STATUTE LAW SOCIETY

Monday, 19 March 2012

The Data Protection Act 1998 & Personal Privacy

Philip Coppel QC

Synopsis: Described in *Campbell v MGN* [2003] QB 633 at [72] as "a thicket" and as "certainly a cumbersome and inelegant piece of legislation", the *Data Protection Act 1998* is the ugly relation in the law of privacy. As the *Human Rights Act 1998* has extruded the law of confidentiality to protect personal privacy, the *Data Protection Act 1998* has been largely relegated to a backup role: the coda to claims of symphonic complexity. Its occasional appearances in the law reports tell of maverick claims and paltry damages. If these discouraging outcomes are easily understood, the path there rarely is. The sophistication of the Act – both conceptually and practically – appears to have crippled its utility.

From the perspective of privacy law, the outcome is unfortunate. From the perspective of the statutory draftsman, the outcome is salutary. Clarity of object and of logic require more than precise prose. And yet, once understood, the *Data Protection Act 1998* provides the basis for the protection against intrusion upon privacy of record, making good the shortcomings of the common law.

Statute Law Society
21 Goodwyns Vale
London N10 2HA
Tel: +44 - 20 - 8883 1700

E-mail: statutelaw@aol.com

Institute of Advanced Legal Studies
Charles Clore House
17 Russell Square
London, WC1B 5DR

Introduction

On 2 February 1998 Lord Williams of Mostyn commenced his second reading speech for the *Data Protection Bill*:

> "I recognise that data protection does not sound like a subject to attract obsessive interest; witness the general exodus from your Lordships' House as I start to introduce this Second Reading. Data protection is redolent in many ways of computers and electronic processing: necessary but essentially technical providers of services. In fact it affects our well-being in a much more general way. It shares common ground to that extent with the Human Rights Bill. That Bill will improve the position of citizens of this country by enabling them to rely on the wide range of civil and political rights contained in the European Convention on Human Rights. Those rights include the right to respect for private and family life. The Data Protection Bill also concerns privacy, albeit a specific form of privacy; personal information privacy. The subject matter of the Bill is, therefore, inherently important to our general social welfare."[1]

As I penned this talk, with more than a decade having passed since Lord Williams's speech echoed in the House, I did wonder whether his words would similarly resonate tonight. A colleague told me that my topic was "anorak." I do not know exactly what he meant: but I did not understand it to be entirely complimentary.[2] Nevertheless, given that I have been asked to talk about it tonight, there is cause for hope.

The immediate difficulty lies in the title of the legislation. It suggests whirring machines with blinking lights, serviced by technicians in white

---

1 *Hansard*, House of Lords, 5th series, vol 585, col 436. Viscount Astor, who spoke next, gave the bill a "rather guarded welcome" (col 445), stating:

> "We need to protect the rights of individuals to privacy, but we do not need a back door privacy law."

Baroness Nicholson of Winterbourne (Lib Dem) was more supportive:

> "The kernel of the legislation — that is the meat of the Bill — seems to me a fresh attempt to create an oasis of individual privacy for each European Union citizen or resident in the face of the octopus of largely electronic knowledge..." (col 449).

Lord Williams reiterated his views in his keynote speech to the OECD global workshop on data protection, held 16-17 February 1998:
www.oecd.org/document/63/0,3343,en_2649_34255_1905855_1_1_1_1,00.html

2 In *Campbell v Mirror Newspapers Ltd* counsel for the defendant (Mr Desmond Browne) is reported to have likened the *Data Protection Act 1998* to "a thicket": [2002] EWHC 499 (QB) at [72]. Nobody in that case appears to have had a nice word for the Act. In the Court of Appeal, Lord Phillips expressed the view that "the Act is certainly a cumbersome and inelegant piece of legislation": *Campbell v MGN Ltd* [2002] EWCA Civ 1373, [2003] QB 633, [2003] 1 All ER 224 at [72].

dust coats. For many — practitioners and lay people alike — data protection is a dark hole; its strange concepts miring previously unhindered activities with needless complexities. That the immediate[3] source of these complexities is a European Directive only deepens the instinctive hostility.[4]

This is unfortunate. The legislation is a modest response to an important issue: protecting the privacy of recorded information relating to an individual.[5] While "privacy" captures the public imagination, "data

[3] "Immediate" because the Directive itself was the response to OECD guidelines on the protection of privacy and transborder flows of information: see Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted 23 September 1980, which can be found at:
www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
The OECD Guidelines set eight basic principles of national application which are immediately recognisable in the *Data Protection Act 1998*: (1) The collection limitation principle; (2) the data quality principle; (3) the purpose specification principle; (4) the use limitation principle; (5) the security safeguards principle; (6) the openness principle; (7) the individual participation principle; and (8) the accountability principle.

As the Hon Michael Kirby, the Australian judge who chaired the OECD expert group that formulated the OECD Guidelines on Privacy in 1978-1980, noted in his address to the OECD on the 30th anniversary of the Guidelines:

> "One normally thinks of the OECD as a body of sober economists, statisticians and technologists. One does not normally expect such people to be dripping with human rights sentiments. Generally speaking basic rights, the rule of law, and democratic governance are the broad assumptions upon which the OECD operates for the provision of technical advice and assistance, mainly on economic and technological issues....ordinarily, the OECD is not concerned with human rights protection. That task is generally left to other bodies. Yet the OECD Guidelines have proved to be one of the more effective international statements of recent times in affording protections for the basic human right of privacy, as that right has come to be understood in the context of contemporary information technology."

Based on his speech, Kirby subsequently published "The history, achievement and future of the 1980 OECD guidelines on privacy" *International Data Privacy Law*, 2011, vol 1, no 1, 6-14.

[4] It would be misplaced to found any hostility on the place from where the Directive sprouted. The Commonwealth Secretariat has promulgated a model privacy act, which bears more than a passing resemblance to the 1998 Act:
www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7B82BDA409-2C88-4AB5-9E32-797FE623DFB8%7D_protection%20of%20privacy.pdf
On 14 December 1990 the United Nations adopted guidelines on personal privacy:
www.ec.europa.eu/justice/policies/privacy/instruments/un_en.htm
In 1974 the United States passed a Federal Privacy Act:
www.justice.gov/opcl/privstat.htm

[5] In *Johnson v Medical Defence Union Ltd (No 2)* [2007] EWCA Civ 262, [2008] Bus LR 503 Buxton LJ said that "it is not easy to extract from this Directive [95/46/EC, of which the 1998 Act is a transposition] any purpose other than the protection of privacy.." (at [16]).

protection" somehow fails.

I am going to suggest that the *Data Protection Act 1998* is in fact all about protecting the privacy of recorded personal information, that it is capable of doing the job well, that it makes good the shortcomings of the common law in achieving that objective.[6] And, most important of all, that we should appreciate the worth of the Act by giving true effect to its terms.

