Privacy Issues as Limits to Access

Charles D. Raab
School of Social and Political Studies,
The University of Edinburgh, Scotland, UK

DRAFT: NOT FOR QUOTATION

Introduction

How far should privacy protection limit access to public sources of information? The answer is not so straightforward as the simple and conventional construct, 'privacy *versus* openness', would lead us to expect. As the debates about access to government-held information have progressed into the age of online dissemination of information, the extent to which principles and laws of privacy protection that originated in their contemporary form more than thirty years ago can, and should, still exert an influence over greater accessibility, has taken on some new dimensions. The place of privacy protection in the context of access is limited in scope but fundamental in importance, and it remains controversial. This is not least because both access to information and privacy protection are regarded as human rights, and are enshrined in important international instruments including the European Convention on Human Rights. It is also, and particularly, because the reflection of these rights, and their interaction, in a variety of technological and economic contexts is highly complex, and because it is at this level that different patterns and conflicts of interest make themselves felt. This gives policy-makers, regulatory officials and the courts plenty of work to do.

This paper cannot answer the normative question. Instead, it will review the way in which, over a period of years, the question of the protection of privacy has woven its way in and out of policy and debate about access to public sector information - sometimes seriously, sometimes in a perfunctory way, but only occasionally as the main issue in the midst of what have been seen as major obstacles to the development of the information society and the information market. These variations in salience may be attributed to the different interests involved either in emphasising the importance of protecting personal data in the information market, or in relegating it to a position of considerably less importance in the light of other objectives and other impediments to information access. Three prominent and overlapping areas in which access to public-sector information raises concerns about the protection of personal data are the regimes of 'freedom of information' (FOI) or 'open government', uses of public registers and similar collections of public information for commercial or other secondary purposes, and the sharing of personal data across different domains or sectors. In all of them, the basic questions are similar: how far does, or should, the fulfilment of the aims of accessibility overrides the claim or right of personal privacy? is privacy best thought of as a barrier to access? how should any conflicts be resolved? The brief discussions in this paper aim to cast light on these questions and to illustrate the particular contexts that generate them.

Freedom of Information

At a general level, access to public-sector information is the subject of laws and regulations for FOI. We cannot deal extensively with FOI as such here, except to note the privacy implications of such access regimes. These were canvassed in detail in the early 1980s by Burkert (1983), who described the legal positions for FOI and data protection in a large number of European and other countries. The observation was made that 'data protection and freedom of information become partly conflicting partly complementary objectives for information flows between the public sector on one side and the private sector and individuals on the other side' (Burkert, 1983: Management Summary). The analysis considered the way privacy exemptions in FOI laws acted in relation to the operation of data protection laws tending in the same direction, possibly leading to integrated legal solutions to bring together approaches whose historical trajectories were quite separate in many countries.

Debates about these approaches have continued to reappear in the context of countries legislating for FOI or for data protection for the first time, as for example in Central and Eastern Europe in the 1990s and in the articulation of the United Kingdom's new FOI law of 2000 with a pre-existing data protection regime. Integrationist approaches seek to keep conflicts within one decision-making framework, and to deal comprehensively with issues of law, information management and information technology as they arise in specific instances. As Burkert (1983: p. 120) argued, 'reflections on freedom of information and data protection go hand in hand with reflections on the automated handling of information and the introduction of information technology in general. It is this over-all perspective following the inherent logic of the information and communication systems approach which leads to reflections and practices to integrate freedom of information and data protection legislation…'. Thus access and protection issues must be seen as part of a wider development of information policy involving technologies, systems and rules operating within the public sector and between it and the private sector, covering not only the processing of data within organisations but their flow across these domains, and across national boundaries as well. More modestly, perhaps, examples of integration of laws and regulatory authorities, at least, can be found in the jurisdictions of Hungary, British Columbia and, less clearly, the United Kingdom (with the exception of Scotland).

Laws that provide rights of citizen access to public-sector information, or other instruments that aim to put otherwise closed information in the hands of individuals and groups, are widespread, and the list of FOI countries is growing. Because collections of public-sector information include large amounts of information about identifiable individuals, a typical resolution of a conflict between the important human rights of privacy and access to information is by means of an exemption that makes personal data inaccessible to anyone besides the individual herself. The general rule of FOI laws is that the right of access to non-personal data should not be limited by discretionary decisions whether to grant access or not that may arise from the requester's having to give any reason for wanting access, and whether she was a proper person to have the information. Discretion is, however, exercised where judgements are made about the harm that might be caused to the state by the disclosed information. Nonetheless, FOI laws place out of bounds solutions to the privacy/access conflict that rely on

considerations of the uses to which the accessed data might be put; they thus invert the use-limitation principle of data protection.

Public Registers and Records

Public registers and the like pose more difficult issues, and have attracted considerable attention in terms of the privacy-invasion risks to which persons might be subjected through the exploitation of particular registers in commercial operations or for secondary public-sector purposes. An enormous amount of personal data is maintained on public registers of a wide variety. For the United States, Gellman (2001) describes these as including drivers' and occupational licenses, motor vehicle and voter registrations, property tax, police and court records, and regulated activity records, in addition to records of political contributions, financial records, and many more at local, state and federal levels. Some of these are accessible through online searches. In many other countries, population registers, credit registers, company registers and others may be found; variations in access rules have been perceived as a problem in the European Union. Every country has its own vast inventory of records, and the use of such data beyond their primary function, including matching and electronic manipulations, poses acute privacy risks.

