WHEN WORLDS COLLIDE: FREEDOM OF INFORMATION AND THE PROTECTION OF HEALTH DATA[1]

Dr Renate Gertz
AHRC Centre, School of Law, University of Edinburgh
Old College, South Bridge, Edinburgh EH8 9YL, UK
Rena.Gertz@ed.ac.uk

I. Introduction

On 11 January 2005 both the Freedom of Information Act 2000 (hereinafter FOIA) [2] and the Freedom of Information (Scotland) Act 2002 (hereinafter 'FOISA') [3] came into force. The purpose to introduce the two Acts was to provide people with a general right of access to information held by or on behalf of public authorities, thus promoting a culture of openness and accountability across the public sector. The Acts enable people to gain access to the desired information in two ways, through publication schemes, where public authorities must make some information available as a matter routine, and through a general right of access, whereby a public authority must respond to a request within 20 working days.

Both Acts, however, recognise that there may be reasons for withholding information and provide a number of exemptions from the right to know. Since both Acts name the same exemptions, when discussing the 'Freedom of Information Act' or (FOIA), this paper includes both FOIA and FOISA. A distinction is made between absolute and qualified exemptions. The application of an absolute exemption will always prohibit disclosure. For a qualified exemption to apply, a public interest test is employed: the public interest in maintaining the exemption must outweigh the public interest in disclosure. One of the absolute exemptions is that of personal data in s 40 of FOIA. However, for defining personal data, s 40 refers to the Data Protection Act 1998 (hereinafter 'DPA'). [4] S. 1 defines personal data as "data which relate to a living individual who can be identified- (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller." S. 2 defines sensitive personal data as "personal data consisting of information as to … (c) his religious beliefs or other beliefs of a similar nature..."

This referral to DPA leaves us with two diametrically opposed pieces of legislation: one which promotes a culture of openness and disclosure and one which promotes a spirit of confidentiality. The difficulty lies in attempting to find a sensible way of, if not combining both, at least agreeing on a feasible compromise. In Scotland, such a first attempt had to be made only eleven days after FOISA came into force.

II. The first health data case

On 11 January 2005, the Common Services Agency for the Scottish Health Service (hereinafter 'the CSA') received a request for information on incidences of childhood leukaemia, from 0 – 14 years, by year and census ward from 1990 to 2003 for a relatively small Scottish region. The CSA refused the request for the following reasons: the

combination of the rare diagnosis, specified age group, small geographical area and low numbers resulted in individuals being identifiable, hence the information fell within the definition of 'personal data' under DPA and should not be disclosed; and that having never performed the necessary analysis of the data by census ward, the CSA did not hold the data. The applicant, Mr Collie, requested that the CSA review its decision and subsequently appealed to the Scottish Information Commissioner (hereinafter 'the SIC') for a ruling.

The SIC accepted that the requested data constituted personal data under DPA, however, he nevertheless ruled that a perturbed, 'barnardised' version of the requested table, i.e. one that involved changing small figures by adding 0, +1 or -1 to maintain anonymity, could have been provided.[5] On this basis the SIC held that the CSA was in breach of FOISA because it had not provided sufficient advice and assistance to Mr Collie as to what information it was able to supply as required under section 15 of the Act.[6] The CSA has decided to appeal this decision and the case is scheduled to be decided by the Court of Session in Edinburgh.

III. Implications of the *Collie* case

The *Collie* case is the first appeal to an information commissioner which focuses on the interface between data protection and freedom of information with an impact on healthcare. [7] The case hinges on the definition of personal data with the outcome having potentially wide-ranging implications for the future of data protection and freedom of information regimes alike. The policy issues raised are significant and have the potential to create a dangerous precedent for public health authorities that are charged, simultaneously, with protecting patient data and complying with provisions of freedom of information legislation.

1. Defining personal data

Besides the problem of a potential breach of data protection principles, the definition of personal data is challenging. The precedent in the UK dealing with a definition of personal data is *Durant v Financial Services Authority*, heard by the Court of Appeal in 2003.[8] To qualify as 'personal data', so said the Court of Appeal, the information must have a focus on an individual or be of biographical significance for the individual concerned. What needs to be taken into consideration, however, is the fact that DPA is the UK implementation of the European Data Protection Directive 95/46. It is the duty of member states to adopt legislation implementing directives in such a way as to give full effect to the Directive's aim and meaning. Since in the UK, both statute and common law provide the full tapestry of law, both are taken into account when determining whether a Directive has been properly implemented.

