Web Journal of Current Legal Issues

Wong, 'Assessing the Status of Medical Information in the light of the UK Data Protection Act 1998' [2008] 5 Web JCLI
http://webjcli.ncl.ac.uk/2008/issue5/wong5.html

Assessing the Status of Medical Information in the light of the UK Data Protection Act 1998

Dr Rebecca Wong

Senior Lecturer in Law
Nottingham Law School,
Nottingham Trent University

R.Wong@ntu.ac.uk

Summary

In this article, the current data protection framework as applied to the medical information is examined with a discussion into the broad scope of the definitions provided under the European Data Protection Directive 95/46/EC and how this is reflected within the UK Data Protection Act 1998.

Contents

Bibliography
Legislation
Articles and Books

---

1. Introduction

This article will consider the current privacy laws as applied to healthcare in the UK, taking into account the UK Data Protection Act 1998, which implements the European Data Protection Directive 95/46/EC (hereinafter "DPD"). Whilst the data protection laws in the UK deals with the overall protection of an individual's personal information, there are certain issues that still need to be addressed by UK Courts including the subject of anonymous data; sensitive data; electronic patient records and genetic databases. To understand these issues, we will need to understand the context in which the UK data protection laws apply and the recent caselaw emerging from the UK courts and the European Court of Justice. Part 2 will consider the scope of the Data Protection Act 1998 followed by a discussion of "genetic data". The discussion of "anonymous" and "pseudonymous" data is then considered before examining health records with final concluding remarks.

2. Data Protection Act 1998

To begin with, the Data Protection Act 1998 ("DPA") (see Jay and Hamilton, 2003; Carey, 2004) replaces the Data Protection Act 1984 and was enacted to transpose the European Data Protection Directive 95/46/EC, the latter is applicable within the European Union. The UK DPA 1998, Sch. 1 contains eight main data protection principles. These are:

> "1.Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
>
> (a) at least one of the conditions in Schedule 2 is met; and
> (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
>
> 2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
>
> 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
>
> 4. Personal data shall be accurate and, where necessary kept up to date.
>
> 5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under the Act.

7. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection."

A few preliminary points to be made about the interpretation of personal data beginning with the European Data Protection Directive 95/46/EC. Art. 2 of the Data Protection Directive 95/46/EC defines "personal data" as '

> "any information relating to an identified, *directly or indirectly*, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

What constitutes "personal data" has recently been the subject of analysis and interpretation by the European Court of Justice and the UK Court of Appeal. Should "personal data" be defined broadly so that it encompasses the legal theory of an individual's personality or should the notion be limited to an individual's identity? (see AHRC. Privacy, property, personality project at http://www.law.ed.ac.uk/ahrc/personality/). The UK Court of Appeal recently held in *Durant v FSA* [2003] EWCA Civ 174 that:

a. Not all information retrieved from a search against an individual's name or unique identifier is personal data within the 1998 Act.
b. That mere mention of an individual in a document held by a data controller does not mean that the document contains personal data in relation to that individual.
c. That whether information is capable of constituting personal data depends on whether it falls in a continuum of relevance or proximity to the data subject.
d. That in answering that question it is relevant to consider whether the information is *biographical in a significant sense*; and whether it has the *putative data subject as its focus* and
e. That personal data is information that affects the privacy of the putative data subject, whether in his personal, business or professional capacity (see also the UK Information Commissioner, 2004).

This decision contrasts with the European Court of Justice (ECJ) judgment in *Lindqvist* C-101/01 [2004] 1 C.M.L.R, a case referred by the Swedish Appeals Court, which held that the notion of "personal data" ought to be defined broadly, such that mere mention of an individual's injured foot on a webpage constituted the processing of sensitive personal data (see also Blume, 2001; Klang, 2003; Wong, 2005).