The concept of privacy

I want to start by saying something about the notion of "privacy." We tend to think of discussion of the legal protection of "privacy" as a recent phenomenon. Those writing about it often pinpoint its conception to an article written by Samuel Warren and Louis Brandeis, published in 1890 by the *Harvard Law Review*.[7] They spoke of the "right to be let alone."[8]

While the title of their article may support that view, the protection of personal "privacy" had been at the centre of legal proceedings 40 years earlier in *Prince Albert v Strange*.[9] Prince Albert had sought an injunction to

[6] In his dissenting judgment in *Victoria Park Racing v Taylor* (1937) 58 CLR 479, Rich J (at 505) recognised that "protection against a complete exposure of the doings of the individual may be a right indispensible to the enjoyment of life."

[7] S. Warren and L. Brandeis, "The Right to Privacy", *Harvard Law Review*, vol. 4 (1890), p 193. Interestingly, it was from English case-law that they discerned an intention to protect personal privacy, relying on: *Prince Albert v Strange* (1849) 1 Mac & G 25 (41 ER 1171), as to which see below; *Abernethy v Hutchinson* (1825) 1 H & Tw 28 (47 ER 1313); *Pollard v Phonographic Co* (1880) 40 Ch D 345. They saw the problem as being one of the artificial use of existing causes to deal with privacy, when it was inevitable that they would not be able to cover all situations in which the law ought to recognise a wrong.

[8] Which phrase they credited Judge Cooley's *Torts*, 2nd ed, 1888, p 29. The "right to be let alone" is self-evidently a useless description of a right. It may go some way to explain the deployment of somewhat fluid concept of "privacy" to support preclusion of the state involving itself in a person's decisions relating to that person's body.

[9] (1849) 1 Mac & G 25 (41 ER 1171), (1849) 2 De G & Sm 652 (64 ER 293). De Gex & Smales's report is the more comprehensive. Prior to this, the courts had only intervened where there was a misuse or threatened misuse of confidential information that would have constituted an infringement by the defendant of a right of property recognised at common law, a breach of contract by the defendant, a breach of trust by the defendant, or a use of information obtained by the defendant from a third party in the knowledge that the third party was in breach of contract or trust. Warren and Brandeis

prevent Strange from publishing a catalogue which Strange had prepared, describing private etchings made by the Queen and Prince Albert "principally of subjects of private and domestic interest." Unknown to Strange at the time he prepared the catalogue, the copies of the etchings he had seen had been obtained without the artists' consent. It was not suggested that Strange's catalogue breached their copyright: he was simply describing what he had seen and what he hoped visitors would be able to see. Although Counsel for the Prince contended that property in the drawings had been had interfered with, he submitted that that interference was not essential to the argument mounted.[10] So it was that Strange's counsel submitted in reply:

> "So shadowy and evanescent is the nature of the right asserted by the Plaintiff that, in fact, there exists no form of action by which the claim can be substantiated....It cannot be submitted that privacy constitutes property, or that the Court will interfere to protect the owner in the enjoyment of it"[11]

Judgment for the plaintiff was squarely founded upon his having property in the sketches, such that (somehow) any catalogue listing them thereby impaired the property. Nevertheless, it was the breach of privacy which supplied the basis for the relief:

> "Where privacy is the right invaded, postponing the injunction would be equivalent to denying it altogether. The interposition of the Court in these cases does not depend on any legal right, and to be effectual, it must be immediate."[12]

We shall never know whether the Lady of Justice had a peek at the parties before deciding which way the scales should fall. In any event, over the next century and an half — until the advent of the *Human Rights Act 1998* — she never seemed to feel the same need to protect against invasions of personal privacy without requiring something more.[13] So it was that on 16

acknowledged the significance of *Albert v Strange*, relying on in it in support of their thesis.

10 2 De G & Sm 652 at 677-679 (64 ER 293 at 304-305).

11 1 Mac & G 25 at 33-35 (41 ER 1171 at 1174-5). Similarly, another passage in 2 De G & Sm 652 at 695 (64 ER 293 at 312).

12 1 Mac & G 25 at 47 (41 ER 1171 at 1179).

13 *Duchess of Argyll v Duke of Argyll and Others* [1964] Ch 302 comes perhaps closest. Although the Court required that there be confidentiality, once so satisfied it granted plaintiff an injunction to restrain the defendant, her former husband, from publishing

October 2003 Lord Hoffmann was able to declare in *Wainwright v Home Office*:

> "I would reject the invitation that since at the latest 1950 there has been a previously unknown tort of invasion of privacy."[14]

Arguably, the invasion of the Wainright's privacy was greater than that of Prince Albert.[15]

Meanwhile, in 1948 the United Nations had accorded privacy the status of a human right.[16] The 1960s saw the emergence elsewhere of the notion of privacy as a legal right.[17]

Identifying the moral or philosophical underpinning of the concept of privacy seems to have proven easier than the expression of a right with which to animate it. Thus, Cory J in the Canadian Supreme described privacy as a right which:

"secrets of the plaintiff relating to her private life, personal affairs or private conduct, communicated to the first defendant in confidence during the subsistence of his marriage to the plaintiff and not hitherto made public property."

14 [2003] UKHL 53, [2004] 2 AC 406 at [31]. This rejection of any basis for claim provided the European Court of Human Rights with the platform to find that the applicants did not have available to them a means of obtaining redress for the interference with their rights under Article 8 of the Convention: *Wainwright v United Kingdom* [2006] ECHR 807, (2007) 44 EHRR 809 at [55]. Lord Hoffmann's pronouncement is to be contrasted with *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804, where Laws J suggested (at 807) that the law recognised "a right to privacy, although the name accorded to the cause of action would be breach of confidence."

15 Where, in breach of prison rules, mother and son were strip-searched for drugs on a prison visit. The son, who was mentally impaired, was also poked in the armpit, his penis handled and his foreskin pulled back. The incident cause humiliation and distress, and the son suffered post-traumatic stress syndrome. The House of Lords held that there was no liability for the mother's of privacy. The battery of the son had at trial resulted in an award of £3,750, which the Court of Appeal reduced by £750 — schooled greater, maybe. Only Lord Scott of Foscote questioned this figure (at [60]-[61]).

16 Article 12 of the *Universal Declaration of Human Rights* (1948) provides: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks." Similarly, art 17 of the *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966.

17 For example: R. Prosser, "Privacy," *California Law Review*, vol 48 (1960), 383; E. Bloustein, "Privacy as an Aspect of Human Dignity", *New York University Law Review* vol 39 (1964), 962.

> "inheres in the basic dignity of the individual. This right is of intrinsic importance to the fulfilment of each person, both individually and as a member of society. Without privacy it is difficult for an individual to possess and retain a sense of self-worth or maintain an independence of spirit and thought."[18]

Lord Mustill attempted to define the essence of privacy as follows:

> "To my mind the privacy of a human being denotes at the same time the personal 'space' in which the individual is free to be itself, and also the caraspace, or shell, or umbrella, or whatever other metaphor is preferred, which protects that space from intrusion. An infringement of privacy is an affront to the personality, which is damaged both by the violation and by the demonstration that the personal space is not inviolate."[19]

One difficulty lies in translating these sentiments into the description of an enforceable right. In fact, "privacy" is not a unitary concept. The different types of interest encompassed within the concept doom any attempt to describe a single tort of privacy. Professor Prosser[20] noted in 1960:

> "The law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by a common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff....'to be let alone.'"[21]

Professor Prosser taxonimised "privacy" into four classes:

(1) an intrusion upon the plaintiff's physical solitude or seclusion (including unlawful searches, telephone tapping, long-distance photography and telephone harassment);

(2) a public disclosure of private facts;

(3) publicity putting the plaintiff in a false light; and

(4) an appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[22]

[18] *Vickery v Nova Scotia Supreme Court (Prothonotary)* [1991] 1 SCR 671 at 687.

