

# SCRIPT-ed

*Volume 3, Issue 4, June 2006*

## **Squeezing Information out of the Information Commissioner: Mapping and measuring through online public registers**

*Philip Leith\**

### **Abstract**

*Access to public registers has to date been primarily through physical observation of the printed record, thus allowing only the most basic searching and recording of that information. This is clearly changing with, for example, property sales information being commodified and made available over the internet, and a more open attitude to the re-use of government data. Is this 'open data' path the one that all registration agencies that handle publicly accessible records should follow? Or are there limitations – self imposed perhaps – that the agencies should rely upon to constrain the use of such data for any number of reasons? How far should this access be allowed – an online version of the printed register, or should something more powerful be offered to the public?*

*In this article I look to one register which is particularly relevant to this discussion – principally because the register is held by the organisation with a responsibility for making public information accessible to the UK public – the UK Information Commissioner's Office (ICO).*

*I will argue that an extended right of access to public registers should be enabled which allows processing and analysis of the data contained within the register. In terms of the ICO, this 'right to process public information' is essential that we may better understand the privacy and data protection debate.*

DOI: 10.2966/scrip.030406.389

© Philip Leith 2006. This work is licensed through [SCRIPT-ed Open Licence \(SOL\)](#).

---

\* Professor Philip Leith, School of Law, Queen's University of Belfast; [p.leith@qub.ac.uk](mailto:p.leith@qub.ac.uk).

## **1. Introduction**

There are strong public interest reasons for enabling online access to the various types of registers that deal with public information. Indeed, we see a growing interest in making some registers more accessible to the public. However, it is not quite clear what kind of online access should be enabled to these registers: should access simply model the classical ‘births, deaths and marriages’ form (that is, access by printed extract) or should holders of public registers be expected to go further by integrating more advanced analytical facilities into these registers, or at least allowing these facilities?

In this article, I focus on access to the public register of notifications held by the UK Information Commissioner’s Office (ICO) and argue that it could much better help us understand the developing field of the right to privacy. This article assumes, rather than outlining in detail, the thesis that we do not understand how the new rights to informational privacy are working in practice. However, I give some indication as to why we may want to research these rights, and, in particular, how the register of notifications may help in that research.

Despite the availability of the notification register as a potential research tool, it is becoming clear that the ICO has shown little interest in developing access methods, despite being allowed to do so through the Data Protection Act 1998. In this article, I outline the process of notification, my attempts (via Freedom of Information rights) to get usable research information from the online system and give suggestions as to what an ICO with a positive approach to developing understanding of the data processing environment might consider adding to a re-engineered online public register. A re-engineered register would provide a significant research tool at minimal cost and be appropriate to all European Union countries – all of which are currently required to have registers of notifications.

Access to this corpus of information is particularly relevant in a period when we are trying to map and measure the use and processing of personal and sensitive personal data by the users of that data: We have presently, I suggest, too few ways to do this mapping and measuring to ignore the mass of analysable information held on the public register.

## **2. Public Registers and Notification**

The Data Protection Public Register is an online register of those data controllers who have registered under the 1998 Data Protection Act. S19 of the Act requires that a register will be maintained of those who register and that under S19(6):

*The Commissioner –*

*(a) shall provide facilities for making the information contained in the entries in the register available for inspection (in visible and legible form) by members of the public at all reasonable hours and free of charge ...*

The register was a requirement under the older 1984 Act (S4)<sup>1</sup> and became part of the data processing harmonisation process throughout Europe with Art. 18 of the Data Processing Directive<sup>2</sup> requiring all processors of personal data in Europe to introduce a 'notification' scheme. In the UK, notification is clearly a source of considerable income<sup>3</sup> to the Information Commissioner's Office (ICO) – some £9 million per annum – which allows the provision of a free service to the public in both data processing and freedom of information matters.

In total the number of entries on the register was 259,296 on March 2005, but even a cursory analysis of the public register demonstrates that many data controllers are not represented. For example, perhaps only 30% of solicitors in the Yellow pages in Northern Ireland were to be found through a search on the public register.<sup>4</sup> The ICO appears to be developing a robust attitude to maximising this income through, for example, prosecution of non-notifiers: Eight such prosecutions are noted in the 2005 Annual Report, most of whom were solicitors, with the ICO taking the view that non-notification was 'serious'.<sup>5</sup> There have been complaints about the need for a notification process – particularly since there are other ways that some data controllers might ensure correct processing of their stored information. For example, the Department of Constitutional Affairs (DCA) has suggested: 'Increasingly, notification is seen as burden for data controllers which serves no, or very little, data protection purpose'.<sup>6</sup>

The EU in response to this complaint by the UK and other countries has pointed out that no country is obliged to have total registration and that there are other methods of resolving this issue,<sup>7</sup> because Art 18 of the Directive provides a mechanism where simplification or exemption is allowed. For example, 'for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects ...' Such exemptions are currently

---

<sup>1</sup> Section 5 of The Data Protection Act 1984 made it an offence to process personal data without registration. The Information Commissioner was at that time entitled, the 'Registrar'.

<sup>2</sup> Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

<sup>3</sup> See, The Information Commissioner's Office, *Annual Report 2004-2005*, @: [http://www.ico.gov.uk/upload/documents/library/corporate/detailed\\_specialist\\_guides/Annual\\_Report\\_2005.pdf](http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/Annual_Report_2005.pdf) (Outlining the fee/budget regime).

<sup>4</sup> December 2005. The Northern Ireland office of the ICO, though, appears to have decided to take a less aggressive approach at present.

<sup>5</sup> 'I am pleased that the magistrates' court has recognised the seriousness of a failure to notify. Complying with the Data Protection Act ensures that individuals' personal information is secure, accurate, up-to-date and is processed fairly. This prosecution should remind solicitors and other organisations of their responsibilities under the Act'. ICO Press notice, 1<sup>st</sup> March 2005.

<sup>6</sup> Department of Constitutional Affairs, "Proposals for Amendment made by Austria, Finland, Sweden and the United Kingdom Explanatory Note", (2002) @: <http://www.dca.gov.uk/ccpd/dpdamend.htm>

<sup>7</sup> 'The European Commission shares to a large extent the criticism expressed by data controllers during the review concerning the divergent content of notification obligations placed on data controllers. The Commission recommends a wider use of the exceptions and in particular of the possibility foreseen in Article 18(2) of the Directive, that is the appointment of a data protection officer which creates an exemption from notification requirements.' Report from the Commission – First report on the implementation of the Data Protection Directive (95/46/EC). COM/2003/0265 final.

to be found in the Danish implementation of the Directive<sup>8</sup> in, for example, Section 49(7) where the exemption is given to lawyers and accountants if ‘the processing is carried ... in the course of business, to the extent that only data concerning their clients are processed’.<sup>9</sup> Thus the processing that most Danish solicitors would carry out would be expected to be covered by this exemption. Other countries too, have taken this route. For example Italy, in March 2004, changed its notification system to incorporate more exemptions.<sup>10</sup> However, there currently appear to be no plans to change the UK system: Perhaps the potential loss of income appears to have muted DCA criticism of the notification process.

