

Access denied?

Peter Jenkins investigates issues of personal data and privacy in the 'surveillance society'

Counsellors tend to be strong on the issue of confidentiality, by virtue of their training and code of ethics. But where do they stand on issues of personal privacy? Are privacy and confidentiality the same concept, just covered by a different label? Recent widespread media coverage of the loss of major personal databases has raised concerns about personal privacy and data security. Questions, as they say, have even been asked in the House (of Commons) about the growing threat to our personal information.

Privacy or confidentiality?

From a legal perspective, privacy and confidentiality refer to different, though related, concepts. According to Pattenden, privacy is a condition, namely 'a state of voluntary physical, psychological and informational inaccessibility to others'¹. Privacy denotes the possession of personal information not in the public domain: A, for example, holds information about himself that he a secret drug habit, or perhaps has savings of £20,000. Confidentiality involves a triangular relationship, which opens the possibility of disclosure to a third party. Client A tells counsellor B a personal secret. Counsellor B may then disclose this to C, which could be a social work agency, employer or a GP. Confidentiality, where the counsellor is the 'custodian' of sensitive client information, thus entails a dynamic tension about potential or actual disclosure of the information to a third party.

Recent media coverage has focused on threats to personal privacy brought about by the emergence of an economy hungry for personal data in all its forms. Perhaps few of us realise that any individual can easily be identified on the basis of correlating three innocuous bits of information, namely age, gender and postcode². The Data Protection Act 1998, originally hailed as a defence of citizens' rights to personal data security, has proved unwieldy and cumbersome in practice. It is not surprising that it is now widely seen as not fit for purpose, given that it was originally designed to cater for the emerging needs of the corporate and financial markets, rather than for more sensitive and nuanced issues related to health and welfare.

Growth of databases

Personal privacy is further challenged by the rapid and seemingly unstoppable growth of large, information-sharing databases. The police national database of DNA now holds samples on three million citizens, whether or not convicted of an offence. An estimated four million

CCTV cameras record the average person about 300 times a day. The argument that this is necessary to monitor and reduce crime, or antisocial behaviour, is somewhat undermined by the counter-argument that the less intrusive measure of improved street lighting actually has the edge in this respect.

Internet innovations, such as Google and Facebook, appear to be, at one level, simply about rapid information retrieval, or access to fun social networking. In reality, the relentless algorithms powering them are geared much more towards the identification of individual consumer preferences and carefully targeted marketing, with a potential breach of e-privacy.

The databases have not quite won the day, however. The much-troubled NHS national database has been unable to win over key constituents, despite a barrage of favourable PR. Two thirds of GPs fully intend to boycott the uploading of patient medical records, unless they receive specific consent from the concerned individual. Opposition in Iceland over a similar scheme led to the whole system being abandoned in 2006.

Information sharing on children

With regard to more vulnerable social groups, the rapid erosion of personal privacy has passed largely without comment. Three and a half thousand schools have agreed to the finger-printing of around three-quarters of a million children, for easier management of libraries and school meals. This has been set up without parents being informed or required to give their consent. According to Terry Dowty of ARCH (Action for Rights of Children www.arch-ed.org) 'a huge number of children are being taught to give out biometric information without even a second thought'.

This shift towards processing vast amounts of personal information on children is at the heart of government strategies for tackling child abuse and the coordination of services, via the children's databases brought in by the Children Act 2004. Professional access to sensitive information on children is seen as a key measure for avoiding tragedies like the death of Victoria Climbié. However, critics of the rush to construct these databases point to a serious flaw in using this latter case as a lever for change. In the Climbié case, the problem was not professionals lacking information, but their failure to grasp the significance of key abuse indicators. Holding more information may make childcare bureaucracies feel more secure, but it does not necessarily lead to improved quality of decision-making³.

Losing personal records

Media publicity has, predictably, focused on recent large-scale security breaches and lapses regarding personal data. The loss of 25 million sets of personal data by HM Revenue and

Peter Jenkins is co-director of counselling and psychotherapy at the University of Salford and author of *Counselling, psychotherapy and the law*, 2nd ed, (Sage, 2007).

Customs was rapidly followed by further losses by the Northern Ireland DVLA. In some cases, personal data is lost through theft, rather than carelessness, as when the client records held by a Manchester bereavement service on a flash drive were stolen.

