Journal of Information, Law and Technology

Sources of Literature on Data Protection and Human Rights

Adam Warren
Phd Student, Information Science
a.p.warren@lboro.ac.uk

Dr James Dearnley
Lecturer of Information Science
j.a.dearnley@lboro.ac.uk, and

Professor Charles Oppenheim
Professor of Information Science
c.oppenheim@lboro.ac.uk

Department of Information Science
Loughborough University, UK

This is a **refereed** article published on: 2 July 2001

Citation: Warren A et al, 'Sources of Literature on Data Protection and Human Rights', 2001 (2) *The Journal of Information, Law and Technology (JILT)*.
<http://elj.warwick.ac.uk/jilt/01-2/warren.html>

Abstract

In this paper, we analyse and discuss the current state of knowledge and research concerning data protection, human rights and the right to privacy within the workplace. This follows on from recent legislation in this area, in particular the 1995 European Data Protection Directive, the UK Data Protection Act 1998 and the UK Human Rights Act 1998. Although drawing reference to a number of studies conducted around the world, this paper focuses on legislation in the United Kingdom. It assesses whether the recent legislation potentially offers adequate protection for individual privacy, providing concluding remarks on the experience so far.

The paper is split into three sections concerning the research issues surrounding: the Data Protection Act; the Human Rights Act; and privacy in the workplace. Landmark studies that help define information privacy have been identified. Additionally, sources of information regarding legal text, current awareness and so-called 'grey literature' have been discussed and analysed. The paper concludes that there is some uncertainty with the new legislation, especially in regard to the use of personal data in employer-employee relationships. Nevertheless, certain strands can be identified. Firstly, the tension between the competing interests of personal privacy and the ability of organisations to use personal data in their day to day activities. Secondly, the possible development - in the absence of explicit privacy legislation - of privacy common law by the UK courts. Finally, the regulatory morass regarding privacy in the workplace. Yet, in spite of ambiguity over the course of recent legislation, there is a flourishing and vibrant debate in this field - with contributions from civil liberties organisations, the quality press, academics and discussion groups.

Keywords: Data Protection, Privacy, 1995 European Data Protection Directive, Data Protection Act 1998, Human Rights Act 1998, Methodology, Workplace Privacy.

1. Introduction

Following the 1995 European Union (EU) directive relating to data protection[], and the subsequent introduction into the UK of the Data Protection Act 1998[] (DPA) together with the incorporation of the European Convention of Human Rights [] (ECHR) into UK law with the Human Rights Act 1998[] (HRA), a range of research concerning data protection, privacy and human rights has been published. This research has built upon a generation of previous work that commenced in the late 1960's and early 1970's. Recently, studies have been pitched at varying levels, examining - for example - international concerns, European issues and experience within specific sectors of industry.

In this paper, we analyse and discuss the current state of knowledge and research concerning data protection, human rights and the right to privacy within the workplace. Although surveillance of employees in the workplace is not a new one, the practice has become more ubiquitous and contentious in recent years. Devices range from CCTV to

email monitoring programs. Some staff have been the subject of covert surveillance. Yet, employers need to manage. They need to ensure that company policies are adhered to and that individual staff are doing their jobs and responding to company training. The enactment of the DPA and HRA in the UK have resulted in guidelines viewed by many employers and employees as conflicting and unworkable. The difficulties experienced in interpreting constantly changing legislation will be discussed in section 4 of this paper. Data protection is increasingly a global issue. Whilst focusing on legislation in the United Kingdom, this paper draws necessary reference to a number of high quality studies conducted around the world. The literature in this field is vast, and only a limited number can be incorporated into this paper. However, we believe enough have been included to render this paper worthwhile.

It can be argued that recent legislation potentially offers adequate protection for individual privacy. Conversely, the new legal measures can be interpreted as acting in a piecemeal fashion, inadequate for protecting individual privacy. This paper separates and analyses these strands, and offers some comments on the experience so far. The paper is split into three discrete sections. In the first, we consider research sources available for data protection issues. This section identifies a number of landmark studies that have helped define information privacy in the UK and elsewhere. Additionally, sources of information regarding legal text, current awareness and so-called 'grey literature' are discussed and analysed. We also draw reference to research and methodologies that have recently or are currently being used to measure and report reaction, and experience, of the new law.

In the next section, we consider research issues regarding the much-feted HRA 1998. In comparison to data protection issues, this topic has not been the focus of significant research. However, as we discuss and analyse in this section, there is a growing corpus of research that provides a basis for further consideration in this area.

The final section considers privacy issues within the workplace. There is considerable uncertainty with the new legislation in regard to the use of personal data in employer-employee relationships. This section also outlines various landmark studies in this complex area.

Finally, conclusions are offered.

This paper has been facilitated by a considerable number of research tools. The most useful were found largely through a process of trial and error. This section provides a brief overview of some key sources; others are mentioned throughout this paper. One of the most frequently used tools has been the newspaper databases available on CD ROM. The British Newspaper Index (BNI) indexed the quality UK press from 1990 providing bibliographic information together with abstracts. FT McCarthy was a more detailed database, containing full-text articles on business, companies and industry from a range of prominent daily newspapers. In researching academic papers, electronic sources provided indispensable. ASSIA Plus indexed international English language periodicals covering social sciences. Cambridge Scientific Abstracts (CSA) represented a large collection of databases, again, including social sciences, with the results displayed in

citation, abstract or full record format. Web of Science Proceedings (WoSP) covered published proceedings from over 45,000 conferences per year - providing access to academic papers, with weekly updates. For active updates of particular publications, the ZETOC Alert service - which emails table of contents from specified journals proved invaluable. Finally, for tracing 'grey' literature such as UK Parliamentary reports, COPAC provided a good starting point.

In terms of researching EU sources, the annual *EU Encyclopedia and Directory* provided a hard copy insight into the European Union decision-making processes. An electronic database, Eurotext, enabled access to key European Community full-text documents, for example founding treaties, in addition to narratives concerning the background to key EU institutions. For greater detail, Eurolaw provided a full text legal database of the EU covering not only the treaties establishing the Union, but also the Directives, Regulations and preparatory works with national implementation details. It further included the Court case decisions and Parliamentary questions. Finally, for EU-funded research, the CORDIS gateway was a good starting point with nine databases providing access to complete information on the research programmes, in addition to summaries of official documents relating to the EU's legislative and decision-making processes.