The current situation is that there is a standard fee for every notification: One may hold 10 records or one may hold 100 million records – one pays the same notification fee.<sup>11</sup> This fee also covers any number of different branches or addresses where the data is processed. This does show some lack of imagination: It would be perfectly possible to imagine a situation where the fee represented the philosophy and goals of data protection. For example, a higher fee could be associated with a higher number of records; more sensitive information could be charged more highly; the number of locations utilizing data might figure into the costing algorithm; and situations where data is interlinked with other data might also receive a higher fee level. Those who are under an obligation (fiduciary, perhaps) to control data would be exempted. This does not happen and we thus have a situation where many (solicitors included) do not view themselves as ‘data controllers’ in any meaningful way and do not therefore notify.

Whatever the fees applied for notification, the coverage which arises from the current situation where almost all commercial users of data are expected to register should lead to an enormously useful collection of data describing the usages of data in the UK, as well as throughout Europe.<sup>12</sup> Access to such a tool could be of immense utility in the mapping and measuring of privacy in Europe – the silver lining on the cloud of near universal notification would be an abundance of analysable data on how the new rights to informational privacy actually work out in practice. Unfortunately, though, these benefits are not available to the research community.

### **3. The Need for Research in Data Protection issues**

The register is a source of potentially highly useful information about the developing world of information processing and, because one of the functions of the ICO is to promote understanding of data usage,<sup>13</sup> one might imagine that such a corpus of data

---

<sup>8</sup> The Act on Processing of Personal Data (Act No. 429 of 31 May 2000).

<sup>9</sup> An English version of the Act is available at [www.datatilsynet.dk/eng/iindex.html](http://www.datatilsynet.dk/eng/iindex.html)

<sup>10</sup> The Annual Report of the Art 29 Working Group details these national changes in notification. See *Eighth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries – covering the year 2004*, @: [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/annual\\_reports\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/annual_reports_en.htm)

<sup>11</sup> At time of writing, £35.

<sup>12</sup> The requirement for a register for all member states is found in the Data Processing Directive, *supra*.

<sup>13</sup> “See Information Commissioner’s Office, “What we do”, @: [http://www.ico.gov.uk/about\\_us/who\\_we\\_are/what\\_we\\_do.aspx](http://www.ico.gov.uk/about_us/who_we_are/what_we_do.aspx) (“We influence thinking on privacy and access issues.”)

would be promoted as an analytical tool. This does not, however, appear to be the view of the ICO, which gives little attention to the utility of this register. For example, the ICO does not provide information pertaining to access statistics by the public (even though these must be collected by default via their web site). In the 2005 Annual Track report,<sup>14</sup> which carried out a survey on the functions of and knowledge about the ICO and its legislative functions, the only mention of the register was in response to question concerning the role of the ICO: 2% of the people surveyed noted that one role of the ICO was to register data controllers under the data protection act.

This attitude is certainly surprising: The ICO funds a number of projects that attempt to define the problems of privacy in a data processing environment and on the meaning of such elements as ‘personal data’ and ‘privacy’. Why not investigate with the information that they have to hand?

A sceptic might suggest that an agency that sees itself as building up awareness (‘education’) of data processing as a problem and that argues that data protection legislation is effective, may not be quite so keen on having the negative conclusions that can be drawn from the public register made quite so public. As an example of these negative conclusions, for teaching purposes I will usually cover the goals of the DP Act and something of its history. Having lulled the students into a sense of comfort where they clearly feel that ‘something is being done’ I then point to the entry from the Countryside Alliance on the register.<sup>15</sup> The Countryside Alliance is a pro-hunting organisation which fought for the right to continue hunting and opposed the anti-hunting ‘hunt saboteurs’. Why would an organisation dedicated to the pursuit of the fox be so interested in information about its opponents, which includes, for example:

- Family, Lifestyle and Social Circumstances
- Financial Details
- Racial or Ethnic Origin
- Political Opinions
- Religious or Other Beliefs of A Similar Nature
- Trade Union Membership
- Physical or Mental Health or Condition
- Sexual Life

The spread of information collected which their entry covers is quite striking, given that these are supposedly examples of *sensitive personal data*, a class of information which is treated in a more rigorous way under the 1998 Act. And how, I ask the students, can the Countryside Alliance get away with such intrusion if the Act was effective in achieving its goals of ‘fair processing’ of data? What can ‘fair’ actually

---

<sup>14</sup> SMSR Ltd., *Report on Information Commissioner’s Office Annual Track 2005: Individuals*, (2005) @:  
[http://www.ico.gov.uk/upload/documents/library/corporate/research\\_and\\_reports/dp\\_annual\\_track\\_2005\\_-\\_individual\\_report.pdf](http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/dp_annual_track_2005_-_individual_report.pdf)

<sup>15</sup> The Countryside Alliance was runner up in the Privacy International “Most Invasive Company” section of the 2002 Big Brother awards. See <http://www.privacyinternational.org/bigbrother/uk2002/>

mean? Further, how can the register entry of *dunnhumby Ltd* be so sparse and uninformative in comparison to the heights of the company's data processing ambitions, which ambitions have been described elsewhere:

*'It contains details of every consumer in the UK at their home address across a range of demographic, socio-economic and lifestyle characteristics,' says the marketing blurb. ... It has 'added intelligent profiling and targeting' to its data through a software system called Zodiac. This profiling can rank your enthusiasm for promotions, your brand loyalty, whether you are a 'creature of habit' and when you prefer to shop. As the blurb puts it: 'The list is endless if you know what you are looking for.'*<sup>16</sup>

Seeing the contents of the public register for themselves certainly begins to make the student understand that control of data processing in the real world is not quite as comforting as suggested by its proponents, whether academic or organisational.<sup>17</sup> And the core organisations do often suggest a comforting success story. For example the Commission's 'First Report on the transposition of the Data Protection Directive' exudes a certain smugness:

*As provided for in Recital 10, the approximation of the national laws pursued by the Directive must seek to ensure a high level of protection in the Community. The Commission believes that this has been achieved. Indeed the Directive itself sets out some of the highest standards of data protection in the world.*<sup>18</sup>

Commercial concerns rarely wish to detail just what they are doing. This seems as true in data processing as it is in applying for patents – even though there is a requirement for full disclosure, patent applicants will do their utmost to hide from their competition the strategic purpose of the application.<sup>19</sup> My reading of the register as it currently stands suggests that the data controller frequently uses disclosure-limiting techniques to pull the wool over the eyes of the data subject. The current design of the register makes this technique easy.

Overall, we have in the public register what could be a powerful resource to tell the public (including the ICO) what is actually happening in data protection terms, and, perhaps through analysis, build legislative strategies to improve this context. Unfortunately, for unstated reasons, there appears to be little desire by the ICO to encourage utilisation of this tool for such analysis. We are left with a public register that currently allows only the most basic of access via:

---

<sup>16</sup> H Tomlinson and R Evans, "Tesco stocks up on inside knowledge of shoppers' lives", (20 Sept. 2005) *The Guardian*.

<sup>17</sup> P Leith, "The Socio-legal Context of Privacy", *International Journal of Law in Context* June 2006, pp 105-136.