[19] *R v Broadcasting Standards Commission, ex parte BBC* [2001] QB 885 at [48]. Phrases such as the "inherent dignity" or the "autonomy" of an individual have enjoyed a certain amount of judicial favour as the lemma upon which privacy law is founded: *Douglas v Hello! Ltd* [2001] QB 967 at [126] *per* Sedley LJ; *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 at [43].

[20] Dean of the College of Law at UC Berkeley from 1948 to 1961. Prosser authored several editions of *Prosser on Torts*, which, for a generation, was widely regarded in the USA as the leading work on the law of tort.

[21] "Privacy" *California Law Review*, vol 48, 1960, 383 at 389.

The taxonomy does not provide an ideal fit with English jurisprudence. It is partly shaped by the premium placed on free speech under the US Constitution.[23] It does, however, provide a useful starting point. It acknowledges that each of the different classes has a different focus and, because of that, different requirements.

For present purposes, I am principally concerned with the first two classes, but concentrating on the second. That is not because the third and fourth classes are of less importance. It is because the first two classes have fared worse in English jurisprudence.

The third class — publicity putting the claimant in a false light — may be seen to be protected through the law of defamation and injurious falsehood.[24] The fourth class — appropriation of the claimant's name for the defendant's advantage — may be seen to be protected through various intellectual property rights.[25]

I consider that Professor Prosser's first two classes of civil wrong can, with a little adaptation, be usefully maintained and re-labelled:

(1) Intrusion upon privacy of person.

(2) Intrusion upon privacy of record.[26]

[22] The classification has found its way into the *Restatement (Second) of Torts*, §§652A-652E, of which Prosser was one of the authors. The principles have been accepted by the US Supreme Court: *Time Inc v Hill* (1967) 385 US 374 at 383; *Cox Broadcasting Corporation v Cohn* (1975) 420 US 469 at 488.

[23] Generally the First Amendment will trump privacy.

[24] As in *Gordon v Kaye* [1991] FSR 62.

[25] For example, passing off. See, for example: *Irvine v Talksport* [2002] EWHC 367 (Ch), [2002] 2 All ER 414. It is, however of limited utility: see *Tolley v Fry* [1930] 1 KB 467 where Greer LJ held that the commercial exploitation of a man's name or photograph without his consent is not by itself tortious. This was not discussed when the matter went to the House of Lords: [1931] AC 333.

[26] Others have termed this "information privacy." Since we are only concerned with recorded information (whatever form that record may take) and since "information" is a slippery term (at least at the edges), I prefer "record." See, also, *Goodwin v NGN Ltd* [2011] EWHC 1437 (QB) at [85], where Tugendhat J refers to these classes as "intrusion"

What do I mean by each? By "privacy of person" I largely mean what Professor Prosser put into his first class: the intrusion upon the claimant's physical solitude or seclusion. That requires, of course, identification of those matters about which and those places in which an individual can legitimately expect to be "let alone." It also requires identification of the types of intrusion into those matters and places which are unacceptable. To a considerable extent, the first has been the subject of legislative activity. Unlawful searches, telephone tapping and the like are now covered by a complex regime of statutory provisions which recognise the need for some control.[27] Further protection is given by the *Protection from Harassment Act 1997*.[28]

Intrusion upon privacy of person is concerned with more than just spying and prying. Properly described, such a right would not be indifferent to an intrusion such as that endured by Wainright mother and son. There are certain facets of an individual which, in a civilised society, demand and are generally afforded respect. It is an atrophied common law which is unable to adapt to meet such an obvious civil wrong.

I am not, however, today going to concentrate on "privacy of person." I

and "confidentiality" respectively.

27 Most notably:
(1) *Regulation of Investigatory Powers Act 2000*, and the regulations thereunder, including *Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003* (SI 2003/3171); *Regulation of Investigatory Powers (Communications Data) Order 2003* (SI 2003/3172); *Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002* (SI 2002/1931); *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000* (SI 2000/2699).
(2) Part III (ss 91-108) of the *Police Act 1997*, dealing with authorisations for police, HMRC and cognate bodies to interfere with property or "wireless telegraphy" for certain purposes. The Act introduced a scheme whereby, for the first time, the police, HMRC and cognate bodies (but not the intelligence services) were required to apply for prior authorisation before embarking on covert surveillance involving entry onto or interference with property or wireless telegraphy without the consent of the owner.

28 At to which, see: *Thomas v News Group Newspapers Ltd* [2001] EWCA Civ 1233, [2002] EMLR 78; *Feguson v British Gas Trading Ltd* [2009] EWCA Civ 46, [2010] 1 WLR 785; *Majrowwski v Guy's and Thoams' NHS Trust* [2006] UKHL 34, [2007] 1 AC 224; *S&D Property Investments v Nisbet* [2009] EWHC 1726 (Ch); *Potter v Price* [2004] EWHC 781 (QB).

introduce it in order to draw it as a separate class of "privacy" with its own constituent elements, with its own defences and with its own heads of damage. These are truly distinct from those involved with an intrusion upon privacy of record. It is only by recognising the separate classes, with their distinct requirements and characteristics, that a coherent law of "privacy" can be described and developed.

That it deserves to develop[29] cannot, I would suggest, be sensibly gainsaid.[30] The failure of the common law to adequately protect privacy stems, in no small part, from its preoccupation with property as the *de facto* touchstone of the matters with which it will concern itself. If a matter can be transubstantiated into property — intellectual property, incorporeal hereditaments, choses in action and so forth — then all is well. However, if a matter cannot be so conceived — such as pure personal privacy — then the common law finds it more difficult to be bothered.[31]

Thus the common law is rich with principles that can protect the ownership of an A4 sheet of paper, regardless of its content – if any. However, that same law can do little to protect against an intrusion upon personal privacy effected through that sheet of paper.[32] On the other hand, if the intrusion

29 Brian Neill, "The Protection of Privacy," *Modern Law Review*, vol 25 (1962), pp 393-405 remains prescient, anticipating the significance of Art 8(1) of the ECHR: see p 401, fn 48. It followed a string of articles to similar effect, including: Winfield, "Privacy" (1931) 47 LQR 23. Similarly: T. L. Yang, "Privacy: A Comparative Study of English and American Law" (1966) 15 *ICLQ* 175.

30 In *Monson v Tussauds Ltd* [1894] 1 QB 671 at 687 Lord Halsbury thought that some protection against the disclosure of a man's private life was desirable.

31 I do not comment on whether confidential information is or is not a species of property. This has been described as "perhaps the most sterile of the debates which have arisen around the subject of information received in confidence": P. Finn, *Fiduciary Obligations*, Law Book Co, 1977, §293.