There is no need to rehearse these problems here at length, for they have formed many of the basic, well-known scenarios of surveillance societies that have shaped the law and practice of privacy protection. Some of these problems affect commercial operations and industries in relation to customers and consumers, while others involve relationships between the states and citizens in the context of the obligations and entitlements of public services and public order. Controversy has surrounded, for example, the availability of electoral registers, particularly online. In New York City, the availability of voters' street addresses and party affiliations on a website[1] for voters' self-registration generated public concern in 2001 over privacy invasions until those two pieces of information were subsequently removed. Until then, anyone knowing the name and birth-date of a resident – say, a famous movie star, the target of a grudge, or the subject of one's stalking – could obtain data which, in these contexts, were sensitive. The decline of 'practical obscurity' in an online environment has had growing consequences for privacy, has challenged assumptions about the primacy of public access, and has pointed up the need to reconsider the relationship between these discrepant values in the context of very specific circumstances. The accessibility of registries of sex offenders, whether available online or in more restricted form, is a case in point; most American states publish these although the legality of publishing them electronically has been decided differently in the courts of different states (Harmon, 2001).

The accessibility of public registers in the UK also illustrates controversy and principles in flux. A study by Davies and Oppenheim (1999) identified and discussed a large number of registers in the UK but concentrated particularly on the largest one, the electoral register. The electoral register is provided free to elected members of local authorities but can be purchased by others, on paper or electronically. The electronic

[1] http://www.registeredtovoteornot.com; see Harmon (2001). For an example of controversy over California birth records, see Coleman (2001).

version's cost has apparently deterred credit reference agencies from purchasing it; instead, they buy the paper copy and send it abroad to be re-keyed at low cost for further processing[2]. Resultant inaccuracies have reportedly had consequences for credit-granting decisions about individuals. Misuses of the register that expose people to risks also arise from the rearrangement, manipulation and combination of the data with other , although risks also result even from the register information in its untouched form. It is possible that the register could be put on the Internet although that was not yet contemplated by the local electoral officers consulted. Attempts to protect privacy by restricting the public availability of the register would be resisted by the direct-marketing industry. Other industries invoke reasons that seem to them legitimate for wanting to maintain no or few restrictions upon access to particular registers. There appeared to be little public concern about abuses of register information.

In the following year, the new Representation of the People Act 2000 changed the rules for the electoral register, following deliberations by a Home Office Working Party. There are now two versions of the register: a complete one restricted to use for electoral purposes and for a very few other limited purposes (to be determined in regulations), and another one, available for general sale, in which voters can choose to opt out of the inclusion of their information. This was welcomed by the Information Commissioner as 'a significant step forward in protecting privacy' (HC 575, 2000: pp. 35-6). The Commissioner pointed out that it was technological development - the provision of electronic registers - that had removed the restrictions on dissemination in practice; even paper copies could now be electronically scanned and made ready for further processing. An example of the commercialisation of the electoral register that had caused complaints was UK Infodisc, distributed by CD-Rom and on the Internet. UK Infodisc combines register data with telephone numbers to enable more sophisticate location of individuals for marketing purposes. The Commissioner believed that this might violate the Data Protection Act, but the legal complication was that UK Infodisc was not compiled within the UK. Products of this kind, she claimed, would now be affected by the new opt-out electoral register. But the privacy problems of other accessible registers remained, and UK Infodisc had now used the register of directors and secretaries to bring out a similar product supplying home details of some 3 million of these persons and their domestic co-occupants.

Other registers were also being abused: the Commissioner also reported that shareholders of a firm connected with live-animal research had received offensive mail, and that shareholders of privatised public utilities had been the recipients of political party mailings (HC 575, 2000: p. 36). The policy implications for the information market were underlined in the Commissioner's observation that '[w]here individuals have no choice but to supply their personal details for inclusion in a public register, they should have the reassurance that there are effective controls in place to ensure that information can only be used to support the purpose for which the register was established. Where there are no controls or controls are ineffective, there must at least be a question over whether the position is consistent with Article 8 of the European Convention on Human Rights' (HC 575, 2000: pp. 36-7). She therefore welcomed any

[2] Whether this practice falls foul of he prohibition on data transfers to countries with 'inadequate' data protection is a good question.

legislative moves to bring some measure of privacy protection to other registers besides the electoral register, by restricting their availability[3].

It is worth noting that the necessary regulations governing the two versions of the register had not, as of November 2001, been made by the UK Government, although the electoral register for 2001 came into effect in February. Meanwhile, however, a case was brought to court, and won, by a man who he refused to register to vote (a criminal offence) because he objected to the unconsented transfer of his personal information by Wakefield Council to credit-reference and direct-marketing firms through sale of the electoral register. He had declined to register because an uncreditworthy person had fraudulently used his personal details. The man claimed that his right to privacy and right to vote was breached; the judge held that the sale of the register without giving the plaintiff a right to object was a 'disproportionate way of reaching a legitimate objective', which the government had apparently described in terms of the benefits of disclosure for consumers, suppliers, the economy and the community (Dyer, 2001; Parker, 2001). Since this decision, local authorities were advised to stop the sale of the register to commercial organisations pending consultations at Ministerial level, or until new regulations can be brought in. But the cessation of sales of the electoral register is at the centre of a dispute within Government because the Treasury is reported to be 'alarmed that the move will seriously undermine the Chancellor's efforts to clamp down on money-laundering by criminals and terrorists…in the wake of 11 September' (Harrison, 2001).