2. Data Protection

2.1 Landmark Studies: Defining Information Privacy

Academic studies concerning privacy and human rights have been limited. It was during the late 1960s and early 1970s that the concept of information privacy, as distinct from other aspects of privacy such as physical intrusion and surveillance, was developed. Two US publications in particular helped define the issue - *Privacy and Freedom* by Westin (1967)[] and Miller's *The Assault on Privacy* (1971)[]. For Westin, information privacy meant the claim of individuals 'to determine for themselves when, how and to what extent information about them is communicated to others'[]. Miller's definition was more succinct: 'the individual's ability to control the circulation of information relating to him'[]. Another publication, Rule's *Private Lives and Public Surveillance* (1973)[] contained an in depth examination of the collection and use of personal information as a means of social control. Detailed case studies of organisations such as the UK Driver Licencing system and the US Consumer Credit Reporting system examined what information the systems collected, through what means, who had access to it, how it was used and how such use impinged on the person it referred to.

From the academic debates of this period, privacy emerged as a value that could not be taken or misused by government without due process of law. This idea was later developed into a set of best practice principles - both in the US and Europe - ensuring fair processing, minimal intrusion and limited purposes for the use of personal data. It was this informational aspect of privacy that was most profoundly affected by the rapid developments in information technology during the 1960's. Concerns about the increased use of the computer and the setting up of national databanks were growing. In these circumstances, the choice of the individual was seen as central to the concept of privacy -

both in allowing physical intrusion and the sharing of information. Westin, Miller and Rule were among the first commentators to articulate and promote such individual choice.

As western countries began to enact data protection legislation during the 1970s and 1980's, comparative studies of national laws emerged. The work of Burkert[] and Nugter [] were particularly significant during the 1980s, and early 1990s. In 1994, a wide-ranging study into the issues surrounding privacy and human rights in the international context was published by Michael as *Privacy and Human Rights*[]. In this work sponsored by UNESCO, the author examined the social, political and cultural context to global privacy and data protection laws. Less detailed than Miller and Westin, Michael however highlighted the cultural difficulties that the term 'privacy' may present and the different legal approaches taken to its protection.

The legal approaches were categorised under three headings: Nordic, civil and common. Nordic was defined as a combination of legal remedy available to the individual through rights of access and the administrative regulation of computerised records. In many ways, this form of remedy pioneered information legislation. Certainly, rights of access were well-entrenched, with Sweden having a Freedom of the Press Act in 1776, the oldest access law in the world. In terms of individual privacy, Norway had passed an early law forbidding violation of 'the peace of private life' in 1899. Finally, it was Sweden that led the way in regulation of computerised records, with the world's first national data protection law in 1973. Arguably, this first generation of data protection legislation was initiated at the Nordic Conference - a meeting of legal authorities in Stockholm in 1967 which resulted in an influential, though not binding, declaration of the meaning of right to privacy[].

The civil law approach differed in that it relied on statements of general principle. Its clear influence has been seen on two significant doctrines in the development of privacy law. Firstly, although not containing an explicit right to privacy, the US Supreme Court was able to extend the US Constitution to protect certain types of behaviour[]. They included a right to privacy from government surveillance into an area where a person had a 'reasonable expectation of privacy'[], and also matters relating to marriage, procreation, child-rearing and education. The second significant doctrine was developed through the European Convention of Human Rights (ECHR), a codification of international human rights law.

If civil law was about assertion of principle, then common law - the third approach identified by Michael - applied the principles through individual cases. In the UK, for example, the emphasis had been on particular legal remedies against particular infringements. Such rights were often developed by judges without reference to Parliament. An example would be the essentials of the English law of confidence. However, following the implementation of the first Data Protection Act in 1984, this trend has been somewhat eclipsed, with the UK establishing a supervisory body to police the legislation. Nevertheless, the arrival of the HRA 1998 has led to speculation that privacy common law may be developed. This issue will be expounded later in this paper.

Michael credited the ECHR as a significant force for change in the UK, with Article 8 (1) setting out the statement of the right to privacy, then listing its qualifications in 8 (2). Individuals have been able to take legal action against the UK in the European Court of Human Rights at Strasbourg in reliance on the Convention since 1966. The Court takes sections (1) and (2) of Article 8 in turn, asking whether the facts interfered with the rights, and, if so, whether the interference was 'in accordance with the law'. Michael concluded optimistically, stating that since the early 1970's the spread of automated information handling has almost been matched by the spread of legislation to protect individual privacy[].

2.2 Standard Legal Texts: A Framework for Information Privacy

Several standard books explain the structure of the Data Protection Act (DPA) 1998. For detailed line-by-line analysis of the DPA 1998, together with a copy of the statute, Carey's *Data Protection in the UK* is a very useful reference source[]. It is a comprehensive guide - assuming no prior knowledge of data protection legislation. The book is structured logically, with chapters on the rights of individuals, the data protection principles, exemptions and enforcement. In addition, specific chapters are dedicated to the Internet, telecommunications and the obligations of employers.

A more critical text is Jay and Hamilton *Data Protection: Law and Practice*[]. Comprehensive like Carey, Jay and Hamilton, however, attempt greater historical detail: making greater reference to case law and to a series of hypothetical cases. The authors highlighted the limitations placed on the 1998 DPA - particularly its failure to address privacy, in spite of the clear provisions in the overarching European Union (EU) Data Protection Directive relating to private life. This, argued the authors, could lead to problems in UK courts with lawyers arguing that the Directive has not been fully transposed into UK law[]. On the Human Rights Act, the authors make the important point that the manner in which the Convention is inserted into UK law does not endow individuals with a direct right to take action in courts for breach of their privacy. The right must be respected by the state, but if an individual's privacy is breached by a private party, the litigant has no basis which to take action in breach of that right alone[]. However, not all commentators agree with this interpretation. The views of Singh, a barrister, will be considered later in this review. Nevertheless, Jay and Hamilton helped highlight such procedural complexities. In addition, they clarified what was missing from the DPA 1998, what needed to be developed through case law, (for example the nature of the right to private life), and included a detailed case study on the definition of 'relevant filing system'. A privacy culture based on both the DPA 1998 and the HRA 1998 may be possible, but it will take many years as it will need to be established via the UK courts.

Business newsletters are essential for providing expert opinion on new developments within organisations - often prior to the publication of academic research in the area concerned. On a global level, *Privacy Laws and Business* specialises in data protection laws and their impact on business and the public sector. A recent issue (issue 56, December 2000) featured the processing of employee data and model contracts for transborder data flows. Other issues have highlighted: the development of privacy policy generators[] - software designed to help companies to customise accurate and legally

compliant privacy policies; and various organisations' strategies to comply with the UK DPA including banks[], retailers[], and charities[].