In *Lindqvist*, L had created a webpage containing personal details (including the interests and hobbies) of some of the members of the parish church and also mentioned that one of the members had injured her foot. The Court took the view that she had contravened the Personal Data Act 1998 and subsequently fined her. When a preliminary reference ruling was made to the ECJ, the Court held that:

> "The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, *constitutes the processing of personal data* wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46/EC of the European Parliament and of the Council 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 (C-101/01 [2004] 1 C.M.L.R. 20 at para. 68)"

How can these two decisions be reconciled? The criticism of the ruling by the UK Court of Appeal has not gone unopposed. For example, Lloyd took the view that:

> "This approach [that the UK courts] adopts, it is suggested, an overly restrictive view of the rationale of data protection laws. Whilst determining the legality of data processing and correcting errors certainly constitute important elements, equally important is the ability to become aware what data is held. Much of the Data Protection Directive and Data Protection Act 1998's requirements relating to the factors legitimising data processing stress the importance of the data subject being aware what is happening with regard to personal data…Such factors support the adoption of an expansive definition of the scope of personal data." (Lloyd, 2004, pp. 89-90)

There is also increased uncertainty in the *Durant's* decision following another Court of Appeal's decision in *R v Rooney* [2006] EWCA Crim 1841, which appears to adopt a wider interpretation of personal data (see Charles Russell, 2006 at http://www.cr-law.co.uk/articles/viewarticle.asp?articleid=1579). The subject of personal data is unlikely to be resolved, until there is a higher court ruling such as the House of Lords, to provide more clarity. However, we can glean some information from a recent opinion published by the Art. 29 Working Party, an advisory group comprised of representatives from the supervisory authorities responsible for data protection of each EU member state, set up under the Data Protection Directive. The Art. 29 Working Party has recently published guidance on the concept of personal data (Art. 29 Working Party, 2007) and reiterated the breadth of the definition under the Data Protection Directive:

> "It needs to be noted that this definition reflects the intention of the European lawmaker for a wide notion of "personal data", maintained throughout the legislative process (Art. 29 Working Party, 2007)."

This is in line with the ECJ's decision in *Lindqvist* and clarifies the discussion over anonymous and pseudonymous data, which is considered later.

Another point to add, is that unlike the DPA 1984, s 2 DPA 1998 contains a separate category of data often referred to as "sensitive data", meriting further protection before this type of data can be processed. Sensitive data is defined under s 2 DPA 1998 as "data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" (see also Simitis, 1999; Bygrave, 2002 at pp. 68-69; Wong, 2007). To process such data, an individual should give their *explicit* consent or be able to use the justifications as provided under Art. 8(2) DPD or corresponding national legislation, UK DPA 1998. There is no definition of "*explicit* consent" provided by the Data Protection Directive. Consent is defined under Art. 2(h) as "any freely given specific and information indication of his wishes [data subject] by which the data subject signifies his agreement to personal data relating to him being processed." Explicit consent has been interpreted by countries such as Germany (see §4(a)(1) Federal Data Protection Act 2001) to refer to written consent, before sensitive data can be processed. However, unlike Germany, UK does not require a written form of consent before sensitive data can be processed (see Jay and Hamilton, 1999, pp. 37-41). A verbal consent by a data subject will be sufficient. Consent by silence will not, however, satisfy the requirement that explicit consent is given (see PRIVIREAL, 2007).

Before discussing genetic data, one should consider, in brief the main provisions applicable under the UK Data Protection Act 1998 (DPA). The UK DPA applies to personal data relating to living individuals (s 1). The Act does not apply to corporations or companies. The Act places responsibility on data controllers, who process personal information to comply with the data protection principles. Data controllers are defined under s1(1) UK DPA 1998 as someone who "(either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed". There could be more than one data controller, so it is vitally important to identify who has control of the personal data in question. Secondly, there may also be data processors, who process personal data on behalf of the data controllers and this is recognised under s 1(1) DPA 1998. Data subjects (individuals, whose personal data are being processed) are entitled to have access to their data as provided under s 7 of the Data Protection Act 1998 by making a "data subject access request". Subject to exceptions under s 7, a data controller who receives such request would be obliged to provide details (including the purposes of the processing and the recipients to whom the data are disclosed) within 40 working days (s 7(7) DPA 1998).

According to the Eighth Data Protection Principle, personal data cannot be transferred to non-EEA countries unless the destination country can show that it has an adequate level of protection of privacy. The main factors to be taken into account when determining adequacy:

a. The nature of the personal data (presumably an acknowledgment, as with the provisions for accuracy that certain types of data require better protection than others);

b. The country or territory of origin of the information contained in the data;
c. The country or territory of final destination of the information;
d. The purposes for which and the period during which the data was intended to be processed;
e. The law, international obligations, codes of conduct or other rules in force in the country or territory in question. With respect to rules and codes of conduct these may be general or made by arrangement in particular cases;
f. The security measures taken in respect of the data in that country or territory.