There is little space here to investigate solutions to the dilemma of privacy in the context of public registers, although Stewart's (1999) multi-stranded approach seems the most sophisticated way of tailoring privacy strategies to the circumstances of these registers. Briefly, he assesses the strengths and weaknesses of five approaches. These are:

'1. Let general data protection laws solve the problems;
2. Apply data protection laws in a limited fashion;
3. Tailor the laws establishing registers to address privacy issues;
4. Look beyond the register tom users of register informatin;
5. Supplement data protection laws with special rules on public registers.' (Stewart, 1999: p. 87)

Each of these has its place, although the first one is the weakest, for the alternatives it embraces - complete exemptions for registers or repeal of exemptions – does not answer the problems that are currently faced. The second one is a small advance, while the third is a long-term strategy, based on intensive study, but which is unlikely to have much appeal in the short term. The fourth one applies controls to the users of public information, but may be ineffective on its own. The fifth, in Stewart's (199) view, has much to commend it, and is exemplified by Part VII of the New Zealand Privacy Act 1993[4], which applies special principles to public registersStewart (1999: p. 95) believes that the fifth one, in conjunction with the second and third strategies, offers the most

[3] The Commissioner is reported to have told the Home Office Working Party that the electroral and shareholders' registers had been used to compile lists of wealthy widows living alone; see Dyer (2001).
[4] Available at http://www.knowledge-basket.co.nz/privacy/legislation/1993028/toc.html

effective solution. This is an interesting approach because it appears to be addressed to several desirable requirements for change, and because it avoids 'off-the-shelf' remedies that might be applied without careful thought and negotiation.

The privacy issues involved in public access to information have also been the subjects of regulatory policy in terms of specific legal instruments or authoritative guidelines. Thus the Council of Europe's Recommendation No. R (91) 10 of 1991 sought to counter the threat posed to privacy by the electronic storage and third-party access to records collected by public authorities for administrative purposes. It applied data protection rules to these collections and disclosures, based on the Council's 1981 Convention on data protection, and enjoined them on Member States[5]. It was also in 1981 that the Council's Recommendation No. R (81) 19 encouraged access to information held by public bodies.

European Policy Analysis and Developments

Finding the appropriate means of regulating access in accordance with privacy protection has remained a salient issue ten or twenty years after these efforts. This is especially so in the context of the intensification of data processing under the aegis of domestic and international policy initiatives of the 'information society'. These include the information market as well as the broader and deeper use of information and communications technologies (ICTs) in public administration (Bellamy and Taylor, 1998). Policy initiatives and deliberation over questions of the accessibility of public records and registers to a wider public, of the commodification of public data sources in the pursuit of commercial objectives, and of the manipulation of personal data in the course of achieving public policy aims have been pursued in other international domains as well as in national policy-making. Let us turn to consider the discussion of these issues in the European Community (EC). Some of the products of this discourse are instructive in showing us the way in which privacy protection has been looked at, and in casting light on its relative standing in the debates over the information market and the information society.

The 1989 document, *Guidelines for improving the synergy between the public and private sectors in the information market*, was a landmark in EC policy towards access. Although it is now largely discredited as ineffective and conceptually deficient, it was the culmination of several years of study and discussion among information industry players and the EC. The main purposes of the EC's information market guidelines were to stimulate the synergy between the public and private sectors in regard to the provision of electronic information services, and to encourage the use and further market-oriented exploitation of public information. Although the first guideline did refer to access restrictions for the protection of legitimate public or private interests, including the protection of personal data, it did not discuss these restrictions further. Only in regard to

[5] 'Unless permitted by domestic law providing appropriate safeguards for the data subject, the interconnection - in particular by means of connecting, merging or downloading - of personal data files consisting of personal data originating from files accessible to third parties with a view to producing new files, as well as the matching or interconnection of files or personal data held by third parties with one or more files held by public bodies so as to enrich the existing files or data, should be prohibited.' Recommendation R (10) 91: 7.1

copyright and contractual rights did the guidelines address legal or other obstacles to information services.

Simultaneous with the long process that ended in the 1995 Data Protection Directive, analysis of the issues involved in achieving better information-market synergy took place in EC and other fora over a period of years in the 1990s, providing a range of information about national policies and regulations, as well as exploring possible policy solutions. The protection of personal data played an important part in these approaches. Prominent among these investigations were the ones conducted within the EC-funded PUBLAW project, which surveyed practices in many countries and explored the privacy question amongst many other important legal and economic aspects of access. This project exemplified the work of a policy community in and around various research institutes in several EU countries including Germany, Belgium, the Netherlands and the United Kingdom, operating in close relation to the Legal Advisory Board (LAB) of the European Commission's DG XIII.

In an early report on general access to information legislation, privacy exemptions to access in several countries were noted, as well as the problem of conflicts between legislation for access and for data protection that occurred owing to the value judgements that were required in weighing up the two sides. Other problems had to do with the scope of the laws and of the bodies established under these laws, a reflection of the compartmentalised, non-integrated way in which legislation had been established in several countries. But the report also highlighted a particular problem, concerning bulk access requests of personal data through electronic means. Registers were thus available for access and further processing in a manner that posed a challenge to access laws where privacy exemptions had not been designed with such practices in mind (PUBLAW, 1991a: pp. 17-18).

The PUBLAW project cast light on the data protection issues involved in a number of more specific activities, involving population registers, registers for cars, companies and credit risks, among others. The availability, from late in 1990, of the first draft of the EC's data protection directive provided a tool for analysis of the way in public access to these registers might be governed by a more harmonised European regime of data protection. It also pointed up the variation in law and practice across Member States in terms of the organisation, accessibility and closure of different collections of personal data. The variation in regulation was regarded unfavourably in terms of achieving the single market, particularly where - as with car registers - the information was economically important (PUBLAW, 1991b). The argument was that a directive - and perhaps a sectoral one - would set out the criteria for judging whether the transfer of register data from the public to the private sector constituted a change of purpose, and was thus in breach of data protection principles.

In the case of company registers, an issue was whether the commercially valuable transfer of bulk data to private sector information stretched the meaning of 'access' and, moreover, exposed persons to privacy risks through retrieval techniques associated with the centralisation of such data (PUBLAW, 1991c). Again, the question of the purpose of a company register was seen as important in deciding whether, in the light of what a directive would say, transfers of this kind would be in keeping with privacy protection. The report saw this issue as part of a more general problem in regard to Member states'

register regulations where 'they have not consciously dealt with data protection problems. Register regulations and perhaps more generally all laws dealing with the handling of personal information in the "pre-data-protection age" can be seen as containing "tacit assumptions" on what would and could happen to personal data, tacit assumptions which are no longer valid or have to be made explicit in the era or electronic data processing' (PUBLAW, 1991c: p. 17).

