either case, the outcome appears unsatisfactory: public authorities are faced with a default which weighs heavily in favour of the processing, or alternatively, a default which accepts that both the processing and the privacy are evenly balanced. Against such a background, how can public sector bodies (and their employees) ever apply a rational and consistent test to determine if their processing is necessary and proportionate?

In fact, it is possible to move away from seeing data protection as an obstacle to data processing in the public interest. Rather than endorsing an adversarial conceptualisation, a more constructive approach would be to move to a cooperative model, which seeks to enhance privacy while still using personal data in the provision of public services. The advantages of a cooperative model are explored by Beyleveld, who points out that the values underlying medical research and privacy do not necessarily conflict:

> Research can increase life choices and improve quality of life. These are privacy values. Conversely, consent to the use of personal data for research, which is centrally protected by the right to privacy, permits more accurate research data to be obtained…[thereby enhancing] research. Perhaps most importantly, respect for privacy… facilitates public trust, which is positively necessary for research, not merely facilitative of better quality research.[84]

These conclusions hold true for public sector services as well as medical research. Whereas Beyleveld focuses on obtaining consent in the medical research context, this is likely to be replaced in the public sector by the need to show necessity in terms of Schedule 2. As explained in section 2 above ("Data Processing and the Public Sector: Schedule 2 Conditions"), consent is unlikely to provide an attractive or available basis for much public sector processing. Instead, the use of personal data must be justified on grounds of necessity and the wider public interest in processing, and these justifications must then be weighed against the public interest in protecting personal data.

Where the data controller has data protection and privacy as a genuine aim, rather than a secondary consideration, then the provision of public services can be facilitated within a rigorous information regime. As Raab notes however, "Theoretical discourse aside, there are only rare and fragile exceptions in public policy that aim to set aside the duality".[85] Critically, one of these exceptions, where public policy has sought to reconcile the two in a practical setting, is:

---

[84] D Beyleveld, "Data Protection and Genetics: Medical Research and the Public Good" (2007) 18 *King's Law Journal* 275, at 287-288.

[85] The duality being the public interest served by the processing of personal data for public services on the one hand, and the data protection and privacy interests of data subjects on the other. See Raab, 'Privacy, Social Values and the Public Interest' at 145.

> The claim – as in the United Kingdom (UK) – that joined-up, information-age government, involving intensive and extensive exploitation of the personal data of citizens in order to provide more effective and efficient public services and to achieve other public policy objectives, can be brought about whilst also enhancing privacy.[86]

The door is already open, in theory at least, for a cooperative model of data processing and protection in the public sector in the UK.

7. A Suggested Solution

To achieve a more integrated and cooperative model of data processing and protection, by ensuring that data controllers take data subjects' interests into account as well as their own interests in processing, we advocate a cumulative three-step test for data controllers to use when determining if their processing under Schedule 2 is indeed necessary. This three-step test is intended to provide greater clarity, by building on the existing legislation and judicial authorities reviewed above. Although it is closely tied to the existing legal framework (as indeed it must be, reflecting the binding nature of this authority), the test is intended to provide a fresh approach through a logical step-by-step guide to each of the key issues in deciding whether processing is "necessary". This should allow data controllers to address Schedule 2 decisions in a coherent and more confident manner, with a clear focus at each step of the way. This goes beyond the current legal provisions in that it provides a finer degree of granularity of the relevant considerations, to allow robust decision-making and the exercise of judgment in application of data protection law.

Thus, the proposed three-step test starts with the existing starting point, which is the need to anchor the processing in Schedule 2 of the DPA. This is then developed to provide a more rigorous framework for data controllers to employ, by moving on to consider the other side of the equation, the interests of the data subject. By identifying these interests in steps 1 and 2, the way is clear for the ultimate balancing test, to determine whether the processing is necessary in terms of Schedule 2: Is the processing proportionate, taking into account the public interests involved? These steps are as follows:

1. Does the processing meet a legitimate objective, i.e., is it in pursuance of a Schedule 2 condition and, where necessary, a Schedule 3 condition as well? (For example, is the processing in compliance with any legal obligation to which the data controller is subject (Schedule 2, condition 3) or for the exercise of any functions of the Crown, a Minister of the Crown or a government department? (Schedule 2, condition 5(c))). Identifying the legitimate objective is a threshold requirement which, unless satisfied, will automatically result in the processing being in breach of the DPA;

2. What personal data is involved in this processing? Is it personal or sensitive personal data? What are the risks involved in using/disclosing it, and what is

---

[86] See C Raab, "Privacy, Social Values and the Public Interest" note 60 above at 145.

the likelihood of actual harm to the individual? Critically, this step transfers the focus of the review from the aims of the data controller (step 1) to the concerns of the data subject; and

3. Does the public interest in processing outweigh the individual's private interest *and* the wider public interest in protecting the personal data?

In order to carry out this balancing test at step 3, the data controller will need to consider a range of risks regarding the personal data involved, such as:

- Is the proposed processing of the personal data the least intrusive means of achieving the public body's objective?;
- Does the processing comply with the other data protection principles including, critically, the third data protection principle, which requires that the personal data processed shall not be excessive?;[87]
- Does the processing only require the use of personal data, and not sensitive personal data?;
- Could anonymisation be used and, if so, is the proposed technique regarded as effective?;[88]
- Has the proposed processing been approved by an appropriate oversight body, where relevant?;
- Has a privacy impact assessment been undertaken to assess and mitigate the risks inherent to the processing in question?;[89]
- Is there an identifiable public interest in processing the personal data?; and
- Is there an identifiable public interest in providing the relevant public services?