The European Commission may find that a country has an adequate level of protection by virtue of Art. 25.6 of the DPD, which would mean that personal data could be transferred to a third country from any of the 25 EU member states and three EEA member countries without any further safeguards. To date, the Commission has made a finding that Switzerland, Canada, Argentina, Guernsey, Isle of Man, the US Department of Commerce's Safe Harbor Privacy Principles have an adequate level of protection (European Commission, 2007).

3. Genetic Data

The question at this stage is whether genetic data can be classed as sensitive data? By the term, "genetic data", I am using the definition given by the Council of Europe Recommendation (see Council of Europe, 2007) that genetic data is "all data of whatever type concerning the hereditary characteristics of an individual or concerning the pattern of inheritance of such characteristics within a related group of individuals" (see also Laurie, 2002).

The lack of a specific category under sensitive data does not necessarily follow that genetic data is excluded, but some EU countries have interpreted genetic data to fall within the remit of health or medical data under Art. 8(1) of the DPD or corresponding national legislation. Indeed, this subject is aptly described by Simitis as follows:

> "Genetic data are another equally significant example. Interpretation assumes in their case, because of the lack of an explicit reference in the lists of sensitive data, a particularly important role. It can indeed help to close the gap. The difficulties should however not be underestimated. There are certainly cases in which it is perfectly possible to regard genetic data as health or medical data. But it is nonetheless not justified to conclude that genetic data can under all circumstances be entered into either of these two categories. Most laws have therefore avoided a general classification and instead put the accent on the specific uses of genetic data. Their growing importance makes it, however, difficult to maintain such a carefully differentiated approach that inevitably leaves an ever greater number of processing operations uncovered. The initial hesitations were hence gradually given up. Genetic data were, as the example of Austrian, Icelandic, Norwegian, Portuguese and Swiss law, but also of the Recommendation R (97) 5 on the Protection of Medical Data shows, simply subsumed in the health or medical data. And even where doubts persisted, the repeated legislative interventions unmistakably restricting the use of genetic data were, as in France, seen as proof

> of their particular sensitivity that fully justifies treating them like all other sensitive data." (Simitis, 2007)

The Art. 29 Working Party has issued some guidance on genetic data (Art. 29 Working Party, 2004). It was identified that some EU member states such as Portugal (Art. 7(1) of the Portuguese Act on the Processing of Personal Data 67/98), Luxembourg (see http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf) and the Netherlands (*Ibid.*) have included a specific category of genetic data within the scope of "sensitive data". The guidance emphasised that there was no question that genetic data cannot be personal data within the definition of the Data Protection Directive, particularly when this data is linked to a specific person. What was less clear was whether samples of DNA constituted personal data. According to the Art. 29 Working Party (*Ibid*), genetic data which related to the disposition and health condition of individuals would be considered data concerning health.

So, the status of genetic data is certainly personal data, and more likely to be data concerning health, thus, we would be handling sensitive personal data. The main provisions under the Data Protection Directive that apply are the data protection principles as described earlier and can be found under Art. 6 of the Data Protection Directive. Exceptions to the processing of genetic data as sensitive data under Art. 8 can be found under Art. 8(2) of the DPD. The relevant provision is Art. 8(3), which provides that sensitive data can be processed (without the need for consent) on the grounds 'that processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services' and according to specific conditions.' This has been implemented under Sch 3 para 8(1) of the UK Data Protection Act 1998, which provides that:

> "(1)The processing is necessary for medical purposes and is undertaken by:
> (a) a health professional, or
> (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
> (2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services."

A final point to be added is the concerns shown by the Art. 29 Working Party on the potential misuse and/or re-use of genetic information by the data controllers or third parties. For example, re-using genetic information for purposes other than was originally provided. A hypothetical example would be patient A agrees to give his DNA for the purposes of diagnosing cancer, but later realises that this is used for statistical analysis by researchers without his knowledge. In those circumstances, consent would be required before the data can be used. Furthermore, in abiding by the data protection principles, the second data protection principle under the UK Data Protection Act 1998 (that personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes) should also be noted.