<sup>18</sup> That said, they do tend to set aside negative evidence: 'However, the results of the online survey suggest that the perception of citizens at this regard is different. This paradox requires further reflection. A preliminary analysis would suggest that at least part of the problem is attributable to an incomplete application of the rules.' Report from the Commission - First report on the implementation of the Data Protection Directive (95/46/EC), COM/2003/0265 Final.

<sup>19</sup> Any of the easily accessible 'manager's guides to patenting' will discuss this tactic, e.g. JH Knight, *Patent Strategy: For Researchers and Research Managers*, (2001).

- Registration Number
- Name
- Address Postcode
- Organisation sub-division

Given that greater data is already collected, verified and stored, such limited processing is dispiriting. Below, I will suggest that the current technical organisation of the data should easily allow much more powerful processing techniques, and also that by better data collection from data controllers, the system could potentially offer an even greater insight into what is happening to personal data.

#### **4. Squeezing Information from the Commissioner**

My early informal requests<sup>20</sup> to the ICO to utilise the public register for research were rebuffed when I was told that the information was not amenable to such usage. This appeared to me as technically illogical: If the data was held in a database then it should be accessible through the query language upon which the system operates. My request was really a fishing expedition, as there has been so little statistical information produced on who was doing what with data that the first steps in looking at this data would have to be general context setting. The most sensitive kind of data held by data controllers is clearly the data listed under the category of ‘sensitive personal data’ under the act, so I constructed a question to the ICO under the Freedom of Information (FoI) regime.<sup>21</sup> The specifically chosen question is not too important for this article, but does indicate the need for careful consideration in any FoI request – the question was posed in the language clearly used in the organisation of the register itself:

*For each of the ‘Other Purposes’ listed from pages 12 to 14 of the Information Commissioner’s Notification Handbook, please list the total numbers of Notifications which specify one or more of the ‘Sensitive Personal Data’ classes (C206 to C213).<sup>22</sup>*

The ‘other purposes’ are standard descriptions that are used in the register entries and detailed in the Notification Handbook.<sup>23</sup> They cover a variety of business tasks – from accounting and auditing, journalism and media, to private investigation, and to trading and sharing in personal information. These ‘Other Purposes’ thus offer a standardised classification of processing type that, when linked with numbers of notifications, would provide some broad context for understanding who was collecting sensitive personal data. The classes of data C206 to C213 are also laid out

---

<sup>20</sup> “Ideally I would like to be able to do a free-text search of the register, but obviously this is not possible with the search screen which is available via the ICO web site. Is there some way in which such a search can be carried out and, if so, it is possible for me to have access to this?” Letter, March 2005. Author to ICO (NI).

<sup>21</sup> The ICO is itself, of course, a public body and thus covered by the FoI Act.

<sup>22</sup> Letter, 1<sup>st</sup> June 2005. Author to ICO.

<sup>23</sup> Information Commissioner’s Office, *Notification Handbook: A complete guide to notification*, @: [http://www.ico.gov.uk/upload/documents/library/data\\_protection/forms/notification\\_handbook\\_-\\_complete\\_guide.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/forms/notification_handbook_-_complete_guide.pdf)

in the Notification Handbook and deal with racial or ethnic origin (C206), and political opinions (C207), among others. The particular detail of this request is, of course, not relevant in discussion of access, but it is included to demonstrate that knowledge of the underlying structure of how the data is stored in a database is important in extracting meaning from the contents.<sup>24</sup> My FoI request was refused:

*[D]ue to the limited search criteria available, we are unable to identify the total number of notifications under the Data Protection Act 1998 which have specified one or more of the 'sensitive personal data' classes (C206–C213) with the purposes.*<sup>25</sup>

This appeared to me to be the non-technical person's attempt at closure. Clearly if the data was being held in a relational database<sup>26</sup> and was being accessed in some manner in order to serve the web browser requests, there had to be a means of specifying 'search criteria' which could have handled my request. I therefore made a further request under FoI for details on the system that was used to handle the public online register. The information which was returned supported my view:

*The language used is a mixture of HTML and ASP pages which use Microsoft SQL and Microsoft Stored Procedures to access the database.*<sup>27</sup>

HTML is the 'mark up' language which formats the information on screen, ASP is the server processing element which prepares the HTML information to be sent to the user's browser, and Microsoft Stored Procedures is a technique for compressing database queries to speed up processing. The most important element of the register is that it uses a powerful query language, SQL, which is, in fact, the *de facto* standard for query languages. A query language is a formalised language that allows access to a database through Boolean search techniques, for example:

*SELECT ALL WHERE price > 30 AND type = "used"*

Lawyers who use legal databases in more than just the most basic way should be reasonably expert in understanding such Boolean access methods.<sup>28</sup> Microsoft advertises their version of SQL as a powerful way of extracting information from a database:

*The SQL Server 2005 ... combines the best in analysis, reporting, integration, and notification. This enables your team to build and deploy cost-effective BI solutions with which they can drive data into every corner of your business through scorecards, dashboards,*

---

<sup>24</sup> Basic texts describing management information systems (MIS) outline such factors, e.g. GL Sanders, *Data Modeling: Contemporary Issues in Information Systems*, (1994).

<sup>25</sup> Letter 22<sup>nd</sup> June 2005. ICO to author.

<sup>26</sup> This means that the data is held as a series of individual records, each with a similar format.

<sup>27</sup> Letter 15<sup>th</sup> July 2005. ICO to author.

<sup>28</sup> See P Leith and A Hoey, *The Computerised Lawyer: A Guide to the Use of Computers in the Legal Profession* 2nd edn(1998). (For an outline of searching and storing information in a legal context).



*Web services, and mobile devices. ... Whether you are a developer, database administrator, information worker, or decision maker, SQL Server 2005 provides innovative solutions that help you gain more value from your data.*<sup>29</sup>

This appears to suggest that the ICO response is incorrect and that the system is perfectly capable of producing search results via the SQL query language for anyone who is knowledgeable in SQL, and in the structure of the underlying database. I raised this with the ICO in a further request but this, too, was declined on two grounds: (i) ‘not holding the information’ and (ii) cost. I look at the first argument below. The cost defence was that the information system suppliers would charge in excess of £1,500 to carry out the requested search.

I requested a decision notice, which provides the ICO’s final assessment as to whether or not a public authority has complied with the Act<sup>30</sup> with regard to specific complaints.<sup>31</sup> The ICO would, under this request, have to provide a decision notice relating to their own compliance; a situation which is not specifically covered by the 1998 Act.

I pointed out that my request was related to the academic study of the Information Commissioner’s Office and the operation of the Data Protection Act 1998 with specific regard to the process of registration and sensitive personal data. The purposes of the register have been, since the need for a DP act was first considered, wider than the Information Commissioner currently appeared to believe. For example, the Lindop Report when discussing functions of registration, noted:

*First, it could go a long way towards meeting the second of the statutory objectives set out in paragraph 34 of the White Paper, namely that ‘the existence and purpose of [computerised personal] information systems should ... be publicly known, as well as the categories of data which they handle, what they do with data and which interests have access to data’. .... The mere existence of a publicly accessible register, even if restricted to particularly sensitive or significant classes of application, could greatly alleviate such misgivings; and even though few ordinary data subjects might actually trouble to consult it, it could be consulted on their behalf by public interest organisations and by the media.*<sup>32</sup>

The Data Protection Act does not explicitly provide for a description of the function of the register, but it is clear from the legislative history that analysis by interested parties of the data protection system and the use of information systems by data controllers has been a major reason for its creation and therefore should be a considerable factor in the design and openness of the registration system by the ICO.

