

Data protection and small print or big picture

Peter Jenkins casts an eye over recent trends

The attraction (or lure) of the internet has always been that it offers you easy access to all this information. What is becoming ever more apparent is that the reverse is also true, in that the new technology equally provides the internet with easy access to *all this information on you*. In the wake of the controversy over Facebook security controls, Google Earth, and consumer profiling via web searches, the exact dimensions of personal privacy are becoming ever harder to define and maintain. Ideas of 'protected personal space' or 'private data' rapidly become obsolete in a context where 98 per cent of the UK's population can be identified by three readily accessible factors – namely age, gender and postcode¹.

Meanwhile, the systems which gather personal data for official purposes grow still larger and more complex. The much-criticised NHS 'spine' of personal medical e-records lumbers slowly towards completion. Sir David Ormand, former Whitehall security coordinator, warns that the 'war against terror' will mean inevitable inroads into personal privacy, via the stockpiling of travel transactions, emails and phone records (Guardian, 25/2/2009). The House of Lords, not an obvious hotbed of radicalism, similarly intones against a modern culture of 'pervasive and routine' electronic surveillance via CCTV (Guardian, 6/2/2009).

Data protection law

Given these concerns about privacy and data protection, the spotlight is falling with increasing urgency on the legislation originally designed to maintain safeguards on personal privacy and to protect personal data. One major plank of this protection, the Human Rights Act (HRA) 1998, is now scheduled for review (and possible replacement) by a UK Bill of Rights. The second, the Data Protection Act (DPA) 1998, is subject to continuing criticism, as to whether it is really still 'fit for

Peter Jenkins is a senior lecturer in counselling at the University of Salford and author of *Counselling, psychotherapy and the law* (2nd ed, Sage 2007).



privacy: sure?



DON BISHOP/GETTY

purpose', as it enters its 10th year of operation.

The Data Protection Act 1998 has certainly enjoyed a somewhat chequered history in the past decade. It derives from two overlapping legal sources: UK case law and European Directive. These streams often seem to pull apart, rather than seamlessly mesh together. Graham Gaskin, a rebellious young man in the care of Liverpool Social Services, brought a partially successful case for access to his social work files to the European Court of Human Rights back in the 1980s. This then opened up access, previously denied, to health, education and social work files – now deemed 'accessible records'. This move anticipated the introduction of a new European Directive, regulating electronic and manual recording, to become the Data Protection Act 1998. Right from the beginning, the language of the Act has been criticised as opaque and technocratic. One senior judge described the law as 'inelegant and cumbersome'. Even the official DPA guide has been forced to admit that 'the legislation itself is complex and, in places, hard to understand'².

Data protection has undergone some distinct challenges in the courts, during its first 10 years' existence. Concerns have been raised about the law's efficacy in regulating a growing corporate trade in illicitly obtained personal data. The individual's right to access personal files has become heavily qualified, with successive re-interpretations of the law. Meanwhile, the implications for therapists and their clients have become ever more complex and hard to unravel, prompting fresh guidance from the Information Commissioner's Office (ICO).

Key challenges to data protection law

The problems involved in grasping the purpose of the Act and applying it sensibly within large, complex organisations quickly became a national media issue in the wake of the Soham murders of Jessica Chapman and Holly Wells. It emerged that Ian Huntley had come to the attention of Humberside Police for eight separate alleged sexual offences prior to the murders. However, this crucial intelligence was not made available in ways which could have reduced or removed the risk to the public. The Humberside Police claimed that the problems arose via the nature of existing data protection law. Lord Richard decisively rejected this argument, pointing instead to 'very serious failings in the senior management of Humberside police'³.

The other major test for the new data protection regime came in the form of a key test case against the Financial Services Authority. This was brought by an applicant seeking access to a



file of correspondence for the purpose of litigation. The radical thrust of the DPA was that it offered access to manual, ie handwritten files, in addition to electronic files held on computer. The ICO initially seemed to take a very broad view of 'manual files', apparently interpreting this to mean that *most* manual files would now become accessible to individuals. This directly conflicted, however, with the stated intentions of those drafting the original legislation. The latter had sought to permit access *only* to those manual files which were clearly based on sophisticated information retrieval systems.