The style and structure of the newsletters varies considerably. *Privacy and Data Protection*, edited by Carey was a new journal established in 2000 and dedicated largely to UK data protection issues. It has featured perspectives from overseas - with views from Australia in issue 2 (November/December 2000) and the US in issue 4 (March 2001). There is a regular feature on electronic privacy, and an innovative information service for subscribers - allowing receipt of documents free of charge.

In the US, the monthly *Privacy Journal* tackles 'privacy in the computer age'. At approximately eight pages in length, it is lighter than the newsletters mentioned above. Additionally, it does not feature contributions from external commentators - being more of a news digest of privacy issues in the US. The only outside contributions - sometimes from privacy experts - come in the letters page. As a result, the journal - although a useful source of information - has a narrower perspective compared with some newsletters.

There is also a body of electronic newsletters. They tend to be less substantial in content, usually structured as news digests. *Act Now* details data protection issues in the UK public sector. In addition to news stories, it lists details of relevant conferences and other resources such as guides to the DPA 1998 by government departments, and training seminars on the Act. In the US, the Electronic Privacy Information Center (EPIC), a civil liberties group and research centre, publishes the bi-weekly *EPIC Alert*. This is a well ordered newsletter, with a table of contents outlining the articles featured, a bookstore cataloguing other publications, and a list of conferences. Additionally, the 'EPIC Bill-Track' feature charts the progress of privacy-related legislation through Congress. Altogether, this newsletter provides a clear, informative picture of current US privacy policy and debate. Another prominent electronic newsletter, and forum for discussion of the effect of technology on privacy, is the *Computer Privacy Digest*[].

Other newsletters include: in the UK, *Data Protection and Privacy Practice*; in the US, *Privacy Times* and *Privacy and American Business*; in Canada, *Privacy Files*; and in Australia, *Privacy Law and Policy Reporter*. Finally, solicitors such as Masons[] and Bird and Bird[] produce their own newsletters detailing recent legal developments in privacy law.

The enactment of the European Data Protection Directive in 1995 dramatically increased privacy research across many disciplines - including law, social sciences and politics. As a forum for detailed analysis of such research, the academic journals proved most enlightening. For instant analysis, electronic journals are particularly useful - combining academic articles with more descriptive commentaries. Publications include *The Journal of Law, Information and Technology (JILT)*[] based at Warwick Law School, Warwick University and the *Web Journal of Current Legal Issues*[] published bi-monthly at Newcastle University. The former has been especially prolific, with a dedicated data protection issue in January 1996[], featuring articles outlining the European Directive - from the introduction by Lloyd[] to features on its impact in various European countries such as Denmark, UK, Ireland and the Netherlands.

The *Web Journal of Current Legal Issues* is less orientated towards the information sector, but has featured some comment on data protection. Kosten and Pounder provide a detailed Article-by-Article analysis of the Data Protection Directive, drawing attention to some of the difficulties that may occur during the implementation of the Directive into UK law[]. Difficulties included exemptions 'in the public interest' (Article 7(e)) - exemptions balancing right to privacy with 'rules governing freedom of expression' which could be problematic, possibly conflicting with Article 10 of the HRA[]; and circumstances in which data can be transferred to third countries. Further detail can be found with Widdison's article which tabulated the key changes between the 1984 and 1998 Data Protection Acts[].

In terms of ongoing research, the hard copy journals proved an excellent source of information, for example: *International Review of Administrative Sciences*; *New Law Journal*; *Cambridge Law Journal*; *Journal of Common Market Studies*; *The Information Society*; *Information, Communication and Society*; *European Human Rights Law Review*; *Science, Technology and Human Values*. Finally, the *International Review of Law, Computers and Technology* dedicated issues one and two to data protection in 1997, whilst in 1999 *Revue Français d'Administration Publique* had a special issue (number 89) featuring the transposition of the EU Data Protection Directive into several countries. The above journals are generally more geared towards refereed articles than commentaries, often showcasing research conducted over a number of years. This includes studies into the effectiveness of the DPA 1998, development of a methodology for assessing the workability of data protection legislation, comparison of data protection law cross-nationally, and questions concerning the causes and effects of surveillance. The following sub-section will outline research into evaluation of the practical effects of data protection policy on society.

2.3 Current Research

The development of an EU Data Protection Directive, with its provisions for judging the 'adequacy' of third country legislation, illustrated the importance of international comparisons. For over a decade, this has been a major feature of the research of Bennett - being defined by his book *Regulating Privacy* (1992)[]. In this work, Bennett examined political responses to the data protection issue in four Western democracies, comparing legislation in the US, Germany, the UK and Sweden. This research built on earlier papers [] where he had contended that, with the definition of privacy being so ambiguous, legislation is most effective if tailored to suit the political and legal cultures of the countries concerned. Bennett found that five different models existed for the implementation of fair information principles[]. The law could be implemented through a licensing approach, as in Sweden or France. It could be via a system of registration as in the UK and the Netherlands. Thirdly, it may be administered by voluntary control through self-regulation. Alternatively, the onus could be on the citizenry to enforce their rights in the courts - the 'self-help' solution in the US under the Privacy Act 1974. Finally, the law may be overseen by a Data Protection Commissioner as in Canada and Germany. However, during the 1990's these boundaries, particularly in the EU, became increasingly blurred.

This ‘blurring of boundaries’ was taken up in a 1997 article by Raab[]. Like Bennett, Raab considered that most, although not all, of the above instruments were used to one extent or another in every system of data protection - therefore being seen ‘more as variables than as the criteria defining different types of systems’[]. It is the relationships within these instruments between people, roles and institutions that provided the focus for Raab’s research in this paper. He concluded, that if privacy is to be safeguarded, it would become increasingly important to comprehend - even shape - the connections among the various mechanisms or strategies, and among those who deploy them. Raab advocated a position in which the various market, civil society and state forces involved in ‘co-producing’ effective data protection were mutually dependent. However, this approach required further detailed empirical and comparative investigation across systems in order for privacy and data protection to emerge as a coherent field of public policy.

There have been plenty of general analyses that outline the provisions of the EU Data Protection Directive. Opinion on its effectiveness, however, has been divided. Bainbridge and Pearce recently argued that the UK DPA 1998 has failed to make a significant contribution to privacy rights in the UK[]. The authors found that whilst the Directive aimed to protect privacy, there was no mention of the word ‘privacy’ in the UK DPA 1998. Further, transparency in the processing of data had been compromised by various exemptions from subject information provisions and, in many cases, from the requirement to notify the Commissioner of processing of personal data. Finally, in order to fully benefit from the legislation, the data subject needed to be well-informed and pro-active. Changes to privacy, the authors argued, could come from the implementation of the Human Rights Act 1998 - with Article 8 of the ECHR being specifically mentioned in Recital 10 of Directive 95/46/EC as underpinning the level of protection for individuals set out in the Directive[].