---

<sup>29</sup> Microsoft.com, “What is SQL Server 2005?”, @: <http://www.microsoft.com/sql/prodinfo/overview/what-is-sql-server.mspx>

<sup>30</sup> Freedom of Information Act 2000, s 50. This also covers compliance with the Environmental Information Regulations 2004.

<sup>31</sup> Details and past decision notices are available the ICO web site @: <http://www.ico.gov.uk>

<sup>32</sup> Home Office, Report of the Committee on Data Protection, (1978) Cmnd. 7341, HMSO, p169. Emphasis added.

‘Sensitive Personal Data’ is one of the core concepts of data protection law, and it is important in the academic study of the system to determine how widely and for what purposes this data is being stored. A publicly available register that only allows access to individual registrations clearly does not allow the consultation and analysis required to properly assess the purposes of information systems, ‘the categories of data which they handle, what they do with data and which interests have access to data’. A register which allows only access to individual registrations and which is seldom accessed by the public, for whatever reason, is open to the criticism of being primarily a means of revenue collection.

After some delay, the information which I had originally requested was provided:

*I am now pleased to be able to tell you that we have added a new reporting tool to our system which makes it easier for us to extract the type of information you requested.*<sup>33</sup>

With the provision of the requested information, the ICO felt that there was no longer any requirement to proceed to issuing a decision notice. This, of course, does raise the question of whether the ICO will be utilising its interest in new reporting tools to further extend the facilities available on the online public register: There are no public indications that these improvements are being planned and I return to this question below.

Cost is certainly an important basis for exemption, given that the FoI Act was not designed to bankrupt public authorities. But if FoI is to operate properly, then it requires that when setting up information systems, that the information will be physically and economically structured to allow the request. A situation where an external agency (presumably a computer consultancy) is contracted to carry out a set of tasks for a given contracted price may lead (as here) to a situation where the contractor becomes the deciding factor in whether information is to be made available after a request. If the contractor has too much work on and does not want to undertake the extra non-contracted task, then the cost exemption will come into effect. If the contractor is short of work and happy to undertake smaller tasks, then the same request may be within cost limits. The error thus lies in either being in a position where one is reliant upon external agents, or, as I would suggest, setting up a system that does not facilitate cheap and cheerful handling of FoI requests, particularly when as in the case of the register, it could be done online without manual intervention.

### **5. ‘Not holding the Information’**

The refusal to provide the requested information had been on the basis of cost (discussed above) but also of ‘not holding this information’:

*Our first ground for declining to supply the information requested is that we do not hold this information. We neither can nor do routinely extract this information from our system. We certainly hold the raw data which would form the basis of the analysis you request, indeed this information is available on the public register*

---

<sup>33</sup> 1<sup>st</sup> March 2006. ICO to author.

*of data controllers, but we do not hold results of the analysis because it is an analysis we never perform ourselves.*<sup>34</sup>

My view was that this argument was perturbing: It provides a mechanism whereby any public authority can resort to technical replies to FoI requests relating to digital data that suggest that accessing the information ‘is too difficult’ or ‘can’t be done’. It is of course well known that technical people will simply provide incorrect advice on what is technically feasible for a variety of reasons, frequently because they can’t be bothered but often because they prefer a different approach to be taken.<sup>35</sup> It seems to me that if the data is held in an SQL accessible format, then it is irrelevant how that data is processed to appear on the public web pages, i.e. ‘with a limited number of search criteria’. Reporting facilities in the Microsoft SQL system will still be available to the technical staff and one might expect that a reasonably able SQL-literate programmer could extract the information with as much or as little effort as that required by other public agencies to carry out FoI searches.

The main thrust of the ICO response was that there was a legal basis for non-supply of the information which I requested – that is, that there is a distinction between ‘raw data’ and ‘information’. But this does not appear to be true. The FoI Act detailing the provision of information makes no such distinction between ‘raw data’ and ‘information’:

*1. - (1) Any person making a request for information to a public authority is entitled -  
(a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and  
(b) if that is the case, to have that information communicated to him.*

In addition, the definition in S84 states that information ‘means information recorded in any form’. The Act refers to the general ‘holding of information’ and does not attempt to fragment it into accessible information and non-accessible data. As to the register, the legal basis for the provision of information arises in Section 19 of the DPA 1998:

*19. (6) The Commissioner -  
(a) shall provide facilities for making the information contained in the entries in the register available for inspection (in visible and legible form) by members of the public at all reasonable hours and free of charge*

Thus, neither is there a distinction drawn in the data protection legislation between ‘data’ and ‘information’ in S19 that deals with access to the contents of the register. The ICO took a highly limited view of their role by seeming to suggest that the register is ‘raw data’, rather than ‘information’. This cannot be the case. The

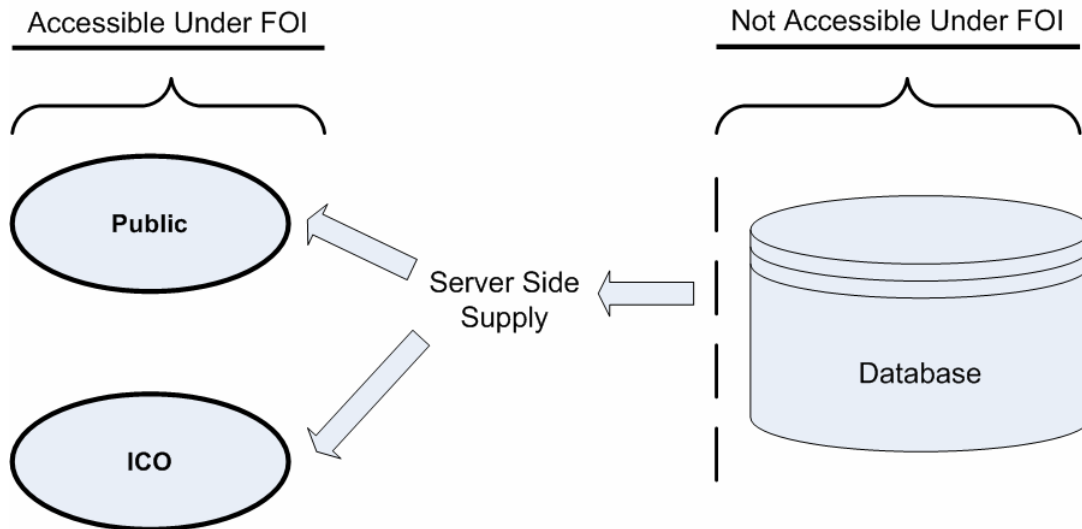
---

<sup>34</sup> Letter, 24<sup>th</sup> August 2005. ICO to author. Emphasis added.

<sup>35</sup> Computer consultants, for example, could find a technical reason to support purchase of a system in which they have an economic interest – often consultants operate in fields where the technology is not understood by the recipients of the consultancy service.

information which is presented on the ICO web site is similarly raw data that the ICO has produced SQL ‘queries’ to extract. The ICO took the decision in implementing the system to provide the public with the narrowest amount of information that complies with Section 19 DPA – that is, access to individual entries rather than ‘facilities for making the information contained in the entries in the register available ...’. Such narrowly based information does not allow the public (or those acting in the public interest) full access to the information which is contained in the register.