As for population registers covering the major 'life events' or the whole population - a political issue in some countries in terms of fears of excessive surveillance or targeting of certain categories of persons - access to these was seen to be 'at the very centre of data protection concern' (PUBLAW, 1991d: p. 2). While noting the commercial value of such information, the project report went no further than to describe the variations in practice across a number of countries in terms of the application of limitations to access. Electoral registers were described as one type in this category; further remarks on these and other registers in the UK will be made later on.

Thus the analysis of access to information was conducted by the PUBLAW project within a framework that gave privacy protection a major role in arbitrating the limits, which some might indeed see as obstacles, but which served to place access to public sector information on a practical footing compatible with privacy rights. The exploration of information issues in the wake of the 1989 *Guidelines* continued in PUBLAW.2, which, in one report (PUBLAW.2, n.d.) was concerned to assess the implementation of the *Guidelines* in Member States. The information it conveyed included remarks about effects on the legal aspects of data protection[6], but it also gave a summary which drew attention to ambiguities in the concept 'personal data' in the light of statistical and company information, including the distinction between legal and natural persons. Legal differences across countries in the accessibility of information of these types was described as inimical to the development of information services across Europe, and definitional problems caused confusion in the private sector. These issues serve as a reminder of the tension that exists among technological, legal, sociological and perhaps cultural concepts of information, and of the practical consequences of this. This complexity is somewhat under-explored in the study of the 'information society'.

The report also noted the importance of the confidentiality rules that often protected personal information collected by the public sector, and of that sector's awareness of the respect for privacy rights. Some government departments were apprehensive, therefore, that the aggregation of data collections could increase the amount of identifiable information becoming available in the private sector. On the other hand, the report also claimed that '[a]wareness of the legal and moral constraints imposed by the need to take account of personal privacy rights may reduce the willingness of public servants to make information available for exploitation, and may in some cases be used as an argument in support of a general reluctance to release information' (PUBLAW.2, n.d.: p. 9). This problem will be considered later in the context of data-sharing within the public sector. The report recommended that the term 'personal information' be clarified, and that the Legal Advisory Board (LAB) of the European Commission's DG XIII

[6] It remarked rather oddly that '[p]ersonal data protection is not regarded as a major issue in Germany' (PUBLAW.2, n.d.: p. 59).

should look into the aggregation problem as well as in to the question of transborder data flows to countries without data protection or copyright laws[7]

Further occurrences of discussion of privacy protection in relation to access can be found in other PUBLAW.2 documents. Thus its report on North America included Canada, commended Québec for its emphasis on privacy and purpose-limitation in the face of commercialisation (PUBLAW.2, 1991: p. 28), and made an invidious but not unusual distinction between Canada, with its 'integrated approach to privacy and access to information' (PUBLAW.2, 1991: p. 15), and the United States. The dissemination of thinking continued with the succession of PUBLAW.2 by PUBLAW III. For example, a 1995 workshop in Luxembourg was informed by research conducted within PUBLAW's network of institutes. Looking prospectively at legal and regulatory frameworks for governing access to government information, it highlighted a number of privacy protection issues. One of these concerned the coherence of the distinction between personal data in the strict sense, requiring protection, and data about company directors and the like in their professional capacity, which might be accessible (Lamoulline, 1995: pp. 13-14). Another issue was the proper balance between an 'internal market' point of view and a 'rule of law' point of view reinforcing citizens' access rights; in the latter, greater clarity and, indeed, greater uniformity in the EC were needed concerning the scope of the right to access, partly in view of the data-protection limitations that were legitimately placed upon it (Prins *et al*, 1995a: p. 38)[8] Contributors to the workshop discussion raised points about the problem posed for commercialisation by the narrow definition of 'purpose' when data are collected, and about the need to differentiate among kinds of public sector in formation and perhaps devise sectoral access laws as well as general ones[9].

The project's final report in 1995 (PSI and CRID, 1995: p. 1) observed that the EC's guidelines had raised little awareness and had had relatively little effect upon the different practices of Member States with regard to improving the relationship between the public and private sectors in the information market. Moreover, the guidelines' distinction between 'raw value', contained in the public sector's information, and 'added value', produced by private sector exploitation, was flawed as an approach to improving synergy; competition between increasingly commercially-minded public organisations and private firms was becoming more common and synergy was rare (PSI and CRID, 1995: p. 79). The question of privacy was present throughout the report. Its survey of Member States and in Norway included brief accounts of each country's data protection legislation as it affected the flow of information from public sources to the private sector. Broad-brush research conducted in these countries seemed to indicate that, in varying degrees and in different ways, data protection was - or at least was considered by some policy actors - to be a barrier to the exchange of information or to commercialisation in Austria, Denmark, Finland, Germany, Ireland, Luxembourg, Spain and Sweden. The picture was more mixed, or not established, in Belgium, France Italy, Portugal and the United Kingdom. Norway was seen as the least restrictive in regard to the effect of data protection law upon the public availability of personal information and

[7] The transborder data flow issue was dealt with in the 1995 Data Protection Directive 95/46/C.
[8] This contribution relates to a larger study, Prins *et al.* (1995b).
[9] On this point, see especially the interventions by Messman (pp. 62-3), Burkert (p. 64) and Seipel (pp. 76-7), in European Commission, Directorate General XIII (1995)

upon its commercialisation. It is of interest that in Greece, which still had no data protection legislation in 1995, the view of some commentators was that it was the *absence* of regulations that contributed to inhibitions on the commercial exploitation of government information.