32 Hence *Kaye v Robertson* [1991] FSR 62, where a journalist and photographer gained access to a hospital room where a television star was recuperating having suffered serious injuries from being struck by a tree branch. As a result of his injuries, the star was unable to consent to the interview or being photographed. He sought to restrain publication based on trespass to the person, defamation, passing off and malicious falsehood. Although an interlocutory judgment was granted on the basis that it was a malicious falsehood to claim that the star had given his consent, the Court of Appeal made it clear that the English common law did not recognise a right to privacy (see esp

touches upon a property interest, then the common law will come to the rescue.[33]

More recently, the law of confidentiality has been pressed in such a way as to protect private information.[34] Thus:

> "As the law has developed breach of confidence, or misuse of confidential information, now covers two distinct causes of action, protecting two different interests: privacy, and secret ('confidential') information. It is important to keep these two distinct."[35]

With only the name of confidentiality to unite the two distinct causes, it was

at 154).

[33] Usually that is supplied by finding a breach of confidentiality. However, as noted in *Philip v Pennell* [1907] 2 Ch 577 the confidence does not run with the paper. Kekewich J hinted that a person's private life might constitute a saleable commodity, at least if the individual was well-known (at 589). It can, of course, also be supplied by a contract, as in *Pollard v Photographic Co* (1888) 40 Ch D 345, where a commercial photographer was commissioned to take photographs of the Pollard family, and started selling prints of Mrs Pollard as a Christmas card. Although earlier cases had found that overlooking real property could be actionable (*Cherrington v Abney* (1709) 2 Vern 646; *Chandler v Thompson* (1811) 3 Camp 80), this was rejected in *Tapling v Jones* (1865) 11 HLC 290.

[34] This was facilitated by two developments in the law of confidentiality. First, that the necessary quality of confidence was not limited to trade or business secrets, but could extend to personal information, which was extended from the secrets of a marital relationship (*Duchess of Argyll v Duke of Argyll* [1967] Ch 302) to any sexual relationship (*Stephens v Avery* [1988] Ch 449). The second was that the obligation of confidence was not restricted to the original confidente, but could also extend to third parties into whose hands the confidential information came (*A-G v Guardian Newspapers (No. 2)* [1990] 1 AC 109 at 281). Using these two developments, the courts showed themselves prepared to act where the media had surreptitiously acquired information that they knew or ought to have known was secret. It was the surreptitious conduct that evidenced knowledge that the information being acquired was confidential (*Shelley Films Ltd v Rex Features Ltd* [1994] EMLR 134; *Creation Records Ltd v News Group Newspapers Ltd* [1997] EMLR 444; *Hellewell v Chief Constable of Derbyshire* [1995] 4 All ER 473. The explicit recognition that the law of confidentiality could be used to protect personal privacy can be seen with *Earl Spencer v United* Kingdom (1998) 25 EHRR CD 105. Subsequently, see: *Wainwright v Home Office* at [28]–[30]; *Campbell v MGN Ltd* [2004] UKHL 22,[2004] 2 AC 457 at [11]–[22], [43]–[52], [85]–[86], [105]–[113], [132]–[141] and [166]–[167]; *Re S (A Child)* [2004] UKHL 47, [2005] 1 AC 593, [2004] 4 All ER 683; *McKennitt v Ash* [2008] QB 73; *HRH Prince of Wales v Associated Newspapers Ltd* [2006] EWCA Civ 1776, [2008] Ch 57, [2007] 2 All ER 139; *Lord Browne of Madingley v Associated Newspapers Ltd* [2008] QB 103; *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB), [2008] EMLR 20; *Inerman v Tchenguiz* [2010] EWCA Civ 908, [2011] Fam 116 at [67], [76], [79] and [144].

[35] *OBG Ltd v Allan* [2007] UKHL 21, [2008] 1 AC 1 at [255] *per* Lord Nicholls of Birkenhead.

likely that "privacy" would ultimately wriggle free from the taxon out of which it was fashioned. Thus, by 2009, the break had been made:

> "It has come to be accepted, under the influence of human rights instruments such as article 8 of the European Convention, that the privacy of personal information is something that is worthy of protection in its own right....human rights law has identified private information as something worth protecting as an aspect of human autonomy and dignity."[36]

With that, I want to return to the ugly relation in all this — data protection. Apart from the occasional proceeding,[37] it has remained very much in the background in the higher courts. Claims under it have attracted a particular judicial vitriol.[38]

It deserves better. Its immediate handicap — its abstraction and adherence to concepts — is its ultimate strength. It is these which give it the ability to logically and consistently work through problems, yielding answers that fairly accommodate competing interests. It does so in a way that is consistent with the requirements of the European Convention on Human Rights. Bear with me for just a few minutes so that I can give a glimpse of its potential for the "law of privacy."

I start with the glossary that is at the heart of the *Data Protection Act 1998*. "Data" more-or-less means information recorded otherwise than by pen or pencil.[39] Any information within a computer is data, whether words or an

[36] *In re British Broadcasting Corporation* [2009] UKHL 34, [2010] 1 AC 145 at [18] *per* Lord Hope of Craighead.

[37] Thus, in the House of Lords: *Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47, [2008] 1 WLR 1550 (a freedom of information case); *R v Brown* [1996] 1 AC 543 (dealing with computer misuse). In *Campbell v MGN Ltd* [2002] EWHC 499 Morland J had judgment, with damages and an injunction, on the basis of both breach of confidence and breach of the duty under section 4(4) of the *Data Protection Act 1998*. By the time the matter it got to the House of Lords, it had been agreed that it "added nothing to the claim for breach of confidence": [2004] UKHL 22, [2004] 2 AC 457 at [130]. The remark is revelatory.

[38] *Durant v FSA* [2003] EWCA Civ 1746, [2004] FSR 28. In fact, because of s 40 of the *Freedom of Information Act 2000* the holdings have turned out to be something of an own goal for the successful party. Whether, after *Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47, [2008] 1 WLR 1550, all of *Durant v FSA* remains good law is doubtful.

[39] See the extracts at the end of this paper.

image.[40] So, too, pictures on a digital camera and voice recordings. "Personal data" means (more-or-less) any such data which relate to a live individual.[41] "Processing" means pretty much any use you might care to imagine: organising, retrieving, using, copying, disseminating, erasing and much else,[42] just provided that it is not done by pen and paper.[43] So we immediately see that whilst labelled the "Data Protection Act," it might just as easily have been labelled the "Use of Personal Information Act."

Next I must introduce the "data controller."[44] This is the person who decides what is to be done with the information.[45] The Act recognises that the data controller may not actually hold the information over which he has control: that may be left with someone the Act calls the "data processor."[46] But, the more important of the two is the data controller. If he does not also hold the information, he is in charge of it. Apart from those introduced, the Act labels everyone else a "third party."[47]

40 Of course, computers hold information in binary form, often compressed through algorithms, which, in raw form, no-one would recognise as a word or image. The complexity of the Act's definition of data accommodates this.

41 See the extracts at the end of this paper.

42 See the extracts at the end of this paper.

43 See, generally *Johnson v Medical Defence Union Ltd (No 2)* [2007] EWCA Civ 262, [2008] Bus LR 503. The Court of Appeal in *Campbell v MGN Ltd* [2002] EWCA Civ 1373, [2003] QB 633, [2003] 1 All ER 224 at [107] rejected an argument that processing did not include putting data into print:

> "...where the data controller is responsible for the publication of hard copies that reproduce data that has previously been processed by means of equipment operating automatically, the publication forms part of the processing and falls within the scope of the Act."