Cumulatively, these questions will allow the data controller to determine if the proposed use "is a proportionate method of achieving a legitimate objective".[90]

---

[87] DPA, Schedule 1, Part 1, para 3.

[88] For example, pseudonymisation is regarded as more of a high-risk technique – see further the 2012 ICO guidance on anonymisation: ICO, "Anonymisation: managing data protection risk code of practice" (20 November 2012) 51, available at www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/anonymisation_code.ashx (accessed 19 March 2013).

[89] Further details re privacy impact assessments can be found on the ICO's website: www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx (accessed 19 March 2013).

[90] Ministry of Justice, *Data Sharing Protocol Annex H* (2012) at 13.

Positive answers to these questions will generally be indicative of legitimate processing; negative answers will tend to indicate that the public interest is best served by protecting the personal data and thus favour non-processing. As demonstrated in the foregoing section, however, it is not appropriate to treat the protection of personal data merely as a private interest. Public sector data controllers will therefore have to assess the two competing public interests, in processing *and* in protection, and the steps to doing so are set out in a structured and logical progression in this three-step test.

Moreover, following these steps will assist the data controller in complying with the test of proportionality recently approved by the UK Supreme Court, which requires an "intense focus on the comparative importance of the specific rights", as identified under steps 1 and 2, followed by the ultimate balancing test between the two.[91]

If, taking these factors into account, the answer to the third question is yes, then the processing is necessary and therefore legitimate: the requirements of Schedule 2 are fulfilled. If not, however, then the public interest in protecting personal data and privacy should prevail over the public interest in processing the data.

This approach still leaves an inevitable element of discretion: it provides a framework for the decision-maker without dictating a final answer. However, it does aim to remove the risk of bias in favour of public sector processing (noted above), by requiring the data controller to make a more considered and defensible assessment between its own aims (step 1) and the rights and interests of the data subject (step 2). Thus, what is advocated in this three-step test is not a rule-based approach, but a principle-based one. Principle-based approaches to delicate decisions such as these are valuable because they require an explicit statement of the core values and standards underpinning decision-making in coherent terms. In this case, a principle-based approach sees the relevant factors as different dimensions of the public interest, while not dictating any particular outcome or favouring any particular bias. Principles guide deliberation and action and as such provide a common frame of reference for taking, and justifying, difficult decisions.[92]

While the three-step test still requires the data controller to make a decision based on the range of considerations of the case before it, and can therefore never be reduced to a simple "yes/no" test, there are nonetheless clear benefits in applying this principle-based test. In the first place, it requires the data controller to identify the full range of potentially competing interests, through steps 1 and 2. This ensures that the data controller has a clear understanding of what interests need to be balanced at the outset. Secondly, the use of a structured and coherent test should give data controllers *and* individuals greater confidence in the decision-making process, and therefore in any subsequent use of personal data.[93] This has particular benefits – and is of

---

[91][2012] UKSC 55 at para 44, citing [2012] EWHC 723 (Ch) at para 117.

[92] G Laurie and N Sethi, "Towards Principles-based Approaches to Governance of Health-related Research Using Personal Data" (2013) 1 *The European Journal of Risk Regulation* 43-57.

[93] M Taylor, *Genetic Data and the Law* (Cambridge: CUP, 2012), at 31.

particular importance – in the field of public sector data processing. It is public sector processing which is far more likely to require an analysis of the relevant public interests in assessing the proportionality (and thus the necessity) of the processing. Rather than relying on the consent of the data subject, public sector data controllers must typically seek another basis under Schedule 2 to legitimise their processing, and that basis will speak to the wider public interest in the provision of public services. Thirdly, it requires the decision-maker to articulate and attach appropriate weighting to various considerations and to justify these are part of the process.

By using this test, data controllers in public organisations can engage more rigorously with the public in order to maintain public trust and confidence: "If trust in the treatment of personal data is to be maintained, then individuals must feel that their rights are treated with respect".[94] Critically, this engagement should lead to a more robust data protection culture in the public sector – a culture which has been demonstrated above to be sadly lacking. Where the public sector has greater confidence in its own ability to take legitimate decisions regarding the processing of personal data, the risks associated with breaches will diminish. Consequently, enforcement action and fines should diminish, together with wasted staff time investigating the breaches, while faster, more transparent decision-making should increase, coupled with greater uniformity across the public sector.

Although it is not possible or desirable to impose a rigid formula for use by data controllers, it *is* possible (and desirable) to provide a clearer guide to determining when processing is necessary. Achieving this requires consideration of "necessity", and because necessity is not an absolute, but rather relative, it thus requires consideration of "proportionality". In turn, proportionality requires a balance to be struck between the competing public interests. The three-step test recognises this and provides a means for decision-makers to work through the relative interests at stake. By advancing this three-step test, we are therefore able to provide an essential tool to guide data controllers through this "necessity-proportionality-public interest" chain, and this stands to benefit everyone in this equation: the data controllers, who often have to determine if their processing is necessary without any clear guidance yet while being predisposed to favour it; the data subjects, who may otherwise be left in the dark about the test applied or the basis for processing; and the public, who stand to benefit if data processing is not unnecessarily hindered, but also need to be confident that data protection and privacy are taken seriously and respected.

[94]See D Townend, "Overriding Data Subjects' Rights in the Public Interest"note 61 above, at 101.