Yet the report concluded with the arguably overstated generalisation that '[t]he question of personal data protection does not seem to pose major problems with regard to marketing public data, as the marketable information is not generally personal' (PSI and CRID, 1995: p. 73). It observed that anonymisation of data could help to overcome restrictions, as for example with regard to statistical data, but that there were certain kinds of data for which access or protection regulations were not clear, thus posing problems; for instance, telephone data and data about company directors or shareholders. It observed that the purpose of data processing was of prime importance in regard to personal data, and that the commercial dissemination of personal data is only acceptable if it is laid down in law or if consent has been obtained from the person concerned. Thus it recommended that a distinction be drawn 'between personal data in the strict sense, which cannot be published without the consent of the interested party, and occupational data, which may be disseminated' (PSI and CRID, 1995: p. 81).

Perhaps in the context of many of the barriers to access to public information, privacy considerations are indeed among the less important obstacles and are overcome with less difficulty. On the other hand, as reflected in the Stockholm conference mentioned earlier, there is the view taken by Yves Poullet, one of the PUBLAW project's leading participants, that '[e]stablishing harmony between the imperatives of data protection legislation and those of legislation for administrative transparency in the public sector is really no easy thing. It is not a question of prohibiting all marketing of nominative data held by the state, but of posing certain limits' (Poullet, 1993: p. 5). This view is in line with the emergent consensus that the finality principle - purpose specificity - might form one of the pillars supporting the legitimacy of communicating personal data to third parties. Earlier on, the final report of PUBLAW.2 (n.d.) had concluded, as we have seen, that public sector information personnel generally saw the need to respect privacy, and that they observed laws or understandings about confidentiality. In particular, information was safeguarded from third-party uses which might breach privacy rights through the disaggregation or analysis of the data in certain ways, and there were sometimes legal provisions reinforcing the purpose-specificity principle.

The LAB's response to the European Commission's *1995 Green Paper on Copyright and Related Rights in the Information Society* found a space for regretting the absence of 'considerations of informational privacy and freedom of expression' (Legal Advisory Board, n.d., p. 3), although they were at stake in any reconsideration of copyright in a digital networked environment. The LAB's two considerations were high on its own agenda of focal points in studying the legal problems of the information market, and it therefore recommended that the Commission give these sufficient weight in any policy initiative in the area of intellectual property rights (Legal Advisory Board, n.d., p. 4).

On the occasion of the European Commission (EC)-sponsored conference on access to public information, held in Stockholm in 1996, there were some interesting contrasts of attitudes toward the importance of privacy protection. Stefano Rodotà pointed out the three Ps that are encountered on the road to electronic citizenship: property,

pornography, and privacy (Rodotà, 1996). Privacy comes last in this formulation, after juicier or thornier issues, although Rodotà's own prominent role as a staunch defender of privacy rights is celebrated. In discussing threats to openness that come from new ways of handling information, Peter Seipel, a leading participant in the development of information privacy policy over many years, quoted another Swedish author as saying that '[I]f the old riksdag of noblemen, clergy, burghers, and peasants had approached the printing press with the same attitude as the lawmakers of today approach the computer, then there would never have been any freedom of the press in 1766' (Seipel, 1996)[10]. Seipel saw a threat arising when privacy protection is over-emphasised to the detriment of freedom of information. For his part, Henry Perritt, Jr. observed that '[p]rivacy is the toughest problem for reengineering dissemination policy because so much of the commercially valuable information involves personal data' (Perritt, Jr, 1996).

The implication of all these contributions was that privacy - whether for good reason or bad - had at least to be contended with. Regulation may be important, but over-regulation was to be avoided. Who should decide the appropriate way of doing this remained unstated, although of course it has been a main subject in the work of these and other commentators. However, personal data constitutes only a proportion of the information held by the public sector, for which Perritt saw Europe as having a regulatory advantage over the United States because it was further along in the establishment of data protection laws and systems. For this subset of information, Perritt, like others, saw that '[t]he starting point conceptually is to subject public information within the scope of a general privacy protection regime to the regime, and let it operate in the usual way' (Perritt, Jr, 1996).

However, surveys of national practice suggest that this seems almost to take the issue off the road too easily, for there may be no 'usual way' in a particular country, or the usual ways may differ across countries, when it comes to some of the particular privacy issues that arise when public sector information is used for further administrative or commercial purposes. These issues may require common approaches through general legislation, or perhaps special legislation covering particular kinds of public records and registers, earlier commentators have shown. Moreover, the 'usual way' may incorporate the resolution of conflicts only after long and sometimes litigious processes aimed at clarifying ambiguities. Stewart's (1999) approach, mentioned earlier with regard to public registers, would appear to be more constructive approach.

Finally, on behalf of the EC, Ulf Brühann pointed up these areas of real or potential conflict between access rights and personal privacy (Brühann, 1996). He located privacy protection alongside protection of the general interest, including state security, defence, and law enforcement, within the scope of restrictions on access rights. Brühann argued that technological developments were now exposing the individual to new risks of privacy invasion through the ability of these technologies to exploit and manipulate data in new ways. Referring to the newly-adopted Data Protection Directive 95/46/C, he highlighted the points at which it was commonly thought that privacy was incompatible with public access. These had to do with purpose limitation, time limitation, the lawfulness principle, the protection of sensitive data, and the principle of informing data subjects about any disclosures and the persons to whom their data were disclosed. The

[10] The quotation is from Anders R. Olsson, *Information Technology and the Free Word*

question was whether these blocked the path of public access to official documents, but the Directive (Recital 72) had already provided for the latter to be taken into account in its own implementation. However, Brühann's more interesting argument was that, at a theoretical level, there was no conflict. 'On the contrary', he claimed, ' both principles can be seen as necessary and complementary elements to serve a more basis constitutive objective of a democratic society: to create the conditions under which the individual is able to fully participate in the democratic process in a given society. In that way data protection can be seen as a necessary part of a more general set of rules on allocation of information in a democratic society' (Brühann, 1996).