4. The Status of Anonymous and Pseudonymous Data

Before discussing the status of anonymous and pseudonymous data, a few points to be made about the terminology. When referring to anonymous data, I am referring to data in non-personal form and cannot be identified by anybody. Whereas, pseudonymous data can still be in personal form, but the identity is, according to the Art. 29 Working Party, in a disguised form (Art. 29 Working Party, 2007). There has been some academic debate about "anonymised data" and by this, we are referring to data that is in the process of being anonymous, but has not reached the status of being completely "anonymous" (stripped of any personal identifiers) (see Beyleveld and Townend, 2004; Walden, 2003) and therefore, until it is completely unidentifiable, such data continues to fall within the scope of the Data Protection Directive. An example would be researcher A, who has a list of donors' details including their names and religions. A decides to remove the donors' details such as their religions and their names from a database. In doing so, A would need to ensure that the data protection principles are adhered to (processed fairly and lawfully etc.).

On the subject of anonymous data, we should consider a recent UK Court of Appeal case, *R v Dept of Health ex parte Source Informatics* [2001] QB 424, in brief, which took the view that releasing anonymous data of doctors' patients to a pharmaceutical company researcher would not infringe the laws of confidentiality in the UK (see also Beyleveld and Histed, 2000; Hughes, 1999). Although this case does not deal with the aspects of data protection, it is perhaps, surprising to find that the laws of confidentiality (see the role of confidentiality in *Stephens v Avery* [1988] Ch 449*; Hunter v Mann* [1974] QB 767) do not apply to anonymised data, even though the main concerns are that data provided by the patient was intended for the doctor and not a pharmaceutical company.

However, in the context of data protection, the status of anonymous data is that nobody is able to recognise that the data in question is personal data. If we recall the broad definition of personal data under Art. 2(a) of the Data Protection Directive 95/46/EC, the preamble of the Directive, Recital 26 provides that:

> "Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the' principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may *be rendered anonymous and retained in a form in which identification of the data subject is no longer possible*." (emphasis added)

The question then arises, what constitutes an identifiable person? The Council of Europe Recommendation on medical data (Council of Europe, 1997) states that 'an individual

shall not be regarded as "identifiable" if identification requires an unreasonable amount of time and manpower (see Ploem, 2006, pp. 41-64)'. Whilst the Directive recognises that anonymous data is not personal data and thus, falls outside the scope of the Data Protection Directive, this cannot be said of pseudonymous data. Although the Directive does not define pseudonymous data, the Art. 29 Working Party has defined this as a "process whereby the identity of an individual is disguised" (Art. 29 Working Party, 2007). A typical example is the use of key-coded data such as numbers that are used in place of names. As the Directive applies to identified or identifiable individuals, it will cover pseudonymous data, because individuals can be indirectly identified.

> "Retraceably pseudonymised data may be considered as information on individuals which are *indirectly identifiable*. Indeed, using a pseudonym means that it is possible to backtrack to the individual, so that the individual's identity can be discovered, but then only under predefined circumstances. In that case, although data protection rules apply, the risks at stake for the individuals with regard to the processing of such indirectly identifiable information will most often be low, so that the application of these rules will justifiably be more flexible than if information on directly identifiable individuals were processed." (Ibid)

Therefore, the DPD or corresponding UK DPA continues to apply to pseudonymous data (Casebona, 2004, pp. 33-49).

Finally, the case that is worth analysing in some detail now, given its likely implications on the use of anonymous data is that of *CSA v Scottish Information Commissioner* [2006] CSIH 58 (at http://www.scotcourts.gov.uk/opinions/2006CSIH58.html) (see also Macqueen, 2007). In this case, Collie made a request to CSA on behalf of a member of the Scottish Parliament for information about the number of cases of children leukaemia in Dumfries and Galloway. CSA refused on the grounds that as the numbers involved were small, there was a possibility that individuals may be identified. Collie referred the decision to the Scottish Information Commissioner. The Scottish Information Commissioner took the view that this data could be given because the data in question could not identify individuals once released. CSA used a process called Barnadisation which did not identify individuals from the data that was released. The CSA appealed to the Court of Session following the Scottish Information Commissioner's ruling. The Court upheld the Scottish Information Commissioner's decision:

> "Although the underlying information concerns important biographical events of the children involved, by the stage of the completion of the barnardised table that information has become not only statistical but perturbed to minimise the risk of identification of any individual child. It is no longer, in respect of any child, 'biographical in a significant sense. The rights to privacy of the individual children are not infringed by the disclosure of the barnardised data." (*CSA v Scottish Information Commisioner* [2006] CSIH 58 at para 23)