Conversely, Pearce and Platten in the *Journal of Common Market Studies*, stressed the importance of the Data Protection Directive at a European level, as being the first Directive to specifically address human rights issues[]. In this respect, the Directive represented a landmark piece of legislation for the EU, although the authors acknowledged that variations in national responses are major obstacles to achieving to achieving data protection equivalence.

However, the growth of the internet, and increased dissemination of personal data - together with the ease with which it can be matched to create new information - point up to the increasing difficulty of regulating the flow of personal data through national and transnational legislation. Thus, industry specific codes of practice have been attracting increased attention. In the Netherlands, van de Donk and van Duivenboden[] outlined their role in the national data protection system, where such codes have been drawn up in consultation with the Dutch data protection authority. This form of ‘controlled self-regulation’ eases some of the pressure of enforcement from the national regulators, whilst allowing sectors of industry a degree of (officially approved) independence from the state - providing the codes are complied with. In the UK, a code of practice has been developed for the use of closed circuit television (CCTV) and more controversially, as will be discussed later, to cover employer-employee relations across sectors.

The case for codes of practice was strengthened by Article 25 (2) of the Data Protection Directive, allowing them to be taken into consideration when assessing the 'adequacy' of data protection in third countries. The academic lawyer, Schaffer[] argued in his 2000 article that the Directive has changed the way all US institutions addressed privacy issues. Since the enactment of the Directive, US businesses have been prodded to change their behaviour in order to avoid confrontations with EU regulators; US regulators have pressed US businesses to enhance their internal standards to avoid a regulatory conflict; and US privacy advocates have been presented with a functioning alternative to US law which they can promote. This analysis implied that the personal data of EU member states should be secure when transferred to the US in accordance with the 'safe harbor' agreement of July 2000[]. However, other commentators are less confident. Swire and Litan[] noted in 1998 that US data privacy protection in the areas of human resources/employment, health, data marketing and insurance was relatively lax and of concern to EU authorities.

2.3.1 Developing a Methodology

Following the academic critical analyses of the legislation, Raab and Bennett have developed techniques to assess the effectiveness of UK privacy legislation. Raab[] has examined the entire implementation process: registration, enforcement, self-regulation, politics, and learning and development, and concluded that infrastructures for data protection are in place in the UK. However, they are fragile and exist alongside what he terms 'adversarial modes of conducting relationships'[] - which when the article was written (1996) included economic and political values, perhaps intolerant of the bureaucracy stemming from the Data Protection Registrar, now Information Commissioner. The focus was on the perspective of the Registrar, since it was her role to promote privacy, buoyed up by an EU Directive that stated a privacy goal. In his analysis, Raab emphasised the importance of the pragmatic conflict-resolving style of UK administration and the context of UK politics, dominated for the 1980's and much of the 1990's by one party.

One of the complications with data protection legislation came in its evaluation. Raab and Bennett considered a methodology for conducting such an evaluation[]. The difficulties of establishing criteria that can be used objectively were discussed, as was the UK Office of the Data Protection Registrar's (ODPR) scepticism of quantitative performance criteria []. When considering who or what should be evaluated, the authors looked at various factors. They included: the law itself; the performance of the supervisory authority (for example dealing with complaints, prosecutions, production of information booklets); the performance of the data controllers in adopting best practice; and finally the performance of the data subjects in taking steps to protect their personal data, for example, by removing their names from mailing lists or requesting access to their own data. In summary, to facilitate evaluation, the following factors were advocated:

- Dominant policy and legal clarity;
- Strong regulatory agency;

- Explicit agency activities;
- A developing system of accountability.

The conclusions drawn by the authors in terms of establishing a sound methodology were that:

- Criteria for assessing performance is difficult - one needs to focus primarily on the activities of the data protection agency and the political processes that drive it;
- The only reliable criteria are procedural - rules, codes, sanctions and decisions. Only evaluate on the basis of whether the system adequately puts in place procedures for data subjects to exercise their own privacy rights;
- Data protection agencies need to define their own system of performance measures and regularly test them;
- Policy implementation requires a 'bottom up' perspective. Observe procedures achieved at ground level through negotiating, bargaining and influence, rather than solely using quantitative goals imposed by senior management.

The emphasis therefore is on qualitative measures. This makes for some promising avenues of research, particularly in the field of comparative, qualitative research. Ideally, it has been argued, the supervisory agencies should be working themselves out of business.

2.4 The Wider Debate

2.4.1 Government and Special Interest Groups

The official source for information concerning data protection policy and implementation in the UK is the Office of the Information Commissioner (OIC). In the Commission's *First Annual Report*[], 2000, particular attention was paid to the 1998 Data Protection Act and the questions arising from its implementation[]. Among those identified were information sharing between government departments, matters relating to the use of NHS number as a unique identifier, and the availability and use of public registers. Wider perspectives include the Regulation of Investigatory Powers Act[] (RIPA) and issuing of a sector specific code of practice on employee/employer relationships. This was an important document for what supervisory authority viewed as key issues, and the direction regulation was taking in the UK. Additionally, chapter six of the *Report* summarised progress made during the year. Quantitative indicators measured performance indicators such number of complaints received, time taken to investigate cases, the number of convictions made and the level of public awareness.

Within the European Union, data protection largely fell under the remit of the Data Protection Unit at the Internal Market Directorate. This Directorate's website has access to a variety of resources[]. They include news, working papers, and studies into data protection, in addition to other international instruments on the topic, for example Convention 108[]. Convention 108 had been drafted by the Council of Europe[], and opened up for signature in 1981 as world's first legally binding international data protection measure, setting a precedent for the 1995 EU Data Protection Directive[].

Civil liberties groups have become increasingly influential in lobbying government for changes to the law, often commissioning their own studies into key aspects of privacy. Considerable information is included on their websites: Cyber-Rights and Cyber-Liberties <<http://www.cyber-rights.org>> containing detailed information on RIPA; the Foundation for Information Policy Research <<http://www.fipr.org>>, also heavily involved in the RIPA issue; Campaign for Freedom of Information (CFOI) <<http://www.cfoi.org.uk>> lobbying the government for changes to the freedom of information legislation; and Liberty <<http://www.liberty-human-rights.org.uk>> which has reported across a range of issues concerning human rights. The above sources have been complemented by the websites of pressure groups such as Statewatch <<http://www.statewatch.org>>, monitoring state and civil liberties in the EU, and the aforementioned civil liberties organisation EPIC <<http://www.epic.org>>.