This was contained by the Court of Appeal in *Johnson v Medical Defence Union Ltd (No 2)* [2007] EWCA Civ 262, [2008] Bus LR 503 at [39]-[43], where it drew a distinction between publication of information that has already been automatically processed (which is captured by the Act) and the manual analysis of data before any automated processing begins (which is not).

44 See the extracts at the end of this paper.

45 The definition is, of course, rather more carefully thought through than that. See: www.ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

46 See the extracts at the end of this paper.

47 Section 70(1).

The Act recognises that some personal information is more sensitive than others: racial or ethnic origin, political opinions, religious beliefs, physical or mental health, sexual life, criminal convictions and so forth. These are labelled "sensitive personal data."[48] Thus, photographs of Naomi Campbell leaving Narcotic Anonymous constituted "sensitive personal data" because they were information relating to her physical or mental health or condition.[49] The photographs were also sensitive personal data because they consisted of information relating to her racial or ethnic origin.[50] So, too, photographs of the 2 year-old son of JK Rowling.[51]

How does it work to protect against intrusions into personal privacy? As a piece of legislation, one of the shortcomings of the *Data Protection Act 1998* is that the order of its provisions bears no relationship to the logical sequence to establish liability for a breach of privacy. The latter requires the following steps in the following order:

(1) Is the conduct complained of "processing" by a "data controller" of "personal data" of the would-be claimant? We may go further and ask whether the data concerned is "sensitive personal data." This involves working through the definitional provisions just discussed.

(2) If "yes" to (1), has the data controller complied with the "data protection principles"? We shall consider what these mean in a moment, but this involves delving into the first three schedules to the Act.

(3) If "no" to (2), do any of the exemptions in Part IV (ss 27 - 39) apply?

(4) If "no" to (3), there will have been a breach of the statutory duty

48 See the extracts at the end of this paper.

49 *Campbell v Mirror Group Newspapers* [2002] EWHC 499 (QB) at [87].

50 *Campbell v Mirror Group Newspapers* [2002] EWHC 499 (QB) at [85].

51 *Murray v Express Newspapers plc & anor* [2007] EWHC 1908 (Ch) at [80]. This part of the judgment would appear to be undisturbed by the appeal: *Murray v Express Newspapers plc & anor* [2008] EWCA Civ 446, [2009] Ch 481 at [62]-[63].

created by s 4(4) and it will be necessary to quantify the loss and distress, as well as consider other forms of relief. All this is dealt with in ss 13 -14.

I turn, then, to the data protection principles.[52] Schedule 1 to the Act spells out eight data protection principles. Each data controller is under a duty to comply with these data protection principles in relation to all personal data held by him.[53] We will come to these principles and the exemptions in a second, but what should be noted is that contravention of them is actionable by the data subject. Their contravention gives rise to a private law claim which the data subject may bring against the data controller.

In one sense the data protection principles can be seen to be setting the yardstick against which to measure the acceptability of particular intrusions into personal privacy. This systematic consideration of intrusiveness by type and by degree gives the Act a sophistication which is well advanced on that which one finds in privacy case-law. To identify something as "private" and to find that someone has touched it are only the first half of what is needed to give rise to civil wrong founded upon privacy. The second half must involve an analysis of what the malefactor has done with the "private information" — or how the "personal data" has been "processed," if you will.

There are, as I have mentioned, eight data protection principles. Interest usually focusses on the first data protection principle, but it is important to remember that a data controller must comply with all of them. The first data protection principle has a three-fold obligation. It requires the data controller to process personal data fairly, to process it lawfully and to ensure that at least one of six conditions is met.

What is meant by "fairly" is spelled out in Part II of Schedule 1. Basically, fair processing requires that it be with the data subject's consent, if practical.[54] The detail of what is and what is not fair processing is spelled

[52] See the extracts at the end of this paper.

[53] See the extracts at the end of this paper. Section 27 introduces the exemptions in Part IV of the Act (ss 27-39 and Sch 7).

[54] The conclusion in *Murray v Express Newspapers plc & anor* [2007] EWHC 1908 (Ch) at [73]-[74] that covert, non-consensual photography is fair if it does not involve a deception would appear not to have survived the appeal: *Murray v Express Newspapers plc & anor* [2008] EWCA Civ 446, [2009] Ch 481 at [62]-[63].

out in Part II of Schedule 1.[55]

"Lawful" means not in contravention of the law. The conditions for the third requirement are set out in Schedule 2.[56] These six conditions all recognise that there are other interests that must be balanced against the data subject's rights. Schedule 2 enumerates these interests and how they are to be taken into account in striking that balance. Importantly, the interests described and the way in which they are to be taken into account embodies the relevant strictures of the European Convention on Human Rights, in particular arts 8 and 10. This makes it generally unnecessary to bolt on a consideration of the *Human Rights Act 1998*. As a corollary, the faithful application of the first data protection principle gives effect to human rights principles as they apply to the use of personal information.

I have already introduced the definition of sensitive personal data. Consistent with the Act's understanding of the need to assess intrusiveness, the first data protection principle requires that processing of sensitive personal data also satisfy of one of the conditions in Schedule 3.[57]

The Act has the sophistication to recognise that some facets of an individual's personal life are intrinsically more private than others. It tunes the level of intrusion to require either explicit consent or a more pressing justification for the particular processing. Here again it gives effect to human rights principles as they apply to the use of personal information.

Data protection principles 2 to 5 are, broadly speaking, directed to securing proportionality in the processing of the data. Temporality features in principles 3 and 5; accuracy features in principle 4. Data protection principle 8 introduces geographical limits.

A further layer of sophistication is added by the exemptions in Part IV of

[55] See extracts at the end of this paper.

[56] See extracts at the end of this paper.

[57] See extracts at the end of this paper.

Act. These disapply certain, but not all, data protection principles (or parts of them) according to the exemption and according to the circumstance.[58] I shall not try to summarise them here. The exemptions relate to a conventional mix of class-based and prejudice-based protected interests (crime and taxation, legal professional privilege, and so forth). What is unusual is that applicability of an exemption does not disapply all the data protection principles: just those necessary to accommodate the legitimate objects of the protected interest.

There is one particular exemption that deserves greater consideration. The Act terms journalism, artistic purposes and literary purposes as "special purposes."[59] The Act creates an exemption from most of the data protection principles to cover processing of personal data processed for the special purposes. This is not, however, a pure class-based exemption. Rather, its engagement demands a reasonable belief on the part of the data controller that:

> "...having regard...to the special importance of the public interest in freedom of expression, publication would be in the public interest....and....that in all the circumstances compliance with [the data protection principles] is incompatible with the special purposes."[60]

Once again the Act accords recognition to the special role of the Press, at least to the extent that their activities are in the public interest. Whilst the exemption does leave the important judgment calls to the data controller (e.g. the newspaper concerned), it is tempered by each of the beliefs having to be reasonable and involving a balancing of interests.[61]

In *Campbell v MGN Ltd*[62] the Court of Appeal gave the exemption a very

58 The definitions in s 27 are important, if not all that informative.

59 See the extracts at the end of this paper.

60 See the extracts at the end of this paper. The provisions apply both pre and post-publication: *Campbell v MGN Ltd* [2002] EWCA Civ 1373, [2003] QB 633, [2003] 1 All ER 224 at [121]. The designated codes of practice are set out in SI 2000/1864.