CSA has made a further appeal to the House of Lords (*Commons Services Agency v Scottish Information Commissioner* [2008] I WLR 1550). The House of Lords took the

view that barnardised data, even if this was statistical information about the incidence of childhood leukaemia concerned information about children's health. The case of *Durant* was not relevant and the House of Lords did not consider it relevant to discuss the issues of "focus" and "biographical data" as required under *Durant*. The House of Lords considered the second part of the issue on personal data. Namely, whether personal data could be identified from barnardised data. Again, the House of Lords took the view that this was *question of fact* to be determined by the Scottish Information Commissioner. They held the view that it was possible that it may be possible for the data to controller to process this information if this was fully anonymous and thereby no longer fall within the remit of the Data Protection Act 1998. However, what was not considered is that until this information containing the personal data was completely *anonymous* (no personal identifiers), then this information would still be "personal data" and thereby the Data Protection Act 1998 would be relevant (see also PRIVIREAL, 2005). The House of Lords judgment clarifies certain question on the case of *Durant*, but as raised by some commentators, could go further in addressing the issues of "identifiabilty" within the UK's DPA's definition of "personal data" (see Campbell, 2008).

Guidance from the Art. 29 Working Party should be welcomed not only in providing uniformity in the interpretation of this concept, but also clarify any ambiguities and its application to anonymous and pseudonymous data.

5. Electronic Health Records

The UK health record system is in the process of being reformed, which would enable GPs to access patients' medical records easily, but the procedure has not gone through smoothly (http://www.infosys.com/industries/healthcare/cases/electronic_health_record_ukgov.asp). There has been some controversy over plans by the UK government to allow almost 50 million patient records to be uploaded onto a central database without obtaining the patients' consent (preferring an opt-out consent) (Leigh and Evans, 2006 and EuroSOCAP, 2006). This has led to calls for GPs to boycott the database. The legitimacy of uploading patient's medical records without their explicit consent appears to be contrary to Art. 8(1) of the Data Protection Directive (http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/uc422-ii/uc42202.htm and http://www.e-health-insider.com/news/item.cfm?ID=268).

The Parliamentary Health Committee has set up an enquiry, which aimed to address five specific questions (Health Committee, 2007 para 6):

1. What patient information will be held on the new local and national electronic record systems, including whether patients may prevent their personal data being placed on systems;
2. Who will have access to locally and nationally held information and under what circumstances;
3. Whether patient confidentiality can be adequately protected;

4. How data held on the new systems can and should be used for purposes other than the delivery of care e.g. clinical research; and
5. Current progress on the development of the NHS Care Records Service and the National Data Spine and why delivery of the new systems is up to 2 years behind schedule.

Although numerous responses (http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422we01.htm) have been received, one will consider the UK Information Commissioner's and the Foundation for Information Policy Research's responses in brief. The UK Information Commissioner was satisfied that the NHS could rely on one of the provisions provided under the UK Data Protection Act 1998 to process sensitive personal data in electronic health records.

> "The DPA requires, amongst other things, that any processing of personal data must be carried out in compliance with certain defined conditions. The DPA provides a number of possible conditions for the processing of sensitive personal data contained within electronic patient records. *One of these conditions is where the processing of sensitive personal data is necessary for medical purposes and is undertaken by a health professional or a person who owes a duty of confidence equivalent to that of a health professional*. The Information Commissioner is satisfied that the NHS can rely on this condition in order to process the sensitive personal data in electronic patient records. However, having established a proper basis for processing, the limitations attached to this basis must be complied with along with other aspects of the DPA most notably the eight data protection principles (see http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422we26.htm)."

By contrast, the Foundation for Information Policy Research (http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422we22.htm) were not convinced of having a centralised database of patient's medical data and were clear to point out the differences between the terms, "privacy" and "confidentiality". They made the following points:

> (Indent)"Electronic medical records already bring many benefits, via faster communications, better record availability, and reduced errors. However, the Committee should not confuse these benefits with the centralisation agenda.
>
> Centralisation is principally about power and control in the management of the health service. It is driven by the conflict between administrative convenience and professional autonomy. The Department seeks to resolve this conflict by controlling all information systems. The inevitable side-effects—mediocre systems and the destruction of patient privacy—would be severe. Patient trust in the medical profession will be undermined, and the Department would be

> vulnerable to challenges under European law. However, the strategy is not working, and is not likely to. It is time for it to be abandoned, and for CfH to return to providing the standards and infrastructure for interoperable systems, as its equivalents do elsewhere."