The identification and availability of reports by such interest groups can be difficult. A key source for such documents has been expert privacy websites such as Privacy Exchange, <<http://www.privacyexchange.org>>, and Privacy International, <<http://www.privacy.org/pi/>>. The former website has an informative section listing reports in the legal privacy sector, and was the first point of reference for a report commissioned by the British Chamber of Commerce titled *The Economic Impact of the Regulation of Investigatory Powers Bill*[]. Published in June 2000, this report detailed the economic and legal implications of this legislation for businesses. The authors argued that substantial increases have been made in the powers of public authorities without any corresponding increase in the scope for oversight and accountability. The effect of Part I of the Bill (now an Act) - 'Interception' - was to permit mass surveillance of internet activities without judicial warrant or adequate oversight.

The economic issues highlighted in the report include doubts over cost, risk and disruption to business, with an estimated cost of compliance by the Internet Service Providers (ISP's) likely to be £640 million over the next five years. Further, the RIP provisions would inhibit investment, impede the evolution of e-commerce and place UK companies at a competitive disadvantage. Legally, the report concluded that Part III of the Bill - 'Surveillance' - contravened the European Convention on Human Rights (ECHR), and elements of Part I may breach the DPA 1998.

Another key report - found on the Privacy International website - was commissioned by Privacy International and the US-based civil liberties group, EPIC. *Privacy and Human Rights 2000*, reviewed the state of privacy in over fifty countries[]. It acknowledged the progress in terms of legislation with over a dozen countries enacting new laws in 1999 -

either to address past government abuses, to promote e-commerce or ensure compatibility with international standards developed by the EU, Council of Europe and OECD. Among the threats reviewed, particular attention is given to the abuse of surveillance authority - with the main targets being political opponents, journalists and human rights activists.

Finally, Privacy Exchange, highlighted several recent reports by the US Federal Trade Commission into areas such as online profiling and fair information practices in the electronic marketplace. Additionally, two reports by the Organisation for Economic Co-operation and Development (OECD) published in March 2001, were highlighted. Both investigated consumer protection laws in the field of electronic commerce[]. Thus, there is a healthy research community regarding data protection.

Testimonies of expert witnesses before various government committees are another excellent source of research information. Privacy Exchange, again, has been a good starting point, listing testimonies before hearings globally. An example is the recent US hearing into the EU Data Protection Directive of 8 March 2001 before the House of Representatives, the subcommittee on Commerce, Trade and Consumer Protection, and the committee on Energy and Commerce[]. During this hearing, the chairmen of both the committee and sub-committee were highly critical of the Directive and its potential impact on US businesses. The Directive was defended by Stefano Rodota, Italian Privacy Commissioner and chairman of the Article 29 Working Party - an advisory body set up by the Directive to consider issues concerning harmonisation and level of data protection in third countries[] - and David Smith, Assistant UK Information Commissioner. Joel Reidenberg, a Fordham University law professor, warned that with the continuing global trend towards national legislative protections for privacy, the US was 'rapidly on the path to becoming the world's leading privacy rogue nation'[].

2.4.2 Data Protection Discussion Groups

The Data Protection Forum is a discussion group bringing together companies, public sector and consumers to discuss personal data in seminars. Presentations have been by organisations as diverse as the National Consumer Council and Deloitte and Touche. During 2001, seminars have been held on data compliance in the public and private sectors, and monitoring the use of personnel data in organisations. Many of the presentations are available, free of charge, at: <<http://www.sbu.ac.uk/dpforum>>.

The JISCmail-hosted *Data Protection Discussion Group*[] helps to promote the discussion of data protection among UK lawyers, academics and data protection officers. Online discussions include how the Act will work with regard to workplace surveillance, sensitive data - such as student names kept by universities - and driving licences and genetic data. The relevance of the discussions, and the standard of the contributions is inevitably varied. Yet, it generally represents a worthwhile contribution to the debate on data protection.

2.4.3 Media Debate

One of the paramount ways of keeping up to date has been via the quality press. *The*

Guardian in particular has produced regular and well-informed pages on information issues, as well as launching its own campaign for greater openness in government in the wake of the proposed freedom of information legislation[]. Additional relevant articles have been found via online newspaper databases such as British Newspaper Index and FT McCarthy. Those references have yielded commentary on the RIPA, as well as a variety of consumer issues such as online purchasing, CCTV and workplace surveillance.

The Guardian has recently featured stories concerning surveillance in the UK[] - in particular the privacy implications of street cameras equipped with facial recognition software, and the tracking capabilities of the proposed third generation mobile phones. Other concerns about the security of online data originating from credit card purchases have been ongoing - from the security flaws involving systems at Powergen and Barclays Bank in July 2000[] to the hacking the customer database of one of Amazon's subsidiaries, which went undetected for four months up to March 2001[].

The online media is now an important source for breaking news. In late March 2001, *Ft.com* - the online arm of the *Financial Times* - featured the deepening dispute between the EU and the US over the Data Protection Directive[]. On the 28 March 2001, the European Commission had rejected US concerns about the provisions for companies transferring data across the Atlantic. The Bush administration had written to the Commission protesting against model contract terms agreed by the EU for the transfer of personal data. *The Independent* online featured the same story[], highlighting the potential disruption to EU trade with the US if the 'safe harbor' agreement is torn up - with companies having to seek permission of individual customers before their data can be transferred to the US.

Further coverage of the debate on privacy is located on online business news services such as Silicon.com and CNET Networks. The latter featured on the speech at the beginning of April 2001 by the Majority leader in the House of Representatives, Dick Amery, that any online privacy bill is likely to do more harm than good[]. Further coverage, and commentary, has been devoted to US administration's reluctance to appoint a new Chief Privacy Counselor to the President[]. Silicon, meanwhile, broke a story on 12 April 2001 concerning UK government plans to sell electoral roll information to credit reference agencies[] - sparking concerns that people with poor credit histories will be discouraged from registering, thus being excluded from the democratic process. From a data protection point of view, the Information Commission has expressed concerns that this breaches the second data protection principle - as information collected for one particular purpose (politics) will be used for another (commerce).

For further international legal perspectives, the EU-based QuickLinks provides links to news items about the legal and regulatory aspects of the Internet and the information society. The website <<http://www.qlinks.net>> contains frequent updates, an events page and news items organised by category (for example, 'Data Protection') as well as chronologically by issue and full text search. This source has proved to be the first point of reference for breaking news, providing citations that can be followed elsewhere.