Privacy as co-equal to openness in a democratic society is an attractive position to take on the level of principle, and I have argued for it myself elsewhere (Raab, 1997). Yet on the lower-level planes where tensions and cases arise in practice, and where interests are more sharply focused, it is not so easy to sustain this 'best of all possible worlds'. Thus Brühann's discussion had to invoke, for example, the finality principle as a real limit to secondary use or re-use of public data where such use - perhaps for commercial gain - falls outside the orbit of the purpose for which it was collected, and even outside the complementary aim of public access, which is to contribute to the workings and debates of a democratic system of politics. In cases involving commercial re-use and the data protection principle of purpose specificity, resolving the issue could appear simple: human rights trump commerce. But in the case of secondary use for other purposes within a broader framework of government in which complementary and equally important democratic purposes are being served by this form of access, we still remain in the idiom of conflict or tension. This is because, as Brühann points out, '[s]econdary uses for different purposes may change the quality of personal data. Data which have been relevant, up to date and complete for one purpose may not qualify the same way in another context. Moreover, they may have been obtained through obligatory procedures which may limit future use for fairness reasons' (Brühann, 1996). Moreover, as Gellman (1999: p. 85) has pointed out, 'defining purposes for a public register can be difficult. If a legislature provides that a register is available only for careful specified uses, then the difficulties may be minimal. But legislative priorities change, and the purposes for which records were collected can be expanded or altered. In some instances, no clear purpose definition can be found in legislation on public registers. In other instances, the purposes have clearly changed over time.'

These considerations may be true of data that remain within the sphere of non-commercial public organisations. Thus, to follow Brühann, we have more principles of data protection, concerning data quality and fairness, being brought to bear upon the legitimacy of further use even within the public sector, and in another part of the state. That raises issues of access to, and control of, information held in public databases that privacy protection has perhaps had less to do with, because the flows involved are not necessarily ones that that cross the (already blurred) boundary between the public sector and the private or commercial sector. Yet privacy protection principles and practices are implicated in these flows and may arbitrate the quality of democratic life, depending on how they are applied, interpreted, or set aside. As it affects data-sharing, this situation will be touched on later.

In other circles of the EC, the question of access to information has also attracted commentary and the formation of responsive positions from a privacy perspective as

successive initiatives have emerged from the information market policy process. The most prominent of these, *Public Sector Information: A Key Resource for Europe*: *Green Paper on Public Sector Information in the Information Society* (COM (1998) 585), is a culmination of consultations following what we have seen earlier as the EC's attempt to devise a framework or regime for access to public sector information. Emphasising the advantages of better access to information for workers, businesses, citizens, and of course the information industries, it complained about the absence of European rules establishing conditions for private-sector exploitation of public-sector information, and about the lack of clear and consistent principles across the Member States. It recognised the abiding problem, that of squaring the commercial information market's implications for citizens' access with the implications for fair competition if the public sector added value to and commercialised its own information. Of some importance to the discussion of data- sharing later in this paper, it put the access question in the contexts of technology and of electronic government, including communication between different administrations and between government and the citizen or business. In particular, it argued that the use of new technologies 'gives public bodies the possibility to share available information when this is in conformity with data protection rules…. Sharing information leads to better informed public bodies, that have access to all data relevant for their functioning.' (paras. 56, 57). One-stop shops or services would be facilitated in this way[11].

Reflecting some of the issues that had surfaced in the previous years, the consultative Green Paper sought advice on clearer definitions of the 'public sector' and classifications of 'public sector information'. It asked for views on what the conditions of access should be for citizens and businesses, and noted privacy as one of the grounds for exemption of information from access. Its treatment of the privacy question saw 'balance' as the main solution: where identifiable personal data form part of the 'commercially interesting information' for marketing or research, as in registers or other records, 'the right to information needs to be balanced with the individual's right to privacy. All national access laws show awareness of the need for such a balance' (para. 110). Moreover, the 1995 Data Protection Directive 'achieves the necessary balance' in question, and 'must be fully observed in cases of personal data held by the public sector' (para. 111). The responsible public bodies must apply the balances, taking into account the purpose-limitation principle and others; national supervisory bodies and the courts play a role here (para. 112). Statistical data was seen to be covered by the confidentiality principle, which stops leakages (para. 113). Finally, it said that '[t]he emergence of the information society could pose new risks for the privacy of the individual if public registers became accessible in electronic format (in particular on-line and on the Internet) and in large quantities' (para. 114).

This way of disposing of the privacy issue seems complacent and formulaic, an invocation of the doctrine of 'balance' that merely postpones the issue and ignores much of the deliberation of many years over the great difficulty in reconciling conflicting principles and rights in actual cases. The fact of the existence of 'balanced' directives and national laws, as well as supervisory authorities and statistical procedures, cannot

[11] Data protection issues in the sharing or accessibility of data are only rarely and patchily described in many accounts of one-stop government services, and are mainly considered in terms of legal and technological aspects of data security; see Hagen and Kubicek (2000).

simply be waved defensively at real issues of privacy and public access[12]. If they could, then the Green Paper's consultative question, 'Do privacy considerations deserve specific attention in relation to the exploitation of public sector information?' (para. 114, Question 7) would appear redundant. Moreover, to place only in the *future* the privacy risk of electronic access to registers is rather strange.