Given the differences in their views, the discussion over electronic health records are unlikely to be resolved, but I want to consider the views of the Art. 29 Working Party, which has issued guidelines on electronic health records (Working Party, 2007), aimed at harmonising patient rights on health records within the EU. The working document emphasised the importance of the European data protection framework and its application to electronic health records. Any data controller collecting personal information should adhere to general data protection principles including Art. 6 of the Data Protection Directive:

1. "Use limitation principle – the processing of personal data should not be incompatible to the purposes for which the data was obtained.
2. Data quality principle – this requires that data be accurate and up-to-date and data collected should follow Art. 6(1)(c) of the DPD.
3. Retention principle – personal data should not be kept longer than is necessary.
4. Information Requirements – data subjects are entitled to have access to their personal data by making a data subject access request to data controllers.
5. Data subject's right of access
6. Security related obligations – data controllers should ensure that they comply with Art. 17 of the DPD that technical and organisational measures are taken to protect the security of the personal information."

Furthermore, the Art. 29 Working Party was of the view that data contained in medical documentation, in electronic health records and in EHR systems should be considered to be "sensitive personal data"**.**

The Art. 29 Working Party also encouraged the use of privacy enhancing technologies (see http://www.petsfinebalance.com/agenda/presentations/PET-TextVersion.pdf and Art. 29 Working Party, 2005). Although the topic is beyond the scope of this chapter (see also Bygrave, 2002; European Commission, 2007), suffice it to state the European Commission has been proactive in looking at privacy enhancing technologies and has also funded two projects, PRIME and FIDIS (European Commission. *Privacy enhancing technologies* available at http://ec.europa.eu/information_society/activities/privtech/index_en.htm).

These are still ongoing, but systems that collect personal information would need to be robust and any electronic health system would have to look at the security of data held on systems (as distinct from privacy).

6. Concluding Remarks

The data protection laws have raised several issues pertinent to the medical profession. Not least, the application of the Data Protection Directive to anonymous, pseudonymous and genetic data and electronic health records. The challenges raised under the current European data protection framework and in particular, the UK's position, is how can this framework be utilised effectively, without hindering research and so forth. As a starting point, greater awareness is needed on the part of doctors, patients and researchers of what the Data Protection Directive 95/46/EC and its implementation in UK law entails. The UK Information Commissioner has been proactive in raising awareness of data protection laws. The distinctions drawn between ordinary and sensitive data under the Directive also means that stringent standards are placed when handling health data and thus, obtaining patients' informed consent will be paramount.

It has been a decade since the Data Protection Directive 95/46/EC was passed and tremendous progress has been made both at a European level and at a UK level, not least by the Art. 29 Working Party and the UK Information Commissioner. However, if there should be confidence in the current data protection framework, then the UK courts should first recognise the importance of the broad scope of "personal data" under the Data Protection Directive. Much work is still needed.

Bibliography

Legislation

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, 23.11.1995, 31.

UK Data Protection Act 1998

Articles and Books

Art. 29 Working Party. *Working document on genetic data*
adopted on 17 March 2004 available at
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp91_en.pdf

Art. 29 Working Party. *Opinion 4/2007 on the concept of personal data*, adopted on 20th June available at
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

Art. 29 Working Party. *Workinig Document on the processing of personal data relating to health in electronic health records (electronic health records)* adopted on 15 February 2007, WP131, available at
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf.

Art. 29 Working Party, *Working document on data protection issues related to RFID technology* available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf, Dated 19 January 2005.

Beyleveld, D. and D. Townend. "When is personal data rendered anonymous? Interpreting Recital 26 of Directive 95/46/EC" (2004) 6 *Med L Int* 73

Beyleveld, D. and E. Histed. "Betrayal of confidence in the Court of Appeal" (2000) *Med. L. Int*., 4(3/4), 277-311

Blume, P. *Nordic data protection law* (Iustus Forlag, 2001).

Bygrave, L.A. *Data protection law: approaching its rationale, logic and limits* (London: Kluwer, 2002).

Bygrave, L.A. "Privacy enhancing technologies – caught between a rock and a hard place" [2002] *PLPR* 55 available at http://www.austlii.org/au/journals/PLPR/2002/55.html.

Grant S Campbell. "Impact of the CSA judgment – more questions than answers?" *Privacy and Data Protection* (2008), 1 August 2008, 8(7) 14 8(7) 14.