2.5 Consumer Opinion

Important raw data can be gathered from surveys. This subsection details a sample from the US and the UK. Privacy Exchange has a detailed list of privacy surveys dating from 1979[]. Among the most prominent is the long series of surveys Equifax/Harris have undertaken since 1979 - under the direction of Alan Westin and heavily funded by industry, in particular the Equifax credit rating service. The most recent in the series is the *2000 ChoicePoint Public Opinion Survey*[] - ChoicePoint being a spin-off of Equifax Insurance Services. This latest survey showed that people had become more aware and concerned about privacy - with 63% of the US population found to be privacy 'pragmatists' up from 55% throughout the 1990's[]. Another US survey is by the Pew Internet and American Life Project who have published reports topics such as new internet users (2000); online workers (2000); and fear of online crime (2001)[].

Another valuable website for such information is <<http://www.nua.ie/surveys>> - an online information database - containing statistics on all aspects of the Internet, including privacy. Usefully, the information is provided in order of date, complete with links. One example is its reference to a preliminary report released by the US Senate Governmental Affairs Committee in April 2001. The report found that 64 federal government websites were violating visitors' privacy, and federal law, by tracking the visitors' online movements using cookies. The report was incomplete, and the final figure is expected to be much higher.

In the UK, annual surveys are conducted by the regulatory authority, the Office of the Information Commissioner (OIC), for fifteen years the Office of the Data Protection Registrar (ODPR). This information can be found on the OIC website <<http://www.dataprotection.gov.uk>>. Commencing in 1987, public attitudes towards the use of personal data were tracked. Questions concerned attitudes towards personal privacy and the DPA - including awareness of the Act among data subjects. This had increased from 34% in 1987 to 69% in the 2000 survey.

Other UK surveys include Perri 6's study *The future of privacy*[] for think-tank DEMOS. Among the findings were that few people saw any loss of privacy as inevitable, and that very few were willing to trust any organisation - with supermarkets found to be the least trusted, few people being convinced that their loyalty cards are treated with enough confidentiality. Finally, the National Consumer Council published a report into consumer privacy in December 1999[]. This survey used focus group research to assess awareness of organisational use of personal data and whether individuals were given adequate opportunity to consent to its use. The findings showed concern about how information was being shared among organisations, together with a general lack of awareness of the scope - though not the existence - of the DPA 1998.

3. Human Rights

3.1 Incorporation of European Convention of Human Rights

As the UK DPA 1998 is ultimately derived from the ECHR[], especially Article 8, an initial understanding of human rights legislation is fundamental. Wadham and Mountfield's *Blackstone's guide to the Human Rights Act 1998* provided an excellent introduction to the Human Rights Act (HRA) 1998[]. The authors began by pointing out that the UK Human Rights Act only incorporates part of the ECHR. It did not incorporate any of the procedural rights of the Convention, nor the right to an effective remedy (Article 13), although regard will be made to Strasbourg case law. The book proceeded to list the limitations of the Act, including issues such as the rule of law and whether any state interference was necessary in a democratic society or proportionate to the ends achieved, for example, the protection of privacy from excessive media interference. Usefully, the book examined each Convention right, and issues that could be raised in UK courts. For Article 8, important issues existed regarding police listening devices, CCTV and employee privacy. The book also has valuable table of cases referred to in the text, and appendices concerning background policy papers, parliamentary debates, rules of procedure for the European Court of Human Rights and the text of the ECHR. Altogether, this is a fundamental reference source.

3.2 Current Research

Specific analysis concerning human rights is more difficult to locate. However, Singh presented a detailed interpretation of the right to privacy[]. Although considering the interface between privacy and freedom of expression, the article made some interesting points in relation to privacy law. Firstly, Article 8 imposes an obligation to 'respect' privacy - not just prohibit interferences to privacy by the State. This distinction, Singh argued, is crucial as Strasbourg has stated the positive obligation will extend to requiring action to protect an individual from the acts of other private parties[]. This could set a precedent, for example making employers accountable to the HRA in the private, as well as public, sector. This differs from the interpretation of Jay and Hamilton, and is strengthened by the precedent quoted from Strasbourg case law, which the UK courts will ultimately have to consider when making their judgements.

Secondly, Singh argued that a provision in the HRA 1998 - Section 6 (6) - which prevents the possibility of a complaint being made that Parliament failed to legislate against a particular right, could lead judges to develop their own common law - extending far beyond the current breach of confidence case law.

The privacy provisions in the statute are, however, checked to some extent by the insertion of a new section 12 - entitled 'Freedom of Expression' - during the House of Commons committee stage. This provision enabled courts to strike the right balance between the Convention right to freedom of expression, including public interest in the publication of certain material, with other rights, particularly the right to privacy. In the workplace this could enhance the protection to so-called 'whistleblowers' who bring to attention lapses by employers, particularly in the area of safety. Additionally, it would make it difficult to obtain prior restraints, or 'gagging orders' preventing news being published. This would be consistent with the universal scheme of the Act - giving no public body a privileged position in the context of human rights. Furthermore, it gives no Convention right priority over any other. To summarise Singh's findings:

- The HRA 1998 may be indirectly applicable against private individuals and companies;

- The HRA 1998 provides a springboard for developing existing causes of action, thus filling gaps in the patchy privacy protection provided in English law.

3.3 Media Debate

Debate in this area has been intense, with the quality press stressing the significance of the HRA. On the day it came into force - 2 October 2000 - a front page caption on *The Guardian* read 'UK law sees the biggest change in more than 300 years'[]. BBC Online ran a special feature during the first week of the Act, analysing its effect on the police, health, councils and workplace among other institutions[]. Additionally, the Act has been warmly welcomed by the OIC, believing it will strengthen the application of the DPA, as well as reinforcing the case for privacy and data protection more widely. An alternative view of the HRA came from Davies, who saw lawyers as the main beneficiaries from the spate of litigation that will stem from the Act[]. The impact of the HRA 1998 on privacy will only be appreciated after some substantial case law. The first judgement to uphold a right to privacy under English law since the HRA came into force was a Court of Appeal ruling in December 2000 on Hello! magazine's illicit pictures of Catherine Zeta Jones' wedding[]. This judgement - recognising the right to privacy as a legal right capable of existing independently from the law of confidence - received substantial media coverage, not least due to the celebrity status of the couple involved.

4. Individual Privacy Protection - The Workplace Dimension

4.1 New Legislative Framework - Potential for Conflict?

In the new legislative environment, perhaps the area where the impact of the new regulations is most uncertain is the workplace. In addition to the DPA and HRA, the Department of Trade and Industry's (DTI's) *Lawful Business Practice Regulations*[] and the OIC's *Draft Code of Practice: The Use of Personal Data in Employer/ Employee Relationships*[] have, or will have, a substantial bearing on workplace privacy. The Public Information Disclosure Act 1998[], which increased employment protection for whistleblowers is also relevant. This, and other legislation from 1988 onwards can be referred to via the HMSO website: <<http://www.hmso.gov.uk/acts.htm>>. Finally, official documents detailing reactions to government proposals are helpful, for example, in the case of the *Lawful Business Practice Regulations*[].