The view of the ICO is based on a two-part model of data:



Of course, a FoI request could be made for the contents of the entire underlying database, but the ICO expressly precludes this under its Publication Scheme. ‘[Th]e system only allows for individual records to be accessed and downloaded. It is not possible to download the entire Register.’<sup>36</sup> This is no doubt based upon the supposition that raw data is not ‘information’ and is thus to be treated in a different manner. My original request could have been answered with a copy of the database on disk<sup>37</sup> but under this conception of ‘held information’ it was not.

What are we to make of this approach? It certainly does not fit any definition of accessibility that a computer scientist would embrace. Anyone with technical understanding will realise that the database is the central part of the information system and that the supply side is simply a tool to represent that underlying database in a specified manner. If the ICO holds to the view that there is a distinction between raw data and information, it leads to a loophole in FoI rights through which many carts and horses can be led: Any public authority that wishes to hide away sensitive information simply needs to ensure that any reporting tools (SQL queries, for example) do not extract information in a sensitive form. If it exists in the database then so long as the public authority does not itself combine the raw elements of the data, it is exempted from FoI access. My request for a decision notice had

<sup>36</sup> The publication scheme is available on the ICO website at [http://www.ico.gov.uk/about\\_us/who\\_we\\_are/corporate\\_information/our\\_publication\\_scheme.aspx](http://www.ico.gov.uk/about_us/who_we_are/corporate_information/our_publication_scheme.aspx)

<sup>37</sup> The database software used by the ICO would be irrelevant – they would only need to output in a field and record delimited format and any other database program would be enabled to utilise this.

emphasised this, but the ICO in providing the originally requested information appeared to feel that this point no longer required discussion.<sup>38</sup>

Might we tend towards the conclusion that at the policy level the ICO appears to have barely considered the legal distinction between data and information? There has certainly been sufficient common law precedent where raw data has been considered accessible by FoI requests – the US legislation, for example, excludes only geological information and data which concern wells.<sup>39</sup> The definition of ‘records’ was discussed by the US Supreme Court in *Forsham v Harris*,<sup>40</sup> when an attempt was made to access the underlying data used to produce medical research publications which had been government funded (access was disallowed due to not being a government agency) and a wide-ranging definition was accepted based upon the US ‘Record Disposal Act’:

‘records’ includes all books, papers, maps, photographs, *machine readable materials*, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business. . . .<sup>41</sup>

A similar attempt to utilise UK legislation is not so simple – the Public Records Act 1958<sup>42</sup> provides a definition of a ‘public record’ but only in terms of where it was produced or held, not its form. Coppel points to the wide-ranging definition used in New Zealand (which has a similar base unit to both the UK and US of ‘information’ in its legislation) where the Court of Appeal stated: ‘Information is not defined in the Act. From this it may be inferred that the draftsman was prepared to adopt the ordinary dictionary meaning of that word’.<sup>43</sup> Unfortunately in the digital age we find that there are few ‘ordinary’ dictionary meanings of a term that is used both colloquially and as a theoretical term.<sup>44</sup> *Durant v FSA*<sup>45</sup> provided definitional aid to the Data Protection Act with respect to what is meant by a ‘filing system’, but does not help us here, since ‘information’ and ‘data’ were used interchangeably in the judgment of Auld LJ, which does tend towards a legal ‘commonsensical’ view that data and information are transposable terms.

---

<sup>38</sup> The ICO had recently set up a system to rebuff requests for notification that it deemed ‘academic’. There are indications that not all in the ICO believe this has a sound legal basis. The aim of the new approach is “to not take up, or continue with, any FoI or EIR case where no useful purpose would be served if we were to proceed with an adverse Decision Notice”. This, of course, leaves the ICO as arbiter of ‘useful purpose’. See Information Commissioner’s Office, “A Robust Approach to FoI Complaint Cases”, (2006) ICO Website.

<sup>39</sup> Commentators consistently point to this exemption being ‘rarely used’. See *e.g.* US Dept. of Health and Human Services – Health Resources and Services Administration, Freedom of Information Act – Exemptions”, @: <http://www.hrsa.gov/foia/foiaexemp.htm>

<sup>40</sup> *Forsham v. Harris*, 445 U.S. 169 (1980).

<sup>41</sup> 44 U.S.C § 3301 Disposal of Records. Emphasis added.

<sup>42</sup> Section 84 of the Freedom of Information Act 2000 defines a public record as “a public record within the meaning of the Public Records Act 1958”.

<sup>43</sup> P Coppel, *Information Rights*, (2004), para 7–005.

<sup>44</sup> *E.g.* Claude Shannon’s information theory.

<sup>45</sup> *Durant v Financial Services Authority* [2003] EWCA Civ 1746 (8 December 2003).

In Sweden, the basic unit of access in its FoI regime has been the ‘public document’, yet this too has been broadened considerably to other formats. In 1987, Petren was describing how:

*In recent years new techniques have made it necessary to enlarge the concept of a public document. Nowadays it also includes all kinds of materials in which information is stored, if it can be made accessible by some technical device; records and tapes are examples. Computers raise special problems. Computerised material is treated as documents and is subject to the same rules as traditional documents ...*<sup>46</sup>

Given that there is no legislative basis for the ICO’s distinction and that other jurisdictions have taken a broad interpretation of what information is, the ICO simply seems to be wrong in law. Its view is not only wrong in law and (I would argue) against the spirit of FoI legislation, but also against the spirit of the Re-Use Directive,<sup>47</sup> and the EU’s encouragement towards producing information products from public sector information. The goal of the Re-Use Directive is to encourage the production of digital information commodities that arise from information produced by European governments, which is reckoned to have a value of €433 billion and employ 4 million in Europe:

*Indeed, public sector information also has a considerable economic potential. The new information society technologies have led to unprecedented possibilities to combine data taken from different sources and create added value products and services. Public sector information is an essential basis for many digital information products and could become an important raw material for new services and in particular for the wireless.*<sup>48</sup>

There would be, I imagine, commercial interest in information products based upon European notification registers which helped analyse the European data industry – exactly the information products that the European Commission is so keen to promote.<sup>49</sup>

---

<sup>46</sup> G Petren, “Access to Government-held information in Sweden”, in NS Marsh (Ed.), *Public Access to Government-held Information: a comparative symposium*, (1987), at 40-41.

<sup>47</sup> Directive 2003/98/EC of 17 November 2003 on the re-use of public sector information. Implemented in the UK by The Re-use of Public Sector Information Regulations 2005 No. 1515.

<sup>48</sup> Proposal for a Directive of the European Parliament And of the Council on the re-use and commercial exploitation of public sector documents, COM(2002) 207 final.

<sup>49</sup> It is clear that there are copyright issues relevant to the contents of public registers. However, it appears likely – given both the recent moves to ease Crown Copyright and the impulse of the Re-Use Directive – that Crown Copyright in such register information will be treated in a non-constraining manner. See, for example, the Office for Public Sector Information’s strategic perspective (e.g. <http://www.opsi.gov.uk/iar/index.htm>) and its Advisory Panel.