Article 249 (ex 189) of the Treaty of the European Union provides that "a Directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods." Hence, a Directive aims for harmonisation rather than unification of law. Contradictions and inconsistencies between national laws and regulations conflicts are to be ironed out to achieve the same conditions all the Member States. Even once the question of the direct effect of Directives had been resolved, [9] problems can still remain about the relationship between Directives and the national law. In *von Colson* [10]and *Harz* [11], the European Court of Justice provided rules to be applied by national courts when interpreting legislation

implemented from Community law. Accordingly, national courts had to ensure that their country's laws implementing a Directive are interpreted in the light of the wording and purpose of the directive. [12] Thus, at the 4th Annual Data Protection Compliance Conference on the 4th of October 2005, the Head of Data Protection at the European Commission confirmed that the UK will be prosecuted before the European Court of Justice if no remedial action is taken to bring the UK's interpretation of 'personal data' as defined in *Durant* in line with the Directive as, according to the European Commission, *Durant* provides an interpretation of 'personal data' which is too narrow by far.

The relevance for the interface between data protection and freedom of information is obvious. Due to FOIA referring to the definition of personal data provided by DPA, the question whether *Durant* will continue to provide the yardstick by which the applicability of 'personal data' is measured is relevant for both Acts and a ruling against the UK will impact on both pieces of legislation. This will have a practical difficulty for the interface between the two Acts in Scotland: In England and Wales, the office of the Information Commissioner is responsible for both data protection and freedom of information. Hence, new policies regarding the definition of personal data will be applied by the same office for both regimes. The SIC is only responsible for freedom of information in Scotland, data protection being a national matter. Accordingly, one would hope that the SIC would obtain a policy on personal data from England before being able to apply it to Scottish freedom of information appeals, as it would be unacceptable if differing interpretations of 'personal data' were to emerge.

2. Breaching the data protection principles

Since delivering the decision in *Collie*, another two cases involving health-related information have been decided by the SIC, *MacMahon* and *Fracassini,* two nearly identical cases submitted within days of each other.[13] Both requests, like *Collie*, were addressed to the CSA and had surgeon mortality rates as their subject. However, while *Collie* mostly dealt with the question of defining personal data, the question whether disclosure of the information sought by the applicants could be considered as a breach of data protection principles was crucial for the two cases. The CSA argued that the data requested had living, named third parties as their subject, a disclosure of which would constitute a breach of the first data protection principle: to process personal data fairly and lawfully. While the SIC accepted that living individuals were easily identifiable as individual surgeons are named, however, he rightly pointed out that for s 38 (1)(b) to provide an exemption, disclosure of the information must have breached a data protection principle. The CSA had not claimed that providing the requested information would have been unlawful, and the SIC decided accordingly. *Fairness*, however, was disputed. The CSA had argued that the information was collected from surgeons in a confidential context, hence, disclosing the information to third parties breached the fairness requirement. The SIC disagreed and decided that no confidentiality was breached, and, referring to guidance from the UK Information Commissioner on the personal data exemption, divided personal information into data relating to private or professional lives.

This, however, raises an interesting point. In the legal guidance DPA regarding the first data protection principle, the UK Information Commissioner does not distinguish between personal data regarding private or public lives. In the legal guidance on DPA, the main focus is on information provided to data subjects about disclosure of their data. No mention

is made of a distinction between private and public lives of the data subject. In the FOIA guidance on the personal data exemption, however, the UK Information Commissioner differed from his previous guidance on DPA and placed a different emphasis. No mention is made of informing the data subject of the disclosure, rather, a brief description of distinguishing between public and private lives is provided. The SIC guidance follows along the same lines. This raises the question of applicability in the light of the boundaries between data protection and freedom of information regimes. Ultimately, several different possibilities exist, as this interface is still very much uncharted territory. Hence, the following discussion is speculative. To summarise, guidance on the 'fairness' requirements of the first data protection principle exists on both DPA and FOIA, however, with both guidances discussing different issues. Both systems rely on protecting personal data through the prevention of breaching a data protection principle with FOIA referring to DPA. Hence, both acts should employ the same definitions and treat the fairness requirement in the same way for, at least, the sake of consistency and, at most, legal certainty.

The first option, applying guidance developed for DPA to FOIA, seems unproblematic due to the very nature of the referral. FOIA refers to DPA for a definition of the personal data exemption in all its facets. This means that the guidance has been provided for personal data in connection with DPA by the UK Information Commissioner who is the UK-wide authority for data protection. Hence, this guidance will need to be taken into account. Similarly, guidance provided by the UK Information Commissioner on the personal data exemption in FOIA will need to be taken into account in the same way in England and Wales, while in Scotland, guidance by the SIC applies. As there is no difference between the guidances in this respect, there is no need to differentiate.