Other threats to personal data privacy have taken other, perhaps unexpected forms. David Southall, a controversial paediatric expert witness, was found by the GMC to have retained 4,500 secret medical records on patients, in spite of supposed restrictions on dual sets of records. Also in the medical field, Channel 4 news exposed the flaws in the electronic system established by the Medical Training Application Service. Altering a single number in the URL provided free access to junior doctor applicants' personal details, including criminal convictions and sexual orientation. The data had neither been safely encrypted, nor password protected, according to C4 news. The latter used a 'public interest' defence to break the story, but was then roundly condemned for doing so, by a hugely embarrassed Department of Health and Secretary of State, Patricia Hewitt.

Information Commission response

Given the growth of huge databases and the recent losses of private information, what has been the authorities' response so far? The outgoing Information Commissioner, Elizabeth France, promised 'vigorous enforcement' of the new data protection law. Her successor, Richard Thomas, has been seen to take rather more of 'hands-off' approach, despite his voiced concerns about our 'sleepwalking into a surveillance society'. The Department of Health fiasco about junior doctors produced no more than a severe reprimand from the Information Commissioner. In parliament, MPs have discussed whether the loss of personal data should now become a criminal offence. Currently, the loss of data by designated 'data controllers' does not carry this level of sanction.

For some critics, such as Privacy International, the Information Commissioner's stance is just not robust enough. Thomas has, for example, focused on the undercover sale of information obtained by deception, via private detective agencies, but has perhaps missed the bigger picture. The European Commission is now threatening legal action over the existence of continuing loopholes in UK data protection law. Even the government itself has refused to comply with a Freedom of Information Request to release a hitherto unknown first draft of the original 'dodgy dossier' on Iraqi weapons of mass destruction⁴. Given the government's apparent unswerving commitment to extending biometric data storage and exchange, via ID cards and as part of the international war on terror, the Information Commissioner seems, so far, to lack real teeth in checking this erosion of personal data privacy.

Implications for counsellors

So what are the implications for counsellors? Threats to counselling confidentiality are perhaps more on the average counsellor's radar, as in the case of recent policy kites trailed for the compulsory reporting of violent crime by council workers, or for GPs to report all knife or gunshot wounds to the police. Perhaps part of the problem regarding counsellors' awareness

of privacy issues has been that, in the past, that there was no coherent law of privacy in the UK. There was, instead, just a collection of individual cases, largely about defending the reputation of the rich and famous. Recent court decisions have begun to alter this, however, and the contours of a more embedded law of personal privacy is beginning to take shape, in the wake of the *Hello* and Monaco court cases⁵.

Crucially, the courts upheld the right to privacy of supermodel, Naomi Campbell, photographed emerging from a meeting of Narcotics Anonymous in 2001. This judgment is about privacy, rather than confidentiality, and it does underline the key point that therapy is a private activity, analogous to medical treatment. Therapy is not something designed for public entertainment in the broadsheets, as when Princess Diana used to run a barrage of press photographers, when visiting her therapist, Susie Orbach.

The wider implications of the Naomi Campbell case are very significant in the long term. Counsellors in the UK have long felt under pressure from courts and solicitors, wanting access to client files for litigation purposes, but have lacked any effective defence against these demands. However, in the US, the right to privacy is enshrined in the Constitution. The principle of therapist privilege (protection from enforced disclosure of client records) has consequently been established, albeit in limited form. US privacy law has provided the crucial foundation for therapist claims to legal privilege in the US⁶. As the counselling profession moves unsteadily towards statutory regulation in the UK, it might just be worth dusting off our position statements on privacy, with this future development in mind. ■

References

- 1 Pattenden R. The law of professional-client confidentiality: regulating the disclosure of personal information. Oxford: OUP; 2003.
- 2 Tranberg H, Rashbass J. Medical records: use and abuse. Oxford: Radcliffe; 2004.
- 3 Anderson R et al. Children's databases – safety and security: a report for the Information Commissioner. London: Foundation for Information Policy Research; 2006.
- 4 Baker N. The strange death of David Kelly. London: Methuen; 2007.
- 5 Tomlinson H, Tench D. Privacy gets the OK. *The Guardian*. 7/5/07.
- 6 L'Heureux-Dube C. The right to privacy. In: Levin C, Furlong A, O'Neil MK. Confidentiality: ethical perspectives and clinical dilemmas. Hillsdale, NJ: Analytic Press; 2003.

PHOTODISC/GETTY