Significant EU grey literature include the COM series of documents. These documents include proposals for legislation, annual reports, and policy statements. They can be traced via the excellent Eurolaw service at <<http://www.ili.co.uk>>. This site also includes Court case decisions and parliamentary questions. Finally, in order to focus on a particular piece of legislation for example, the Data Protection Directive, the European

Parliament website <<http://www.europarl.eu.int>> has a helpful legal observatory with details on documents produced, the agents involved and providing commentary - mainly in French - on the various stages leading to the final text. This is an excellent facility and the first point of reference for any document search regarding EU legislation.

4.2 Current Research

Extensive research into the practice of surveillance has been conducted over a number of years. In 1988 Clarke[] used the term 'dataveillance' in a paper to describe the systematic monitoring of people's actions or communications through the application of information technology. In addition, Flaherty[] - the former Information and Privacy Commissioner for British Columbia - and Lyon[] - analysing the social origins and consequences of processing personal data - have published extensively in this area.

Workplace surveillance has been discussed at length by Mohammed in a *JILT* article in 1999[]. In a 1999 conference paper, Davies provided a detailed overview of the new technologies coming to the fore[] - extending to every aspect of a worker's life. Miniature cameras monitor behaviour. 'Smart' identification badges - popular with IT companies such as Olivetti Research in Cambridge - track an employee's movement around a building. Telephone Management Systems (TMS) analyse the pattern of telephone use and the destination of calls. Computer-based monitoring systems record statistics about the employee assigned to a particular terminal, including the number of keystrokes per minute and the amount of time spent on the computer. Software such as Baltimore's MAILsweeper and WEBsweeper can monitor employee email and web use - blocking access to 'backdoor' email accounts such as Hotmail[]. Finally, psychological tests, aptitude tests, performance tests, and personality tests - many of which are electronically assessed - raise a great many issues of privacy, control and fairness. For many employees, surveillance and monitoring have become part of the modern work environment. The remainder of this sub-section will assess how recent legislation referred to throughout this paper may impact on individual privacy in employment.

4.2.1 Human Rights Act 1998 and UK Employment Legislation

Palmer's paper of March 2000[] gave an interesting insight into the current research being conducted in this area. Beginning by stating that the HRA 1998 will have a momentous impact, attempting to 'graft a rights-based system on to British law'[], the author asserted that what was missing was a unifying concept of the right of the individual to protection in relation to employment. The ECHR may be of limited use to employees as it is restricted to civil and political rights, without directly tackling social and economic injustices. Even then, its scope is limited to 'public authorities'. Although this definition could encompass private utilities that carry out a public function, such as Railtrack, those organisations' employment functions are still likely to remain private. Moreover, the case law draws distinctions between types of employee dispute. For example, a dispute over pay and conditions will not fall under the HRA, but one which raises concerns about the safety functions of Railtrack could. Thus, as with Jay and Hamilton, and Singh, the article returned to the vexed question of whether protests over employer surveillance can be addressed by the HRA 1998.

Palmer argued that, in theory, the UK could be challenged for failing to protect the privacy rights of employees in the private sector. If so, the ECHR could impose a positive duty on the government to legislate for both public and private employees. This, contended the author, would stem from the recognition that the State and other public bodies do not have a monopoly on power. Rather, it is dispersed throughout society and, to be fully incorporative, the HRA 1998 cannot exempt private individuals and bodies from respecting fundamental rights of their fellow citizens[]. The conclusion matches Singh's - that the courts should protect an individual's Convention rights against interference by other persons unless the UK legislation is found to be incompatible with the Convention. However, the scope of this duty remains unclear.

Another difficulty identified by Palmer - also noted by Wadham and Mountfield[] - is the government's decision not to set up a Human Rights Commission. Such a body, it is argued, would have acted as a permanent watchdog, being influential in raising awareness of rights in other countries. Without the Commission, public bodies covered by the Act may be less likely to adopt good practices or be aware of their new obligations. As a result, more litigation is likely.

With particular regard to secret surveillance at the workplace, such practice could infringe the private life of an individual. Where personal information is involved, it could also breach the Data Protection Act 1998. The DPA 1998 may be based on the EU Data Protection Directive, but the UK government has explicitly stated that the legislation draws on Article 8 of the Convention[]. Palmer also pointed out some indirect benefits: for example, that the uncertainty and threat of litigation may persuade some public authorities to change their policies without litigation. Overall, she drew the following conclusions:

- Although limited to civil and political rights, HRA 1998 has the potential to influence the future of UK labour law;

- Development of common law will be based on fundamental human rights principles. The new Act, therefore, may hasten the development of the common law of privacy;

- The effective application of human rights in the private sphere is likely since Convention case law, debates in Parliament, and the HRA itself strongly suggest Convention rights have an indirect effect. The ECHR is a 'living instrument' that can be responsive to change in society.

However, a gloomier perspective on the impact of the HRA 1998 on labour law has been posited by Ewing[]. The author argued that the overall impact of the Act on employer-employee relations was likely to be limited. Ewing backed up this assertion with four arguments, covering four key areas:

- Applicability of ECHR regarding employment legislation;

- Opportunities for employees to enforce rights using the HRA 1998;

- Ability of UK courts to interpret human rights legislation in favour of employees;

- Alternatives to the ECHR and HRA 1998 for protection of workplace privacy.

Firstly, the ECHR applied to a very narrow range of employment issues. Indirectly, limited use has been made of Articles 6 (right to a fair trial), 8 (right to a private life), 9 (freedom of thought, conscience and religion) and 10 (freedom of expression). However, Articles 8-10 are heavily qualified, with exceptions granted 'in accordance with the law' and for actions 'necessary in a democratic society'. On paper, the right most likely to apply to protect employees' rights is Article 11 (freedom of assembly and association). Yet Strasbourg case law has been disappointing in this area - failing to deliver any meaningful protection for trade union activities while being used as an instrument to undermine trade union security[].

Secondly, the HRA itself provided limited opportunities for direct and indirect enforcement by workers. Comments by the Lord Chancellor in the House of Lords suggested that it was unlikely that the HRA would apply to employees in 'mixed function' companies such as Railtrack that have public as well as private duties[]. Such restrictions, therefore, represented a significant narrowing of the potential for direct enforcement of Convention rights by workers. Thirdly, the impact of the duty on UK courts to interpret legislation has been diminished by the narrow interpretation of these rights by the Strasbourg authorities and by the equivocal nature of the rights themselves. Section 7 of the Act stated that proceedings may be instituted only against a public authority.