The other option would be to indiscriminately apply the private/public lives distinction to DPA and the requirement of informing data subjects of disclosure to FOIA. This, however, does not take the fact into account that what we have is a referral in only one direction. FOIA refers to DPA, but DPA does not refer back to FOIA. This raises the question whether this 'unidirectional' referral will require special consideration. Thus, would guidance developed for the referring Act, FOIA, need to be applied to the DP Act to which FOIA refers? Applying FOIA guidance on the first data protection principle to DPA would thus constitute a reversal of the direction the referral takes. FOIA introduces an addition to the definition of personal data as provided by DPA. With regard to this, the situation is clear: newer legislation trumps older legislation, additions to legislation will apply to both the new and the old Act. The question, however, remains whether this can be transferred to guidances, since, obviously, guidance does not have the same status as official legislation.

3. Preventing identifiability

The data protection regime relating to healthcare aims to protect patient privacy by regulating the processing of 'personal data' – data which relate to an individual and from which the individual can be identified. This does not require a single set of data, but identifiability can occur through the linkage of two or more sets of data.[14] Hence, application of the data protection provision hinges on the crucial concept of identifiability. Until the coming into force of FOIA, sensitive medical data were most frequently processed and disclosed in a medical or medically related context. Healthcare in its widest meaning, medical research, clinical audits and registries such as the cancer register were

the most common reasons for disclosing health data. According to DPA, this disclosure requires one condition each from Schedule 2 and 3 of DPA to be fulfilled, such as the data subject consenting to the disclosure, a case of public interest in disclosing the data or where disclosure was necessary for the vital interest of the data subject.

One of the most commonly recognised mechanisms to avoid identifiability and having to fulfil a condition of Schedules 2 and 3 is anonymisation of the data in question. Defining anonymity, however, is problematic, as it remains unclear what counts as a legally acceptable level of anonymisation and what does not.[15] It has been accepted that the law does not require absolute anonymity to be achieved, i.e. that no link can ever be made between data and data subject. [16] That leaves the possibility of relative anonymity, which entails varying degrees of identification depending on the circumstances of the case in question.

With this in mind, the CSA argued in the *Collie* case that the application of the particular type of perturbing the requested data, the so-called 'barnardisation' the SIC sought to impose was not sufficient to anonymise the data in this case to an acceptable degree. The problem raised by disclosing the data, even in a 'barnardised' state, was the remaining possibility of identifiability through the *connectivity* of the data. Even with perturbed data, there remained a significant degree of risk that the data revealed in the statistical table might, on release, be easily linked to other data in a manner that would allow individuals who have suffered from leukaemia, be readily identified. In a case such as this, the spirit of the data protection regime which engenders a culture of caution and where non-disclosure of personal data is the order of the day, would prohibit a disclosure of data to a third party.

The spirit of the freedom of information regime is diametrically opposed to this culture of protection. Its chief obligations are transparency, openness and ease of access for third party requesting data from public authorities. For freedom of information, the data to which third parties have a right of access is, simply, information held by, or on behalf of, any public authority.[17] This, of course, does not apply to all information so held, FOIA provides, as mentioned above, exemptions, such as the one concerning 'personal data' as defined by reference to the Data Protection Act 1998.[18] Requests for access to such data need not be complied with. If they come from the data subject herself they must be handled according to the data protection regime as a 'subject access request'. Moreover, if a public authority receives such a subject access request from within the freedom of information regime it must, nevertheless, process that request as subject to data protection. Thus, it would seem that the statutes draw a clear line in the sand as between their respective competencies.

The *Collie* case demonstrates all too well, however, how the respective regimes cannot be kept entirely apart. There is, in fact, a potential clash of cultures between, on the one hand, a world where the default position is non-disclosure and another where the expectation is that access should be given. The tension at the interface between these two worlds will be heightened depending on where the expectations are set that public authorities will *facilitate* access to information that they hold. This distils into what is meant by the obligation both north and south of the border '…to provide advice and assistance to a person who proposes to make, or has made, a request for information to it.'[19]

This may be a reasonable compromise at first blush: if personal data can be adequately anonymised so as to take them out of the data protection regime then there is no reason why they should not then be made public. But this ruling is based on a number of underlying assumptions which, if allowed to become established precedents, would have deleterious and far-reaching consequences.