Casabona, C.M.R. "Anonymisation and pseudonymisation: the legal framework" In: Beyleveld, D. (et. al). *Implementation of the Data Protection Directive in relation to medical research* (London: Ashgate, 2004), pp. 33-49.

Commission decisions on the adequacy of the protection of personal data in third countries (http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm), Last visited 29 June 2007.

Council of Europe Recommendation No. R(97)5) on the protection of medical data (http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/international_legal_instruments/Rec(97)5_EN.pdf), Last visited 20 November 2008.

Debate over legality of care record guarantee at http://www.e-health-insider.com/news/item.cfm?ID=2683

European Commission Project, PRIVIREAL available at http://www.privireal.org.

European Commission. *Privacy enhancing technologies* (http://ec.europa.eu/information_society/activities/privtech/index_en.htm), Last visited 20 November 2008.

Electronic health records for UK Government (http://www.infosys.com/industries/healthcare/cases/electronic_health_record_ukgov.asp), Last visited 25 June 2007.

The Electronic Patient Record and its use (http://www.parliament.uk/parliamentary_committees/health_committee/hcpn070205.cfm), Dated 5 February 2007.

European Commission. *Privacy enhancing technologies* available at http://ec.europa.eu/information_society/activities/privtech/index_en.htm.

EU Study on Implementation of the Data Protection Directive: comparative summary of national laws (http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf), Dated September 2002.

EuroSOCAP. *GPs threaten to snub NHS database* (http://www.eurosocap.org/News/?id=29). Dated 21 November 2006.

Evidence given to the Health Committee on the Electronic Patient Record, HC 422—ii , 10 May 2007 (http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/uc422-ii/uc42202.htm).

Evidence submitted by the Information Commissioner (http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422we26.htm), Dated 14 March 2007.

Evidence submitted by the Foundation for Information Policy Research (http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422we22.htm), Dated 15 March 2007.

Gertz, R. "Is it 'me' or 'we'? Genetic relations and the meaning of 'personal data' under the Data Protection Directive" (2004) 11 *European Journal of Health Law*, 231-244.

Health Committee (2007) *The Electronic Patient Record* HC422-1

House of Commons – written evidence at (http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422we01.htm).

Hughes, J. "Confidential information" (1999) *European Intellectual Property Review* 21(11) 194-195.

Klang, M. (2003) "Technology, Speech, Law & Ignorance – The state of free speech in Sweden", *Hertfordshire Law Journal*, 1(2), Autumn 2003, 48-63

Jay, R. & A. Hamilton. *Data Protection: Law and Practice*, 1st ed, London: Sweet and Maxwell, 1999

Laurie, G.T. *Genetic privacy: a challenge to medico-legal norms* (Cambridge: Cambridge University Press, 2002).

Leigh, D. & R. Evans. Warning over privacy of 50m patient files, *The Guardian*, 1 November 2006 available at http://www.guardian.co.uk/frontpage/story/0,,1936404,00.html

Lloyd, I.J. *Information technology law*, 4th ed, (Oxford: Oxford University Press, 2004).

Macqueen, H. L. "FoI wins over data protection" (2007) *Edin. L.R.* 11(2) 144-145.

Ploem, M.C. "Towards an appropriate privacy regime for medical data research" (2006) 13 *European Journal of Health Law* 41-64.

PRIVIREAL. *Recommendation around "explicit consent"* (http://www.privireal.org/content/recommendations/#Rece), Last visited 29 June 2007.

Simitis, S. *Revisiting sensitive data* (http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_by_experts/2Z-Report_Simitis_1999.asp#TopOfPage); Dated 1999.

UK Information Commissioner. *The 'Durant' Case and its impact on the interpretation of the Data Protection Act 1998* (http://www.informationcommissioner.gov.uk/cms/DocumentUploads/webversion%204%2004.10.042.pdf) Dated 4 October 2004.

Walden, I. "Anonymising personal data under European Law" In: Nicoll, C, J.E.J. Prins and M.J.M. van Dellen. *Digital anonymity and the law: tensions and dimensions*, 2003, 147-159.

Wong, R. "Data protection online: alternative approaches to sensitive data, (2007) *Journal of International Commercial Law and Technology* 2(1) 9-16.

Wong, R. "The shape of things to come: Swedish developments on the protection of privacy" (2005) 2:1 *SCRIPT-ed*, 98-113 (http://www.law.ed.ac.uk/ahrc/script-ed/vol2-1/wong.asp>