## **6. The Public Register of Notifications as a Research Tool**

The ICO does not appear to be opposed to research,<sup>50</sup> but does appear to wish to set the terms of that research. The research the ICO funds is commissioned<sup>51</sup> rather than put out to open competition, and therefore may suffer from the underlying criticism that the ICO is setting the research questions and thus biasing the results towards those that it wishes to find. ‘Who paid for this research?’ is one of the first questions that a critical reading of any research must be asked in order to set the findings in context. This is not necessarily to say that the quality of the research funded by the ICO is problematical, but it is to say that researchers who were prepared to set different research questions may have arrived at different results. Some organisations, of course, expect favourable results to be returned, but there is no evidence of this in the ICO’s research strategy despite there being a high percentage of projects funded from commercial researchers rather than from the academic community.

It is in this light that full access to the online public register should be viewed. Full access potentially provides admission to foundational data (or, if you like, information) that is usable by all researchers, no matter what philosophical approach they take to data protection law. The data – as was frequently expressed by a colleague in statistics – should be ‘allowed to speak for itself’.

The ICO’s own research is biased towards use of the survey technique,<sup>52</sup> which is only one of the four basic legal analytical techniques – judgment/legislative analysis, opinion surveys, in-depth interviews and data collection/analysis – and is perhaps the least effective. In one project I undertook, which involved a European transnational survey as well as in depth interviews, I certainly found considerable weakness in the use of surveys in comparison to interviews.<sup>53</sup> It may be that survey techniques also produce less insightful results than data collection/analysis. Even if data analysis is not a strikingly more fruitful method of assessing the developments in privacy than surveys, from the point of view of widening the ICO’s own commissioned research findings such a technique using the contents of the notification register must surely provide some further useful information.

But there are problems with the register as it currently exists – particularly in that it has been constructed without proper consideration of how it might be used to understand the data processing environment. It follows the birth, death, and marriages

---

<sup>50</sup> See ‘R Thomas, “Scholarship and the Freedom of Information Act”, (presentation 11 Feb. 2006). @: [http://www.ico.gov.uk/upload/documents/library/corporate/research\\_and\\_reports/scholarship\\_foi\\_1\\_year\\_on\\_rjt\\_110206.pdf](http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/scholarship_foi_1_year_on_rjt_110206.pdf)

<sup>51</sup> Management or research is dealt with in , “Information Commissioner’s Office Corporate Governance and Management Structure”, 16 May 2005 @: [http://www.ico.gov.uk/upload/documents/library/corporate/detailed\\_specialist\\_guides/corporate\\_governance\\_and\\_management\\_structure.pdf](http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/corporate_governance_and_management_structure.pdf)

<sup>52</sup> I include the use of focus groups within this kind of survey methodology. As an example of how the ICO has used this, see Information Commissioner’s Office, “Public Attitudes To The Deployment Of Surveillance Techniques In Public Places Qualitative Research Report” (2004). Currently unavailable, to be restored to the ICO website.

<sup>53</sup> Discussed in P Leith, *Harmonisation of Intellectual Property in Europe: a case study of patent procedure*, (1998) at Appendix 1.

model of being recorded but not usually web-accessible<sup>54</sup> rather than anything more illuminating. It need not have been so designed, given the philosophical aims of *Lindop et. al.* since the Act does not put detailed limits on what may be required for notification, simply stating ‘descriptions’ are required: Quite the contrary since the legislation gives the ICO a considerable flexibility in deciding what the register should contain:

16. - (1) In this Part "the registrable particulars", in relation to a data controller, means-

...

(c) a description of the personal data being or to be processed by or on behalf of the data controller and of the category or categories of data subject to which they relate,

(d) a description of the purpose or purposes for which the data are being or are to be processed,

(e) a description of any recipient or recipients to whom the data controller intends or may wish to disclose the data,

And under the notification regulations<sup>55</sup> it is up to the ICO to decide just what is required for these descriptions:

4. - (1) Subject to regulations 5 and 6 below, the Commissioner shall determine the form in which the registrable particulars (within the meaning of section 16(1) of the Act) and the description mentioned in section 18(2)(b) of the Act are to be specified, including in particular the detail required for the purposes of that description and section 16(1)(c), (d), (e) and (f) of the Act.

And further, having decided what to put into the register, the ICO is also enabled by the DP Act to decide how the public can access it:

19. (6) The Commissioner -...

(b) may provide such other facilities for making the information contained in those entries available to the public free of charge as he considers appropriate.

Put together, this legislative package would allow the ICO to produce a register that was indeed a powerful analytical tool to aid analysis by researchers of the data processing world. Unfortunately, the ICO has chosen not to utilise the powers available in any imaginative way, and we have a situation where only the barest of usable information can be gleaned from the online public register. In its current plans, the web site of the ICO is to have a raised priority in terms of navigability etc., but the proposed strategy does not include increasing research accessibility to the online register.<sup>56</sup> In the next section, I suggest a different approach to the register.

---

<sup>54</sup> Though even this classical registration model doesn't remove information each year as does the ICO's register.

<sup>55</sup> Statutory Instrument 188. The Data Protection (Notification and Notification Fees) Regulations 2000.

<sup>56</sup> See Information Commissioner's Office, "Online Strategy (2004 - 2007)". Removed from ICO Website. Copy with author.



## 7. What should a re-engineered register contain?

There are clearly several areas where the register does not present an accurate picture of data processing reality, and which might be included in a more useful register. For example:

1. *Quantity*: As stated above, the requirement for a simple registration format means that the register does not include any indication of the quantity of information being processed. A company which holds 500 million records on individuals is presently not required to state this in the register even though it may be using it in its advertising.<sup>57</sup>
2. *Frequency*: Data which is collected but rarely accessed differs in effect from that which is frequently accessed and processed. For example, running algorithms over past purchases every time one stands at a supermarket checkout is a different sort of processing from having the situation where the stored information is only infrequently examined
3. *Processing techniques*: The use of techniques to extract information from data is a developing field including such large-scale procedures as data mining. What are the techniques being applied? We now more about the techniques that companies use to process data from data mining textbooks than we do from the register. It would be possible to produce a classification system that indicates the ‘intrusiveness’ of the processing techniques being used, that would provide a much more accurate picture of what is happening<sup>58</sup> and that would allow transnational analysis through a formal category system.
4. *Data transfer*: There are basic indications in the current register that data is being transferred, but, as above, quantities, frequencies and to whom are not required to be stated. Contracts which allow such transfers (through ‘consent’) usually only stipulate ‘may transfer’. The register should provide much more detailed analysis of the recipients of these transfers and whether any contractual terms are being passed on with the data.
5. *Data subject requests*: An organisation could be required to indicate how many requests for access to information or amendment requests are being made and the nature of these.