It was therefore not surprising that the comments of the Working Party established under Article 29 of the Data Protection Directive were somewhat critical, although they still pitched their argument within the 'balance' and appeared to (Working Party etc., 1999). They urged a case-by-case, step-by-step assessment of whether personal data should be accessible, under what conditions, and in what media. They also reasserted the purpose and legitimacy principles, the obligation to inform the data subject and the latter's right to object, and they advocated the use of technologies to protect privacy inn respect of on-line data. The Communication of 23 October 2001, *eEurope 2002: Creating a EU Framework for the Exploitation of Public Sector Information*, was based on the Green Paper. In looking forward to a possible new directive on public sector information within the 'eEurope' programme, it had almost nothing to say on the data protection question beyond reaffirming the importance of compliance with data protection rules.

This excursion into the history of how privacy issues have been handled within European discourse can only conclude that the airing of these issues has had some effect in entrenching some appreciation of the relevance of privacy protection as a condition of public access to information, although not necessarily as a limiting factor, and perhaps as a fairly precarious countervailing value. It is interesting that one of the most frequently mentioned issues in parallel European debates and policy initiatives towards an information society, that of public trust and confidence in the 'information superhighway', has been virtually absent in the language and conceptual formulae of the information-access-and-privacy debate. As seen in the initiatives of the era of the Bangemann Report and thereafter, the trust that privacy protection would promote was considered as a necessary prerequisite to the encouragement of transactions in e-commerce and e-government. This was true not only in the EC, but in other countries as well (Raab, 1995, 1998). Why no similar argument appears in the documentary materials or the conceptual thinking of the subject of this paper deserves further investigation beyond the scope of this discussion. Speculatively, the answer may lie in the way different policy networks operate, and within different institutional structures.

Data-Sharing and Privacy in the Public Sector

Finally, something should be said about a form of access to public records which is not concerned with commercially-related transfers from the public to the private sector, but with transfers within the public sector albeit from one agency or department to another. What brings this within the orbit of the present discussion is the question of using data for purposes other than that for which they were collected, and also the questions of transparency and consent which they involve in a similar way to the issues involved in public access to information more generally. Under the label of 'data-sharing', we are

[12] Garlic and a crucifix might in some circumstances be just as effective. I have elsewhere (Raab, 1999) offered an extended criticism of the doctrine of 'balance' in data protection.

seeing greater pressures to amalgamate personal data into new collections or to transfer across organisational boundaries in ways that may be constrained or forbidden by privacy laws or the laws of confidence. Politicians and administrators justify the use of data in these ways in terms of the modernisation or 'joining-up' of government, improving the delivery of services to the citizen, developing 'one-stop-shop' systems that exploit technologies to advantage in terms of efficiency and effectiveness, and so on.

It is becoming increasingly hard for plans for data-sharing to make much headway without considering their privacy implications, and in some places - the UK, for instance - there is evidence that government planners are taking these into serious consideration (Raab, 2001). The problems, however, include the difficulty of agreeing on the limits to which collections of data can be shared or matched beyond their original purpose if the public policy purposes seem legitimate, whether in terms of better services, combating fraud in the welfare state, promoting law and order, targeting programmes either geographically or socially, promoting new ways of teamworking for health and social care, or integrating processes across the disparate, but mutually functioning, institutions of the criminal justice system. Achieving some of these aims may involve applications of ICT that require special social innovations such as identification cards and the apparatus of authentication and verification of individuals and their entitlements. If so, then public apprehension about what happens to personal information, or about what may be perceived as surveillance, may become an important factor arbitrating success or failure. But there are many other issue involved in the sharing of data in the public sector, not the least of which is the quality of the data that is shared, which has implications for the efectiveness and eficiency of these plans, but also for adherence to several of the relevant data protection principles. On the research side as well as the clinical side of health care, the vexed question of informed consent, perhaps especially where disease registers are involved, has been a matter of great debate implicating our questions of privacy and access[13].

It may also be especially difficult, as well, to invoke privacy considerations, or indeed to launch new joined-up initiatives in a climate of perceived crises that seem to require more intensive gathering and collating of information and intelligence. The current fever of anti-terrorist activities, in which what might have come to be regarded as protected data bases are rendered accessible through the exercise of old or new legal powers, may have changed the nature of the trade-off between privacy and other values that takes place in domains remote from the current climate of insecurity

Conclusion

The question of the protection of personal information in public-sector collections of information has many dimensions. This paper has only referred to a few of them in illustrating some of the discussions and policy actions involved in increasing the accessibility of public records and facilitating its flow for many purposes and in many domains. Conflicts of values and interests shape these issues; how these conflicts can be resolved has been a focus of privacy discourse and practice for a very long time. Various

[13] Owing to a considerable delay in the publication of UK Cabinet Office proposals for data-sharing and privacy, it is not currently possible to extend the discussion of a number of these points.

instruments, principles and formulae exist and have been applied to each new situation where the conflict arises. Assuming they are implemented in practice, these are powerful mechanisms for dealing in a simplified fashion with most situations. Yet there are limits to their application. The pressures to resolve problems in the governmental, commercial and other contexts in which they arise make each situation the potential site of settlements for which fresh solutions need to be innovated and negotiated, thus pointing up the essentially political nature of the privacy and access issues that lie at its heart.

References

Bellamy, C. and Taylor, J. (1998) *Governing in the Information Age*, Buckingham and Philadelphia: Open University Press.

Brühann, U. (1996) 'Privacy and transparency: how can they be reconciled?', paper presented at the conference on *Access to Public Information: A Key to Commercial Growth and Electronic Democracy*, Stockholm, 27/28 June 1996. See http://www.europa.eu.int/ISPO/legal/stockholm/en/brühann.html

Coleman, J. (2001), 'Calif. Lawmakers Mull Online Records', *The Washington Post*, November 29; available at http://www.washingtonpost.com/wp-dyn/articles/A34631-2001Nov29.html

Computer/Law Institute (1990) *Confidentiality of Database Searches (CONFI) Final Report*, Amsterdam: Vrije Universiteit Amsterdam.