Ewing concluded stating that incorporation of Convention rights - a useful basis for filling in gaps - was no substitute for carefully tailored legislation dealing specifically with matters such as workplace privacy and various forms of discrimination. The potential for effective application was at best uncertain and highly speculative, and there was the 'incontrovertible fact'[] that the interpretation of ECHR protected rights in Strasbourg had not recognised the calls of workers and trade unions. Indeed, in terms of incorporation, the author looked towards giving the same status in UK law to other treaties such as the Council of Europe Social Charter and the International Labour Organisation (ILO) Conventions 87 and 98[]. They may prove altogether more useful in terms of protecting labour rights. Essentially, this is a considered and direct article that deflated some of the bold claims made - as well as scotching the scaremongering conducted in certain political circles - since the HRA was passed by Parliament.

4.2.2 Developing Employee Data Protection Policy

A detailed policy statement on the regulation on protection of employees' data was been

drawn up by Simitis in 1999[]. The author - a leading force behind Europe's first sub-national data protection law in Hesse, Germany - believed that employees needed to be empowered to protect their own privacy. This is the reverse of current situation where the onus appears to be on employees, and the community at large, to show that surveillance is not necessary. The author defined eight areas - closely linked to the DPA's eight data protection principles - as being crucial to the regulation of employee data. Chief among these, were the way the data is collected, with informed consent of the employee being crucial, and the collective rights of the employees.

In many ways, the last factor summarised Simitis' point - that employees, collectively through representatives, should at least be informed and consulted prior to the introduction or modification of automated data processing systems; before direct and indirect electronic monitoring; and as to the purpose, content and prospective uses of any questionnaires or tests. However, it is highly unlikely that organisations, particularly in the UK, would accept such an increase in regulations. The course that the UK government has chosen to regulate employees privacy is altogether more moderate, as demonstrated by the *Lawful Business Practice Regulations 2000*. This measure actually legally permits employers to read staff emails and monitor websites visited by staff - if they *think* an employee is committing a crime or doing something 'unauthorised'.

At the same time, the OIC's recent draft Code of Practice in this area is almost certainly relevant to monitoring of personal electronic communications such as email. According to the draft Code, employers have to ensure that monitoring is in such a way that it does not intrude unnecessarily, otherwise employers who acquire information under the *Lawful Business Practice Regulations* could still be prosecuted by the OIC. The employer clearly needs a system that complies with three Acts - the DPA, HRA and RIPA - so the one most favourable to employees will determine how much employers can intercept. Currently, the DPA's draft Code of Practice offers most protection. However, this code is not due to be finalised until the end of 2001[].

4.3 Media debate

In this subject area, it is the press that have been raising awareness and highlighting inconsistencies. In March 2000, a piece by Langdon-Down considered the whole culture of surveillance[]. The article welcomed the enhanced access to personal information, including manual files, brought about by the DPA 1998. Additionally, the introduction of the concept of sensitive personal data - relating for example to race, religious beliefs, and medical circumstances - was highlighted. Only to be processed for specific purposes with the individual's explicit consent, it should, it was argued, outlaw employment blacklists. Nevertheless, concerns were expressed in the article regarding the Information Commissioner being powerless to monitor compliance or carry out checks without the consent of the data controller in the absence of a complaint. This is a power considered essential in most EU countries, and its absence could enable companies to ignore the data protection regulations -providing an employee does not complain.

More recently, there has been a furore concerning email monitoring. Publicity has been given to staff suspensions - and some sackings - for circulating inappropriate emails at

Norton Rose, Royal Sun Alliance and Sellafield, amid TUC concerns that employers were overreacting in wake of RIPA[]. Further to this, in April 2001, psychometric testing entered the news with a report concerning the dismissal of a B&Q employee following the return of the results of a personality test conducted prior to commencing employment []. This was in spite of his being promoted during the period he was employed at the store. Thus, with the publication of the OIC's draft Code of Practice imminent, the current debate surrounding workplace privacy and employer-employee relationships is proving highly relevant.

5. Conclusions

At this early stage, three strands of the debate can be identified that are of particular interest with regard to the UK:

The challenge of balancing the competing interests of personal privacy against the ability of organisations to use personal data in their day to day activities.

This has proved particularly problematic for the UK government, enacting a Data Protection Act that specifically failed to mention 'privacy' and raising questions as to whether the Data Protection Directive has been fully incorporated into UK law.

The possible development - in the absence of privacy legislation - of privacy common law by the UK courts.

The method of incorporating the ECHR into UK law devised by the government has ensured that the HRA guarantees the right to privacy. However, an individual cannot take action in breach of that right alone. The ruling involving Catherine Zeta Jones suggested that, although the HRA is still in its infancy, a privacy common law remains a distinct possibility.

The regulatory morass regarding privacy in the workplace.

In particular, the relationship between the *Lawful Business Practice Regulations* and the *Draft Code of Practice: The use of personal data in employer/employee relationships* is causing confusion. The OIC believe that the two can work in tandem, but trade unions and employers' organisations remain to be convinced[]. Additionally, it is unclear to what extent the HRA will safeguard employee privacy. In this debate, commentators such as Jay and Hamilton, and Ewing take a pessimistic view. They argue that the text of the ECHR is limited, and that employee protection is unlikely to extend to the private sector. Ewing goes further, looking towards other international treaties for greater labour protection. Singh and Palmer are more optimistic. Whilst acknowledging the limits set out in the text of the HRA, they view the ECHR as a 'living instrument' that will be interpreted more liberally by the UK courts.

There is considerable ambiguity as to whether recent UK legislation offers adequate protection for individual privacy. However, both the HRA 1998 and the DPA 1998 are recent Acts of Parliament, with little case law so far. Consequently, the bulk of the

literature concerning the legislations' impact on the workplace has been necessarily speculative. Critical journal articles are emerging as the academic and legal community research into these issues. It is expected that further academic literature will appear in the future.

Moreover, comparative studies have increased the knowledge of experience overseas. Indeed, the EU Data Protection Directive can be viewed as a testament to incorporation of some of the diverse legislative strands identified by Bennett - particularly the ombudsman approach from Germany, and the promotion of sector specific codes of practice which are especially strong in the Netherlands. Methodologies have been developed and applied to measure adequacy of data protection legislation[]. Finally, there is a flourishing and vibrant debate in this field - with contributions from civil liberties organisations, the quality press, academics and discussion groups. Various fora for exchanging ideas exist - providing important stimuli for the future development of data protection policy research.