---

<sup>57</sup> Equifax UK, for example, has advertised its relationship with the Department of Constitutional Affairs (responsible for government policy on data protection): “Equifax provides the DCA with data via Equifax eTrail, a powerful online system designed specifically for government departments. In addition to providing access to more than 500 million records on individuals in the UK, the new contract will include commercial data on Directors and Businesses, enhanced searching reports, improved audit functionality and access to multiple search techniques via batch processes.” Equifax UK, Press Release, 6<sup>th</sup> Feb 2006, [http://www.equifax.co.uk/our\\_company/press\\_room/2006/ContractRenewal\\_etrail.html](http://www.equifax.co.uk/our_company/press_room/2006/ContractRenewal_etrail.html)

<sup>58</sup> Technology is routinely classified in the patent system so the idea is hardly novel. See e.g., the International Patent Classification @: [http://www.wipo.int/classifications/fulltext/new\\_ipc/ipcen.html](http://www.wipo.int/classifications/fulltext/new_ipc/ipcen.html)

There are no doubt other areas where information could usefully be entered into the register – and perhaps once entered, the data could remain available<sup>59</sup> so that a historical picture can be developed of what is happening in the information marketplace. None of these pieces of information is sensitive in terms of privacy or data protection since they are not about individuals. They certainly have the potential to be sensitive in terms of commercial activities – the kinds of processing being applied may be viewed by the data controllers as trade secrets. However, we have – through passing the Data Protection Act – accepted that personal data processing is a special case and must be treated in a special manner, which should mean in terms of registration having it open to view and analysis: The logical conclusion of having a registration scheme is that there should be a ‘right to process’ information which is ‘public’ and ‘register based’.

The data that is being processed by data controllers is often highly marketable information. It can have a considerable economic value to the collectors and processors, but this value does not presently come across in the limited model of registration which is now required. A more developed and analytical approach to collecting information for the register would clarify just what is happening to privacy and personal data.

The ideal, of course, is a unified approach to research-based notification by those whose responsibility is data protection throughout Europe. Unification should provide a common analytical framework. Given that these are often agencies which have also been tasked with Freedom of Information (and other information-related tasks)<sup>60</sup> it does not appear impossible that a coherent approach could be built across Europe to better utilise the process of notification and upgrade it from its current task of revenue raising.

The EC in its analysis of where data protection harmonisation had arrived at noted that there were a significant number of differences in implementation, some of which of course are to do with notification procedures. The Commission suggested:

*Closer cooperation among the supervisory authorities of the Member States and a general willingness to reduce the negative impact of divergences are therefore to be seen as one alternative, while amendments to the Directive reducing the amount of choice left to the national legislator and to national supervisory authorities are the other. The Member States and their supervisory authorities will no doubt prefer the first option and it is up to them to show that it can work.<sup>61</sup>*

However, there does appear to be a lack of desire to interact within the supervisory authorities – seen by the fact that even in 2003 the UK and the other countries suggesting amendments were unaware that some notification schemes were less onerous than their own. The report also notes complaints that resources have been

---

<sup>59</sup> The current model allows only current notifications to remain: “S19 (4) No entry shall be retained in the register for more than the relevant time except on payment of such fee as may be prescribed by fees regulations.”

<sup>60</sup> For example, the Spanish office also concerns itself with spam issues.

<sup>61</sup> Report from the Commission - First report on the implementation of the Data Protection Directive (95/46/EC), COM/2003/0265 Final.

limited for supervisory authorities. There is no over-arching supervisory system except, perhaps, for the Art 29 Working Party group which is advisory and independent of the Commission. Unfortunately there appears to be no discussion as to how to utilise registers for research, or even just what is the purpose of notification.

### **8. The Wider Picture**

It is important to realise that the development of online public access to registers information is usually a relatively trivial offshoot of the main administrative computerisation project. Gathering and verifying the data is the expensive part of the process, and often the one that causes problems in system development. In contrast, it is cheap to store and to make available from a server-side system to the user's browser once this process has been completed. Despite this, there are many registers that are notionally public yet which are difficult to access even post-computerisation of their data. For example, the Royal Courts of Justice in London had for many years operated a 'cause book' where one had to visit one or more offices and view a loose leaf folder, which contained information on upcoming cases (at a fee of £5 per half hour). Computerisation of this cause book has been recently carried out, but there is no public system whereby journalists or researchers are enabled to easily carry out processing, searching or similar activities – the system was designed for the benefit of Court Service staff rather than for public access. Compare that situation with the US federal court system, which – under pressure to improve public access – has developed the PACER system.<sup>62</sup> In addition, online filing of court documents allows a researcher in the UK to follow US cases as they develop much more easily than those in the UK, or to better carry out statistical analysis of courts in the US than in the UK.<sup>63</sup>

Also important in the wider picture is that data access generally continues to be seen as a valuable goal. For example, the science community suggests that access to underlying data is a necessary development to promote trust:

*Departments should aim to publish all the scientific evidence and analysis underlying policy decisions... . Openness will stimulate greater critical discussion of the scientific basis of policy proposals and bring to bear any conflicting scientific evidence [that] may have been overlooked. These are good reasons for releasing information, an action which could itself avoid controversy in the long run.*<sup>64</sup>

This kind of call has been taken up with a call for the development of public registers which contain medical data.<sup>65</sup> Clearly, the notion of a public register is a powerful

---

<sup>62</sup> "The PACER Service Center is the Federal Judiciary's centralized registration, billing, and technical support center for electronic access to U.S. District, Bankruptcy, and Appellate court records." See <http://pacer.psc.uscourts.gov/>

<sup>63</sup> For a broader picture of the UK, see I Hare, "Access to Governmental Information and the Judicial Process: United Kingdom Law and the Influence of Europe", in A Dashwood and A Ward (eds) (1999) *Cambridge Yearbook of European Legal Studies* 329-354.

<sup>64</sup> Office of Science and Technology. *The use of scientific advice in policy making*. London: Department of Trade and Industry, (March 1997).

<sup>65</sup> MB Roberts et al, "Intellectual property, drug licensing, freedom of information, and public health", (1998) *The Lancet* 352:726-729.

one and one which we can expect to see develop in the information age rather than wither away.

There are perhaps two approaches to developing better public access to these registers in the UK: We can either hope that there is a public spiritedness in the administration undertaking computerisation projects sufficient to include good, public online access systems. Or, we can expect the pressure from the FoI Act to create a culture whereby online access is viewed as a vital element to be considered when developing a record keeping system. The latter situation is what one might have expected the Information Commissioner to support.

### **9. Public Registers: Public Interest v. Privacy**

There are few real potential problems relating to privacy concerning the registers of notifications – clearly because they do not hold personal data, and they relate to commercial entities who are not normally perceived as having privacy rights.<sup>66</sup> However, this is certainly not the case with all public registers – indeed the provision of Land Registry information in the UK (detailing house prices) was awarded with a ‘Most Heinous Government Agency Award’ by Privacy International for ‘openly placing details of all house purchases and purchasers online for a fee’.<sup>67</sup> There are many other public records that contain information which some believe should be removed from the public sphere – indeed, much of the early writing on the subject of privacy was concerned with such computerised registers since there may have been registers in existence, but the difficulty in access methods meant that these were rarely consulted. Court records in particular have been a primary area of this kind of concern.<sup>68</sup>

The critics of open registers say it is the access technology which has changed the situation and this requires a change of attitude to the openness of public information. Amongst these critics there is a feeling that access to these registers should be more controlled. Many reasons are used to demand such control. For example the UK Patent Office recently suggested that names of inventors should not necessarily appear on patent documents because they may be targeted by animal right’s activists. Similarly, required shareholder information – it has been suggested – should be amended for the same reason. Online planning applications and suchlike, too, are being viewed as invasions of personal space.