61 The section creates a procedural bar so as to stop gagging injunctions against the Press. A claimant must await publication before commencing proceedings: *Campbell v MGN Ltd* [2002] EWCA Civ 1373, [2003] QB 633, [2003] 1 All ER 224 at [117].

62 [2002] EWCA Civ 1373, [2003] QB 633, [2003] 1 All ER 224. This part of the Court of Appeal's judgment did not form part of the appeal to the House of Lords.

wide reading in order to conform with its own ideas about data protection:

> "The overall scheme of the Directive and the Act appears aimed at the processing and retention of data over a sensible period. Thus the data controller is obliged to inform the data subject that personal data about the subject have been processed and the data subject is given rights, which include applying under s 14 for the rectification, blocking, erasure or destruction of the data on specified grounds. These provisions are not appropriate for the data processing which will normally be an incident of journalism.
>
> This is because the definition of processing is so wide that it embraces the relatively ephemeral operations that will normally be carried out by way of the day-to-day tasks, involving the use of electronic equipment, such as the lap-top and the modern printing press, in translating information into the printed newspaper. The speed with which these operations have to be carried out if a newspaper is to publish news renders it impractical to comply with many of the data processing principles and the conditions in Schedules 2 and 3, including the requirement that the data subject has given his consent to the processing.
>
> Furthermore, the requirements of the Act, in the absence of s 32, would impose restrictions on the media which would radically restrict the freedom of the press. Arguably, but in individual cases the argument would be likely to be intense, condition 6(1) of Schedule 2 might enable the lawful processing of personal data that was not sensitive, but the requirement to satisfy a condition in Schedule 3 would effectively preclude publication of any sensitive personal data, for the result would be a string of claims for distress under s 13. There would be no answer to these claims, even if the publication in question had manifestly been in the public interest."[63]

The reasoning flips the logic of the Act on its head. The Act recognises that it is the ease and speed with which personal data can be processed (including disseminated, linked to other personal information or otherwise used, all without the subject's knowledge) that facilitates the intrusiveness upon personal privacy. With the Court of Appeal having snuffed out the data protection claim, the need to wring some sort of right out of the law of confidentiality re-asserted itself. On analysis, it is not easy to see why the facts in *Campbell v MGN Ltd* were better accommodated by a claim for breach of confidentiality than by a claim for breach of the *Data Protection Act 1998*.[64]

63 At [122]-[124].

64 The outcome is particularly unfortunate, as the power of the Information Commissioner to issue an enforcement notice under s 40 is largely disapplied where the processing of personal data is for the "special purposes" (see s 3, set out at the end of this paper): ss

One of the difficulties with imposing a liability upon a person holding recorded personal information about someone else is that the person holding the information may quite easily be unaware of the sensitivity of the subject to the information being held and otherwise dealt with. Section 10 of the Act anticipates the difficulty, allowing a data subject in certain circumstances to notify a data controller to desist from processing information in which he is the data subject. With certain limitations, a data subject can give such a notice on the ground that the processing of the data is causing or would be likely to cause substantial damage or distress to him and that that damage or distress is unwarranted.[65] The data controller then either counters with a notice stating that he has complied with the request or, alternatively, that he considers the request completely or partially unjustified.[66] If there has been non-compliance, the Act confers a free-standing right to commence proceedings to order compliance.[67]

Next, I want to turn more conventional claims for breach of the obligations under the Act. The Act specifically provides that an individual who suffers damage as a result of any contravention by a data controller of the requirements of the Act is entitled to compensation from the data controller for that damage.[68] The Act also provides that distress is compensable, but only as a supplement to free-standing damage or where the processing complained about was for one of the special purposes (*i.e.* journalism, or artistic or literary purposes). Claims may be brought in a county court or

40(10) and 46(3). The special information notice procedure (s 44) fundamentally differs from s 40, both in its scope and in its consequences. Practice has shown it to be worthless.

65 See the extracts at the end of this paper.

66 See the extracts at the end of this paper.

67 Section 10(4), which provides:
"If a court is satisfied, on the application of any person who has given a notice under subsection (1) which appears to the court to be justified (or to be justified to any extent), that the data controller in question has failed to comply with the notice, the court may order him to take such steps for complying with the notice (or for complying with it to that extent) as the court thinks fit."

68 See the extracts at the end of this paper.

in the High Court.[69]

This all sounds fair enough. The practice and principles have been otherwise. In practice, until very recently the amounts of damages awarded have been minuscule, easily eclipsed by the costs of the proceedings. Thus, Naomi Campbell, in addition to her claim for "breach of confidence and/or invasion of privacy," included a claim to compensation under the 1998 Act. At first instance, she was awarded £2,500 on alternative bases for the two causes.[70] Mr Justice Morland held that "damage" meant special or financial damages in contra-distinction to distress in the shape of injury to feelings.[71] He held that aggravated damages were available, and added £1,000 for that.[72] Of course, her 1998 Act claim was ultimately defeated, spurring her on with her claim for breach of confidentiality. Mr Michael Douglas and Ms Zeta-Jones did not so fare so well in their trial. They received £50 damages under s 13.[73]

What underlies this is an insistence on treating an intrusion upon personal privacy by reference to the principles by which wrongs to property are measured. These — unsurprisingly — often result in a diminution in the value of that property. The damage effected by the baring of an individual's details, however degrading, is not so measurable. That nakedness is not shared by inanimate things, and so for them is not "damage." Thus, Buxton LJ felt able to say:

> "There is no compelling reason to think that 'damage' in the Directive has to go

69 Section 15(1).

70 *Campbell v Mirror Group Newspapers* [2002] EWHC 499 (QB). The Data Protection claim was overturned in the Court of Appeal on the basis that the s 32 exemption had been made out: *Campbell v MGN Ltd* [2002] EWCA Civ 1373, [2003] QB 633, [2003] 1 All ER 224 at [138].

71 *Campbell v Mirror Group Newspapers* [2002] EWHC 499 (QB) at [123].

72 *Campbell v Mirror Group Newspapers* [2002] EWHC 499 (QB) at [161].

73 *Douglas & Ors v Hello! Ltd & Ors* [2003] EWHC 786 (Ch), [2003] 3 All ER 996 at [239]. On appeal, to the evident relief of the Court of Appeal, the DPA claim was not considered: *Douglas & Ors v Hello Ltd & Ors* [2005] EWCA Civ 595, [2006] QB 125, [2005] 4 All ER 128.

beyond its root meaning of pecuniary loss."[74]

Only if:

> "..a party could establish that a breach of the requirements of the Directive had indeed led to a breach of his article 8 rights, then he could no doubt recover for that breach under the Directive, without necessarily pursuing the more tortuous path of recovery for a breach of article 8 as such."[75]

The so-called "root meaning" only acknowledges things of marketable worth. Personal privacy — like life, limb and liberty — cannot be bought or sold in the marketplace. The law of damages is not so myopic.[76]

Having crippled the Act with restrictive readings of key rights[77] and expansive readings of key exemptions, the prosthetic of Article 8 has been bolted on: just enough to enable the Act to hobble to Convention compliance.[78] The Act does not need this. Its language is naturally Convention compliant. Its structure and the considerations placed within that structure are an embodiment of Convention principles. It is only when dismembered that devices are needed to make it compliant.