First, is it the case that mere perturbation of data of this kind is enough to meet the requirements of relative anonymity and non-identifiability? The SIC was content to assume that the risk of identification would be 'substantially removed' by these means. But this raises the question of what is required in law to ensure an *acceptable* level of anonymisation. There is, in fact, no clear legal ruling on the matter, although the UK Information Commissioner has issued guidance to the effect that it is '…incumbent on anyone processing data to take such technical and organisational measures as are necessary to ensure that data cannot be reconstituted to become personal data and to be prepared to justify any decision they make…'[20] This points to the problem of addressing the unknown risk that data may indeed be 'reconstituted' once in the hands of a third party because of the possibility of connecting the disclosed (anonymised) data with other data held by, or accessible to, that party. Data protection culture would have us err on the side of caution.

---

[1] This paper is based on an article published in the Edinburgh Law Review, Volume 10, Issue 1, January 2006, G Laurie and R Gertz, "When Worlds Collide: What are the obligations of the NHS at the interface between data protection and freedom of information regimes"

[2] <http://www.opsi.gov.uk/ACTS/acts2000/20000036.htm>

[3] <http://www.itspublicknowledge.info/legislation/act/foiactcontents.htm>

[4] <http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm>

[5] Decision of the Scottish Information Commissioner 021/2005*, Mr Michael Collie and the Common Services Agency for the Scottish Health Service*, 15 August 2005, available at: http://www.itspublicknowledge.info/

[6] 15. Duty to provide advice and assistance
(1) A Scottish public authority must, so far as it is reasonable to expect it to do so, provide advice and assistance to a person who proposes to make, or has made, a request for information to it.
(2) A Scottish public authority which, in relation to the provision of advice or assistance in any case, conforms with the code of practice issued under section 60 is, as respects that case, to be taken to comply with the duty imposed by subsection (1).

[7] For an overview in the healthcare context, see B Meredith, "Data protection and freedom of information" (2005) 330 *British Medical Journal* 490-91.

[8] [2003] EWCA Civ 1746

[9] Case 33/70, *SpA SACE v Ministry for Finance of the Italian Republic* [1970] ECR 1213, Case 41/74, *Van Duyn v Home Office* [1974] ECR 1337, Case 148/78 *Publicco Ministero v Ratti* [1079] ECR 1629

[10] Case 14/83, *von Colson and Kamann v Land Nordrhein-Westfalen* [1984] ECR 1891

[11] Case 79/83, *Harz v Deutsche Tradax* [1984] ECR 1921

[12] *von Colson*, op. cit.; *Harz*, op. cit.

[13] Decision of the Scottish Information Commissioner 066/2005, *Mr Peter MacMahon of The Scotsman and the Common Services Agency for the Scottish Health Service*; Decision of the Scottish Information Commissioner 065/2005, *Mr Camillo Fracassini and the Common Services Agency for the Scottish Health Service*

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

[15] For a useful discussion see W Lowrance, *Learning from Experience : Privacy and the Secondary Use of Data In Health Research*, (2002).

[16] See, for example, the Council of Europe's Recommendation on Regulations for Automated Medical Databanks (No. R(81)1) and the Council of Europe Recommendation on the Protection of Medical Data (1997, No. R(97)5).

[17] 2002 Act, s. 3(2).

[18] 2002 Act, s.38.
[19] 2002 Act, s.15(1). The equivalent provision in the 2000 Act is s.16.
[20] Information Commissioner's Office, *Legal Guidance*, 2000, p.14.

Bibliography

G Laurie and R Gertz, "When Worlds Collide: What are the obligations of the NHS at the interface between data protection and freedom of information regimes", (2006) *Edinburgh Law Review*, Volume 10, Issue 1

B Meredith, "Data protection and freedom of information" (2005) 330 *British Medical Journal* 490-91

W Lowrance, *Learning from Experience : Privacy and the Secondary Use of Data In Health Research*, (2002)

Scottish Cases

Decision of the Scottish Information Commissioner 021/2005*, Mr Michael Collie and the Common Services Agency for the Scottish Health Service*

Decision of the Scottish Information Commissioner 066/2005, *Mr Peter MacMahon of The Scotsman and the Common Services Agency for the Scottish Health Service*

Decision of the Scottish Information Commissioner 065/2005, *Mr Camillo Fracassini and the Common Services Agency for the Scottish Health Service*

UK Cases

Durant v Financial Services Authority [2003] EWCA Civ 1746

European Cases

Case 33/70, *SpA SACE v Ministry for Finance of the Italian Republic* [1970] ECR 1213

Case 41/74, *Van Duyn v Home Office* [1974] ECR 1337

Case 148/78 *Publicco Ministero v Ratti* [1079] ECR 1629

Case 14/83, *von Colson and Kamann v Land Nordrhein-Westfalen* [1984] ECR 1891

Case 79/83, *Harz v Deutsche Tradax* [1984] ECR 1921