Access to personal records

The Durant case, decided at the Court of Appeal in 2003, established the high-water mark of the attempt to authorise access to the bulk of handwritten personal files. Instead, the court opted for a much narrower standard of relevance for accessing records, defining 'personal data' as 'information that affects a person's *privacy*' (Durant v FSA [2003]). This substantially limited access to 'unstructured' manual records. The later Freedom of Information Act 2000 then reopened access to those unstructured manual records held by public authorities, such as colleges, universities and local authorities.

This has produced a complex mosaic of differing routes of access to records. This is policed by organisational data protection officers, but is understood in its fine detail by few and probably misunderstood by many ordinary citizens. The current guide to the DPA may well claim that 'the right of subject access is central to data protection law', but this right is actually heavily circumscribed and hedged about in real life². Counselling clients, for example, do not hold an automatic right to unstructured manual records held by voluntary agencies, or by those in private practice, unless these manual files closely resemble electronic files in format and ease of information retrieval – the so called 'temp test' referred to in Durant. This is a finding unlikely to be readily accepted by former clients involved in litigation, or, more pointedly, by their solicitors⁴.

Illicit data trading



Data protection regimes face an even stiffer test, in trying to regulate the growing and very lucrative trade in personal data for corporate purposes. Recent cases have highlighted journalists' use of 'hacking' personal data, in the form of emails and mobile phone records. Medical records, outsourced abroad, are ending up for re-sale to interested private medical insurance firms, or pharmaceutical companies. Data theft by disgruntled employees is

now described as 'endemic' within the corporate world. One US survey indicated that 41 per cent of respondents had already taken sensitive information with them to a new position, while 26 per cent would pass on company data, if it proved useful in helping friends or family members to get a job⁵. The sheer scale of the problem with illicit data trading is perhaps illustrated by one report that Angela Merkel, the German chancellor, was apparently considering buying back stolen data about secret Swiss bank accounts. The data, reportedly being offered for sale by a former HSBC employee, held information on 1,500 alleged tax evaders of major interest to the German tax authorities (Guardian, 2/2/2010).

Enforcing data protection rights

The ICO is the independent UK authority charged with upholding information and privacy rights, and with promoting openness by public bodies. No doubt it will be under increasing scrutiny, in light of the proposed governmental cull of quangos, and concerns about the growing intrusions into personal privacy marked by unauthorised data trading. Christopher Graham, the third person to hold the post of Information Commissioner, has called for 'effective sanctions' to stem the illegal trade in personal data. Action is currently planned against covert information held on trade union militants by private data firms, and the Department of Health was 'severely reprimanded' for breaches of web privacy concerning junior doctors.

However, there are continuing concerns that the ICO still maintains something of a 'light touch' when it comes to actual enforcement of data protection law. Controversially, Simon Davies, a prominent critic from Privacy International, alleges that the original law was 'written with the express intention of ensuring that data protection administration was weak, because this government saw data protection as a potential roadblock to profitable commerce' (Guardian, 5/4/2008).

Further potential evidence for this argument comes from the journalist Heather Brooke's account of her struggle to access information on MPs' expenses. The request, made under the Freedom of Information Act for itemised expenses, was blocked by the ICO, as this was deemed to be 'unfair'. At the hearing, the responsible parliamentary officer echoed this stance, claiming, rather unfortunately, that 'transparency will damage democracy'⁶. On appeal, the Information Tribunal ordered itemised disclosure, enabling individual MPs' expenses to be identified, duck houses and all. Nevertheless, according to Brooke, full disclosure of the expenses scandal eventually came, critically *not* through the effective working

of data protection law, but by the simpler, time-honoured route of a deluge of well-targeted leaks to the press.