The less tortuous path is to read s 13, and the rest of the Act, in a way which is consistent with Article 8 and with the object of the Act.[79] The

74 *Johnson v Medical Defence Union Ltd (No 2)* [2007] EWCA Civ 262, [2008] Bus LR 503 at [74]. The passage, like much else in the judgment, is *obiter*. In fact, there is nothing to suggest that this is its "root meaning" and there much authority to suggest that it has long grown out of any such grounding: *Hobbs v London & SW Rly Co* (1875) LR 10 QB 111 at 117; *Rookes v Barnard* [1964] AC 1129 at 1221; *Jarvis v Swan Tours Ltd* [1973] QB 233; *Farley v Skinner* [2002] 2 AC 732.

75 *Johnson v Medical Defence Union Ltd (No 2)* [2007] EWCA Civ 262, [2008] Bus LR 503 at [74].

76 "The function of an action of damages is to provide a remedy for interests that are recognised by the law as entitled to protection. Obvious examples are protection against injury to the person, to reputation and to privacy": *HMRC v Total Network SL* [2008] UKHL 19, [2008] AC 1174 at [26] *per* Lord Hope of Craighead.

77 Most notably s 13.

78 And save the domestic courts from rebuke elsewhere.

79 Lod Phillips of Worth Matravers MR stated in *Campbell v Mirror Group Newspapers* [2002] EWCA Civ 1373, [2003] QB 633 633 at [93] said:

> "In interpreting the Act it is appropriate to look to the Directive for assistance. The Act should, if possible, be interpreted in a manner that is consistent with the Directive. Furthermore, because the Act has, in large measure, adopted the wording of the Directive, it is not appropriate to look for the precision in the use of language that is usually to be expected from the parliamentary draftsmen. A purposive approach to making sense of the provisions is called for."

extent to which a data controller has departed from the Act's requirements — through the character of the personal data processed, the impropriety of the processing and the duration of that processing — supplies the primary measure of intrusion upon privacy and of the damage to that privacy that an individual thereby suffers.[80] The corollary of non-economic loss not being susceptible of measurement in money[81] is that an absence of monetary loss is not indicative of an absence of non-economic loss. On analysis, compensation under s 13(1) can be seen to be independent of the individual's reaction to the contravention, whereas compensation under s 13(2) is entirely dependent upon that reaction. The latter recognises that an individual's degradation, humiliation and sense of violation are all forms of distress that can be suffered by an individual from an intrusion upon his or her personal privacy: or, if you would, from a breach of the data protection principles.[82] These do not require a physician to be recognised.[83] They are readily understandable, unwanted human reactions to any form of forced,

80 Thus, processing that complies with all the data protection principles but which is carried out by a data controller who is not registered will not cause an individual to suffer damage.

81 In the words of Lord Diplock in *Wright v British Railways Board* [1983] 2 AC 773 at 777C

82 This is no different from an award for non-pecuniary damage in a personal injury claim. In *West v Shephard* [1964] AC 326 at 357 Lord Devlin thought that the fair sum was the amount which would allow the wrongdoer to "hold up his head among his neighbours and say with their approval that he has done the fair thing."

83 The law conventionally only compensates distress where there is something "ascertainable by the physician:" *Behrens v Betram Mills Circus* [1957] 1 QB 1; *Bourhill v Young* [1943] AC 92 at 103. Similarly: *Johnson v Unisys Ltd* [2003] 1 AC 518 at [44] (HL). By this is meant that the distress must have induced a recognised illness. However, where distress is caused by a breach of contract and an important object of a contract is to provide pleasure, relaxation, peace of mind or freedom from molestation, then it will compensate for distress (without requiring it to be part of or bring on a recognisable illness): *Jarvis v Swans Tours Ltd* [1973] QB 233; *Watts v Morrow* [1991] 1 WLR 1421 at 1445F; *Farley v Skinner* [2002] 2 AC 732 at [24]; *Johnson v Unisys Ltd* [2003] 1 AC 518 at [70]. Extended by analogy to a gratuitous bailment: *Yearworth and others v North Bristol NHS Trust* [2009] EWCA Civ 37, [2010] QB 1.

public exposure of private matters.[84]

Properly understood, the *Data Protection Act 1998* does provide an adequate system for the protection against intrusion upon privacy of record. Properly applied, it saves the need for bending the law of confidentiality to remedy the obvious wrongs that have spawned a "law of privacy." The Act has a sophistication which is not going to be matched by the fits and starts of the developing common law.

Of late, there has been the start of a change of attitude.[85] In *Murray v Express Newspapers plc & anor*[86] the High Court had struck out a privacy claim founded on the *Data Protection Act 1998*. After repeating that "damage under s 13(1) means ordinary pecuniary loss,"[87] the High Court went on to reject the notion of restitutionary damages.[88] The Court of Appeal held that there was a viable breach of confidence claim, and the majority of its judgment is devoted to that.[89] In the coda to its judgment, the Court of Appeal similarly allowed the data protection appeal, Sir Anthony Clarke MR concluding:

> "...we do not think that the claims under the *Data Protection Act 1998* should be struck out, whatever the conclusions of fact may be. They seem to us to raise a number of issues of some importance, including the meaning of 'damage' in section 13(1) of the *Data Protection Act 1998*. It seems to us to be at least arguable that the judge has construed 'damage' too narrowly, having regard to the fact that the purpose of the Act was to enact the provisions of the relevant directive. All these issues should be authoritatively determined at a trial."[90]

84 It is no answer to say some people might feel unashamed by or even wish such publicity.

85 In any event, it is quite possible that the next Directive on Data Protection, informed by the readings of the implementation of the current Directive, will widen the scope for damages, enabling claims to be brought by organisations on behalf of individuals:
www.ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf
www.ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

86 [2007] EWHC 1908 (Ch), Patten J. The claimant was the 2 year-old infant son of his litigation friends, Dr Neil Murray and Mrs Joanne Murray (better known as JK Rowling and the author of Harry Potter books). The second defendant was a photographic agency. Using a camera with a high-powered telephoto lens, it had covertly taken pictures of him whilst being pushed in a buggy in a public street. The parents were unaware of his being photographed and they did not consent. The pictures were subsequently published in the *Sunday Express* magazine under the headline "My Secret." with what were said to be the thoughts of his mother on motherhood and family life. The public interest in publication of all this does not appear in the reported judgments.

87 At [89].

88 At [90].

89 *Murray v Express Newspapers plc & anor* [2008] EWCA Civ 446, [2009] Ch 481.