We have seen this kind of curtailing approach have practical effect in the UK, where the public electoral register was amended (two versions being produced, one of which could be sold) because of a complaint that the register should not be sold when it contained information which an individual did not wish to have sold.<sup>69</sup> The effect of this is not really to increase privacy – most companies who deal with personal information have many, many other sources from which to fill in the slots left by a

---

<sup>66</sup> Though the UK has certainly given one commercial chain such protection *Broadcasting Standards Commission Ex Parte British Broadcasting Corporation, R V.* [1999] EWHC Admin 659 (9 July 1999).

<sup>67</sup> See their website at: [www.privacyinternational.org](http://www.privacyinternational.org)

<sup>68</sup> See National Centre for State Courts @: <http://www.courtaccess.org/>

<sup>69</sup> *R (Robertson) v. Wakefield MDC* [2002] QB 1052. See also *Robertson, R (on the application of) v Experian Ltd & Another* [2003] EWHC 1760 (Admin).

vacant record in the electoral register. What the decision in *R v Wakefield* does do is make it harder to produce low cost ways for new start up businesses to compete with the established sellers of information. For example, I-CD failed in judicial review hearing to overturn the *R v Wakefield* approach in its attempt to offer a cheap rival service to Experian and Equifax.<sup>70</sup> The decisions make it appear that something is being done to protect privacy, but, in reality, the only result is that we all pay more for services because there is a lack of competition in the financial information service industry.

The demand for reduced access to public registers is, to my mind, a dangerous development. Those privacy advocates who wish to curtail access to public information appear to have a strange model of democratic involvement. They hold that the model should be one where large companies and the government know everything about us (and government accesses the information from the former that it doesn't have)<sup>71</sup> yet we know nothing about our neighbours who are enabled to keep a 'private sphere' only from us. It is almost the reverse of the Athenian ideal where we openly participate in the community – in the 'privacy world' we have a relationship with our neighbours only through our intervention with the State and its professional representatives. We are asked to trust those in professional positions since we cannot be trusted with information ourselves. For example, social workers are given rights to present evidence *in camera* and to access information about child abusers which is otherwise private because the population cannot either be trusted with that information or trusted to participate in the community protection process. The social work profession is given special rights because it is proposed as 'caring' and 'professional' despite the fact that – as Wood was writing some 20 years ago<sup>72</sup> – most people would prefer to see the police at their door than a social worker given that the latter has the more draconian powers to remove children. The professions, as sociology and any number of inquiries into social work blunders have taught us, always have their own agenda and this is not always the agenda best for the public benefit.<sup>73</sup>

It is clear that when the public do get information, they welcome it. The success of the FoI Act in the UK has been striking since it – some might say, at last – gives the public a right to know public information. Where public information has been available and accessed, we often find that attempts to remove this create resentment as when a Ohio court website detailing 'domestic relations' cases was shut down:

*When a pair of Butler County judges shut off Internet access to their courts' records, they opened the floodgates, says Cindy Carpenter, the county's clerk of courts. Hundreds of citizens have complained ... "I feel it's like having a nuclear explosion here in our office. We do the best planning to be efficient and accurate, and - boom! - they put on this order without a single warning, and just every single employee in this office is frazzled," Carpenter said. "I feel public*

---

<sup>70</sup> *I-Cd Publishing Ltd. v Secretary of State* [2003] EWHC 1761 (Admin)

<sup>71</sup> See Note 58 referring to Equifax's relationship with government, above.

<sup>72</sup> M Wood, "Rule, Rules, and Law", in P Leith and P Ingram (eds), *The Jurisprudence of Orthodoxy: Queen's University essays on H. L. A. Hart*, (1988).

<sup>73</sup> The message of my co-authored (with J. Morison) *The Barrister's World and the Nature of Law*, (1990) was that you need the legal profession but no client should ever totally trust his lawyer.

*records are so important. How can I just tell people, 'the judges deny you access, good luck?'"<sup>74</sup>*

Registers of public information will always be necessary and we can either privatise the information within them (or effectively do so by making access difficult) so that they essentially become part of only professional knowledge, or we can make them available to the community so that the community better understands itself. The glory of the public register is that it contains useful and basic information about our community: Who owns what, who has done what, and lets the data speak to us directly. Additionally, as I have been arguing with respect to the notification register, it also allows research-led policy to be developed when researchers have sufficiently useful access to the data.

The world which the privacy advocate proposes is professionalised and paternalistic – a nightmare scenario which they posit as a necessary social advance. It can only produce a dysfunctional society, as I have argued elsewhere.<sup>75</sup>

## **10. Conclusion**

First, I have outlined my particular problems in trying to get research data from the ICO and this has highlighted a potential difficulty in the manner in which Freedom of Information requests will be handled when the information being sought is considered as 'raw data'. If an organisation, part of whose reason for being is to make information available, is unwilling to give up this raw data, we can only guess at how difficult it will be to access that data from other public authorities. The ICO is, of course, the first arbiter in any dispute as to what public authorities should produce – it is hardly likely to impose more strict requirements upon other agencies than it imposes upon itself.

Second, I have suggested that the position being taken by the ICO in respect of a distinction between raw data/information is not valid in law. It has been 'plucked out of the air' by the Information Commissioner and indicates a lack of technical understanding of a basic mode of computer storage and processing.

Third, that even if my interpretation of the legal nature of information is wrong, the ICO has a particular role to encourage research and analysis of the data protection regime. It is failing to fulfil the obligations – the 'spirit' – that a reading of the legislative process and an understanding of the philosophy of data protection would suggest have been imposed upon it.

Fourth, I have suggested that European harmonisation offers an opportunity to work collectively on data gathering and analysis through the register or notifications. In the new Europe there will be many similar public registers which could potentially go on-line is, of course, for discussion elsewhere – but should not be forgotten.

Fifth, and with specific reference to the Information Commissioner, I have suggested that development of the notification register as a research tool is entirely in the hands of the ICO (and the wider European notification community). There exists – allowed

---

<sup>74</sup> J Morse, "Web cutoff causes Butler backlash", *The Cincinnati Enquirer*. (8 July 2003).

<sup>75</sup> P Leith, "The Socio-legal Context of Privacy", in *International Journal of Law in Context*. June 2006, pp 105-136.

by the legislation – the flexibility to promote this as a useful facility which is being ignored by the Information Commissioner. My suspicion is that this is not a deliberate attempt to hide information, but rather that at the policy level there is a lack of understanding of the underlying data technology and how it might be accessed. There is certainly a lack of desire to encourage independent research into data processing which naturally follows on from a lack of policy vision. Data protection legislation is obviously going to be around for some time; data processing is not going to go away; and the need for a better understanding of what is happening will surely continue – particularly since the legislation does not appear to be curbing the processing of personal data in the way that the originators of the legislation intended. Perhaps, therefore, the ICO will reconsider its approach to the use of the register as a research tool?

Finally, I have briefly argued that the idea of a public register is of great social value and they should remain accessible in a manner suitable for the digital age.