Updated ICO guidance

If the bigger picture of data protection resonates with complexity, then the latest small print maybe represents an attempt to return to basics. The latest guidance issued by the ICO comes in a neat, folding Chinese box of a publication, as well as in more prosaic downloadable format. It is divided into three sections: an introductory overview, a more detailed discussion of the data protection principles and concluding detail on rights and exemptions. Somewhat confusingly, the guidance does not have the force of law, as would a formal statutory code of practice. The language of the guidance is determinedly informal, so that 'data subject' is now translated as 'the individual', and 'data controller' becomes, more simply, 'the organisation'.

The principle of fairness in data protection is equated with transparency and accountability. This requires the use of appropriate security measures to protect data, although this does not necessarily always entail the use of encryption for electronic data. The concept of data processing is deliberately framed in very broad terms (what Elizabeth France, the first Data Protection Commissioner, imposingly described as a 'compendious definition'), with no obvious loopholes.

Accessing data

The right of individual access to personal records is, as has been noted above, central to the law on data protection. Thus, deleting or amending data records *prior* to disclosure, for the purposes of preventing access to information (other than third party information) is disallowed. While access is permitted to data in 'intelligible form', the guidance argues rather surprisingly that, in the case of poorly written manual records, this does not mean 'make legible'. However, it does suggest that it would be 'good practice' to assist an individual to make sense of any records which are difficult to read.

The guidance is much clearer than previous versions on those forms of data which constitute *exemptions* to data protection principles, such as that permitting individual access. Data which is processed, even on a PC, *purely* for 'domestic purposes', such as the well-worn example of the Xmas card list or similar, is exempt. Holiday and camcorder photos shot purely for personal use are also exempt, despite their status as digital images. Also exempt is personal data which is processed solely for research, statistical or historical purposes.

The limitations of data protection law, as noted

above, are briefly rehearsed. The ICO is unable to award compensation for data processing which has caused an individual substantial damage or emotional distress, such as featuring on a list of suspected union activists, for example. Financial penalties will only be used in the case of 'deliberate or reckless' breaches of the data protection principles and failure to comply with the data protection principles is not, in itself, a criminal offence.

Implications for therapists

The new guidance tidies up some of the existing confusion around data protection law, using relatively user-friendly language and examples. However, the fact remains that data protection law was clearly never written with therapists in mind, or, come to think of it, other professional groups, that work across and beyond the established organisational boundaries which separate private practice from employed work, or the statutory sector from voluntary agencies, and which rely more on *manual* than electronic forms of recording. If, as a society, we are currently struggling to make sense of the bigger picture of personal privacy, in an age of electronic data, then we are probably unlikely to find the answers here in the ICO's small print, at least for the time being. ■

Further guidance for therapists on data protection

Bond T, Mitchels B. Confidentiality and record keeping in counselling and psychotherapy. London: Sage/BACP; 2008.

Bond T, Jenkins P. Access to records of counselling and psychotherapy. BACP Information Sheet G1. Lutterworth: BACP; 2008.

Information commissioner's office (ICO) guide to data protection. Wilmslow: ICO; 2009.

Jenkins P. Counselling, psychotherapy and the law. London: Sage; 2007.

Contact details for Information Commissioner's Office: ICO, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF Tel: 08456 306060/01625 545 745; mail@ico.gsi.gov.uk; www.ico.gov.uk

Legal reference

Durant v Financial Services Authority [2003] EWCA Civ 1746.

References

- 1 Tranberg H, Rashbass J. Medical records: use and abuse. Oxford: Radcliffe; 2004.
- 2 Information Commissioner's Office (ICO). Guide to data protection. Wilmslow: ICO; 2009.
- 3 Bichard M. The Bichard inquiry report. HC 653. Stationery Office: London; 2004.
- 4 Jenkins P. Therapist responses to requests for disclosure of therapeutic records: an introductory study. *Counselling and Psychotherapy Research*. 2003; 3(3):232-238.
- 5 Data theft 'endemic'. *Professional Manager*. 2010; 19(1):45.
- 6 Brooke H. The silent state. Heinemann: London; 2010.