More recent events should compel us to re-examine the *Data Protection Act 1998* and its application. The wide, self-regulatory reading given to the section 32 press exemption just 10 years ago in *Campbell v MGN Ltd*[91] no longer seems connected to reality. "Radically restricting the freedom of the press"[92] to protect privacy does not ring with the same conviction it did then. That there would be "no answer to these claims" seems an attractive, rather than a repellant, proposition. Incantation that "the publication had manifestly been in the public interest" no longer has the talismanic effect it once did. So, too, awarding £50 in damages to Mr Michael Douglas and Ms Zeta-Jones[93] for the breach of the 1998 Act seems out of touch. It bears no relationship with recently reported settlements for press breaches of privacy. The conduct is, after all, much the same, whatever the appellation of the claim.

The time has come, then, to give true effect to the *Data Protection Act 1998*.[94] We should learn to appreciate what we have already got. And with that, I would suggest, the cry for a privacy law will in no small part be answered.

PHILIP COPPEL QC

e-mail: pcoppel@4-5.co.uk

C:\Docs\Admin\Statute Law Society 19 Mar 2012 Privacy and DP mk2
17 Mar 2012 - 7:18pm

90 At [63]. The matter was resolved without trial. Words of encouragement are also to be found in: *Law Society & ors v Kordowski* [2011] EWHC 3185 (QB) at [100] and [134].

91 [2002] EWCA Civ 1373, [2003] QB 633, [2003] 1 All ER 224.

92 See quotation at page 18 above.

93 *Douglas & ors v Hello! Ltd* [2003] EWHC 786 (Ch), [2003] 3 All ER 996 at [239].

94 The EU Commission has now published reforms that would see the Directive upon which the *Data Protection Act 1998 is* repealed, replaced with a Regulation. The proposed Regulation adheres to the structure of the existing Directive, albeit with some important changes.

Extracts from the *Data Protection Act 1998*

Section 1(1)

Key definitions

"'data' means information which–

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68; or

(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d);

....

'data controller' means, subject to subsection (4), a person 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;

....

'data processor', in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

....

'personal data' means data which relate to a living individual who can be identified–

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

....

'processing', in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including–

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data;"

Section 2

The meaning of sensitive personal data

"In this Act 'sensitive personal data' means personal data consisting of information as to–

(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the *Trade Union and Labour Relations (Consolidation) Act 1992*,

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings."

Section 3

The special purposes

"In this Act 'the special purposes' means any one or more of the following–

(a) the purposes of journalism,

(b) artistic purposes, and

(c) literary purposes."

Section 4(4)

The statutory duty to comply with the data protection principles

"Subject to section 27(1), it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller."

Section 10(1)-(3)

Distress and damage notification

"(1) Subject to subsection (2), an individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing, or processing for a specified purpose or in a specified manner, any personal data in respect of which he is the data subject, on the ground that, for specified reasons–

(a) the processing of those data or their processing for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another, and

(b) that damage or distress is or would be unwarranted.

(2) Subsection (1) does not apply–

(a) in a case where any of the conditions in paragraphs 1 to 4 of Schedule 2 is met, or

(b) in such other cases as may be prescribed by the Secretary of State by order.

(3) The data controller must within twenty-one days of receiving a notice under subsection (1) ('the data subject notice') give the individual who gave it a written notice–

(a) stating that he has complied or intends to comply with the data subject notice, or

(b) stating his reasons for regarding the data subject notice as to any extent unjustified and the extent (if any) to which he has complied or intends to comply with it."'

Section 13

Compensation

"(1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.

(2) An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress if–

(a) the individual also suffers damage by reason of the contravention, or

(b) the contravention relates to the processing of personal data for the special purposes.

(3) In proceedings brought against a person by virtue of this section it is a defence to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned."

Section 32(1)-(3)

The press exemption

"(1) Personal data which are processed only for the special purposes are exempt from any provision to which this subsection relates if–

(a) the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material,

(b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest, and

(c) the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes.

(2) Subsection (1) relates to the provisions of–

(a) the data protection principles except the seventh data protection principle,

(b) section 7,

(c) section 10,

(d) section 12, and

(e) section 14(1) to (3).

(3) In considering for the purposes of subsection (1)(b) whether the belief of a data controller that publication would be in the public interest was or is a reasonable one, regard may be had to his compliance with any code of practice which–

(a) is relevant to the publication in question, and

(b) is designated by the Secretary of State by order for the purposes of this subsection."

Part I of Schedule 1

The data protection principles

"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 this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised 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 for the rights and freedoms of data subjects in relation to the processing of personal data."

Part II of Schedule 1

Fairness

"1(1) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.

(2) Subject to paragraph 2, for the purposes of the first principle data are to be treated as obtained fairly if they consist of information obtained from a person who–

(a) is authorised by or under any enactment to supply it, or

(b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on the United Kingdom.

2(1) Subject to paragraph 3, for the purposes of the first principle personal data are not to be treated as processed fairly unless–

(a) in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3), and

(b) in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3).

(2) In sub-paragraph (1)(b) "the relevant time" means–

(a) the time when the data controller first processes the data, or

(b) in a case where at that time disclosure to a third party within a reasonable period is envisaged–

(i) if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed,

(ii) if within that period the data controller becomes, or ought to become, aware that the data are unlikely to be disclosed to such a person

within that period, the time when the data controller does become, or ought to become, so aware, or

(iii) in any other case, the end of that period.

(3) The information referred to in sub-paragraph (1) is as follows, namely–

(a) the identity of the data controller,

(b) if he has nominated a representative for the purposes of this Act, the identity of that representative,

(c) the purpose or purposes for which the data are intended to be processed, and

(d) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

3(1) Paragraph 2(1)(b) does not apply where either of the primary conditions in sub-paragraph (2), together with such further conditions as may be prescribed by the Secretary of State by order, are met.

(2) The primary conditions referred to in sub-paragraph (1) are–

(a) that the provision of that information would involve a disproportionate effort, or

(b) that the recording of the information to be contained in the data by, or the disclosure of the data by, the data controller is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract."

There is more. In relation to paragraph 3(1), see also SI 2000/185.

Schedule 2

The first data protection principle conditions

"1. The data subject has given his consent to the processing.

2. The processing is necessary–

(a) for the performance of a contract to which the data subject is a party, or

(b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary–

(a) for the administration of justice,

(aa) for the exercise of any functions of either House of Parliament,

(b) for the exercise of any functions conferred on any person by or under any enactment,

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied."

Schedule 3

The first data protection principle sensitive personal data conditions

"1. The data subject has given his explicit consent to the processing of the personal data.

2(1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order–

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary–

(a) in order to protect the vital interests of the data subject or another person, in a case where–

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing–

(a) is carried out in the course of its legitimate activities by any body or association which–

(i) is not established or conducted for profit, and

(ii) exists for political, philosophical religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing–

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7(1) The processing is necessary–

(a) for the administration of justice,

(aa) for the exercise of any functions of either House of Parliament,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order–

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

7A(1) The processing–

(a) is either–

(i) the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or

(ii) any other processing by that person or another person of sensitive personal data so disclosed; and

(b) is necessary for the purposes of preventing fraud or a particular kind of fraud.

(2) In this paragraph "an anti-fraud organisation" means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes.

8(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.

9(1) The processing–

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph."

Orders under paragraph 10 are: SI 2000/417; SI 2002/2905; SI 2006/2068; SI 2009/1811.