Davies, J. and Oppenheim, C. (1999) *Study of the Availability and Use of Personal Information in Public Registers - Final Report to the Office of the Data Protection Registrar*, Loughborough University: Department of Information Science

Dyer, C. (2001), 'Court challenge to councils' sale of electoral rolls', *The Guardian,* Thursday, 6 September.

European Commission, Directorate General XIII (1995), *Workshop on Commercial and Citizens' Access to Government Information*, Luxembourg, 26-27 June.

Gellman, R. (1999), 'Public Registers and Privacy: Conflicts with Other Values and interests', in *Privacy of Personal Data, Information Technology and Global Business in the Next Millennium*, 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13-15 September.

Gellman, R. (2001) 'Public Record Usage in the United States', paper presented at the 23rd International Conference of Data Protection Commissioners, Paris, September 24-26.

Hagen, M. and Kubicek, H. (eds*.), One-Stop-Government in Europe: Results of 11 National Surveys*, Bremen: University of Bremen

Harmon, A. (2001), 'As Public Records Go Online, Some Say They're Too Public', *The New York Times*, August 24; available at http://www.nytimes.com/2001/08/24/nyregion/24VOTE.html?ex=999677779&ei=1&en=5646

Harrison, M. (2001) 'Brown and Byers clash over money laundering', *The Independent*, 23 November, p. 17

HC 575 (2000) *First Report of the Data Protection Commissioner on the 16th Year of Operation of the Data Protection Act 1984*, London: The Stationery Office.

Lamoulline, C. (1995) 'Presentation of Publaw 3 findings. Legal Assessment', paper presented at the European Commission, Directorate General XIII *Workshop on*

Commercial and Citizens' Access to Government Information, Luxembourg, 26-27 June.
Legal Advisory Board (n.d.) *Reply to the Green paper on Copyright and Related Rights in the Information Society* The
Parker, S. (2001), 'Sale of electoral roll breaches human rights, rules judge', *The Guardian*, Friday, 16 November.
Perritt, Jr., H. (1996) 'Reinventing government through information technology', paper presented at the conference on *Access to Public Information: A Key to Commercial Growth and Electronic Democracy*, Stockholm, 27/28 June 1996. See http://www.europa.eu.int/ISPO/legal/stockholm/en/perritt.html
Policy Studies Institute (PSI) and Centre de Recherches Informatique et Droit (CRID) (1995) *PUBLAW III - Final Report*, London: Policy Studies Institute
Poullet, Y. (1993) **'**The Commercialization of Data held by the Public Sector - Legitimacy and Conditions', PUBLAW 2 Workshop, 4 March, Legal Advisory Board (LAB) File 93/1
Prins, J., Klaauw-Koops, F., Vunderdink, P. and Zwenne, G. (1995a) 'Study on a Green paper regulating Public Access to Government Information', paper presented at the European Commission, Directorate General XIII *Workshop on Commercial and Citizens' Access to Government Information*, Luxembourg, 26-27 June.
Prins, J., Klaauw-Koops, F., Vunderdink, P. and Zwenne, G. (1995b*) Access to Public Sector Information*, Tilburg: Schoordijk Institute, Tilburg University
PUBLAW (1991a) *Subject Report - General Access to Information Legislation*
PUBLAW (1991b) *Subject Report - Car Registers*
PUBLAW (1991c) *Subject Report - Company Registers*
PUBLAW (1991d) *Subject Report - Population Registers*
PUBLAW.2 (1991), *Draft Final Report – North America*
PUBLAW.2 (n.d.), *Final Report – Europe*
Raab, C. (1995) 'Connecting Orwell to Athens? Information Superhighways and the Privacy Debate, in Donk, W. van de, Snellen, I. and Tops, P. (eds.), *Orwell in Athens: A Perspective on Informatization and Democracy*, Amsterdam: IOS Press.
Raab, C. (1997) 'Privacy, Democracy, Information', in Loader, B. (ed.), *The Governance of Cyberspace*, London: Routledge.
Raab, C. (1998) 'Electronic Confidence: Trust, Information and Public Administration', in Snellen, I. and Donk, W. van de (eds.), *Public Administration in an Information Age: A Handbook*, Amsterdam: IOS Press.
Raab, C. (1999) 'From Balancing to Steering: New Directions for Data protection', in Bennett, C. and Grant, R. (eds.), *Visions of Privacy: Policy Choices for the Digital Age*, Toronto: University of Toronto Press.
Raab, C. (2001) 'Electronic Service Delivery in the UK: Proaction and Privacy Protection', in J.E.J. Prins, J. (ed.), *Designing E-Government: On the Crossroads of Technological Innovation and Institutional Change*, Boston & The Hague: Kluwer Law International
Rodotà, S. (1996) 'Citizens' participation in an electronic democracy: building an electronic citizenship?', paper presented at the conference on *Access to Public Information: A Key to Commercial Growth and Electronic Democracy*, Stockholm, 27/28 June 1996. See http://www.europa.eu.int/ISPO/legal/stockholm/en/rodota.html
Seipel, P. (1996) 'Public access to public sector-held information and dissemination policy – the Swedish experience', paper presented at the conference on *Access to Public*

Information: A Key to Commercial Growth and Electronic Democracy, Stockholm, 27/28 June 1996. See http://www.europa.eu.int/ISPO/legal/stockholm/en/seipel.html
Stewart, B. (1999), 'Five Strategies for Addressing Public Register Privacy Problems', in *Privacy of Personal Data, Information Technology and Global Business in the Next Millennium*, 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13-15 September.
Working Party on the protection of individuals with regard to the processing of personal data (1999*), Opinion No. 3/99 on public sector information and the protection of personal data*, WP 20, 3 May, Brussels.