

# Privacy Protection in the Virtual Society (ESRC Grant No. L132251019)

**Charles Raab**

**Department of Politics  
University of Edinburgh**

(The Centre for Computing and Social Responsibility  
(<http://www.ccsr.cse.dmu.ac.uk/>) collaborates with this project of Charles Raab  
(mailto:c.d.raab@ed.ac.uk) through the dissemination of information and results.)

## **Overview.**

The project forms part of the ESRC's 'Virtual Society' Programme, which concerns social, cultural, economic and other implications of new information and communications technologies (ICTs). The project investigates data protection as a crucial adjunct of the intensive use of ICTs in the 'Virtual Society'. It aims to understand outlooks on issues, conflicts of roles and emergent relationships amongst main participants in the British system in terms of the way various strategies for privacy protection relate to each other. In the context of the current revision of data protection law, it seeks to develop practice-and policy-related theory concerning new policies, criteria and strategies for privacy protection.

## **Other Information.**

Application of a methodology designed to assess the adequacy of the level of protection of individuals with regard to processing personal data: test of the method of several categories of transfer - final report  
([http://www.regard.ac.uk/research\\_findings/L132251019/summary.pdf](http://www.regard.ac.uk/research_findings/L132251019/summary.pdf))

## **Full Project Description.**

Aims and Scope of the Research

The research investigates the British system of privacy or data protection as a crucial adjunct of the 'Virtual Society' in regard to the maintenance of trust, and therefore of social cohesion, in the context of new electronic technologies in the private and public sectors. Given the current revision of the data protection system, the research aims to understand outlooks on issues, interdependencies, conflicts of roles and emergent relationships amongst the main participants in this system in terms of the dovetailing of various strategies for privacy protection. It seeks to develop practice- and policy-related theory concerning new issues and criteria for privacy protection systems, and to explore the strategic and policy implications of new thinking for the workings of the system.

The research analyses the processes and interplay of interests through which privacy-protecting solutions are arbitrated in the UK. This includes the involvement of European Union-level activity in harmonising national approaches under the aegis of the Data Protection Directive up to, and beyond, the October 1998 appointed day. Processes and perspectives from the EU level are investigated, but the main focus is within the UK, where implementing the Directive has set in motion an intensive process of rethinking and reconstruction of a regulatory system that has developed over the last 13 years. A good deal of this process is occurring in the Office of the Information Commissioner; between her office and organised groups of data users, citizens, consumers and technology providers; amongst these groups themselves; between the Registrar and her counterparts abroad; and within policy-making parts of the British government, including the Central Information Technology Unit (Cabinet Office, Office of Public Service), the Department of Trade and Industry and the Home Office. At the EU level, there are driving forces in some of the Directorates General, and also within the terms of the 1994 Bangemann Report, which recognised the importance of privacy for the development of a 'global information society'.

Implicit in the perspective of this research is the assumption that privacy does not detract from social cohesion; on the contrary, it provides a necessary platform for the individual's social and democratic political engagement with others, perhaps especially in 'virtual' communication, and thus is grounded in both a conception of human rights as well as utility. By focusing upon the system of data protection, the project assesses the way in which the roles and relationships amongst participants in systems that bear upon data protection - public policy-makers, official regulators, legal and consultancy firms, technology providers, data users who provide goods and services, and the public - may help to provide an important dimension of reassurance as the 'virtual society' poses new risks. The research is expected to contribute not only to empirical knowledge and understanding, but to practical discourse amongst policy-makers and practitioners involved in the system of privacy protection. It also aims to contribute to theoretical developments and their application concerning issues including equity, risk, democracy, strategies of regulation and control, and what might be called 'the governance of trust' in the context of new electronic technologies.

Previous Research

The academic basis upon which the research draws consists of research and other writings on privacy, and on information and communication technologies (ICTs) in society, the economy, government and other spheres. The work of the ESRC's former PICT Programme is a major component of the general and specific background. Studies of surveillance, of corporate and individual attitudes towards technology and privacy, of the advent of the 'information polity', and of computer ethics provide a more specific range of themes, issues and findings. Works dealing with public sector ICTs, including implications for democracy and privacy, are particularly useful for some of the questions taken up in the research project. There is a large number of government documents of relevance to issues of public service delivery and commercial uses of ICTs. Comparative studies with a legal or public-policy perspective on the development of privacy protection laws and systems in a number of countries constitute a more specific background for the research. Recent work on smart cards and privacy-enhancing technologies (PETs) gives a basis for understanding new techniques for privacy protection that are arousing considerable interest amongst regulators and other participants. Other writing in fields removed from privacy and ICTs also provide important analytical themes and interdisciplinary perspectives that the research draws upon and adapts, in particular, for the theoretical component and for its use in relation to the strategies, new criteria and relationships. These include work on the concepts of risk and trust, and on organisational relations and governance.

#### Relevant Background and Contexts

The research aims are best seen in terms of a policy and practical background that includes governmental and business developments using new electronic technologies, the issue of privacy, and the formation of policies and practices for privacy protection. These are discussed below.

The increasing pervasiveness of ICTs in the worlds of work, leisure, consumption and government will continue to exert a powerful influence on social cohesion, in part by altering the terms in which people perceive that they can conduct their lives with a degree of privacy that is considered appropriate to the social contexts in which they participate. Innovations in selling goods and services using electronic means include sophisticated direct marketing and consumer targeting processes, electronic banking and the development of electronic cash systems and other smart-card applications. Workplace surveillance, the use of the Internet for commercial and public-service transactions as well as for the formation of on-line 'virtual communities' of shared interests and discussion, thus fostering democratic discourse, are other domains which bring privacy issues to the surface. The fields of policing and public order, transport and health also provide examples of technological processes and systems that involve issues of privacy and surveillance: the proliferation of CCTV in public places, vehicle location and tracking for purposes of travel pricing, the creation of DNA and other population databases, and the heightened prospects for identity and smart cards for use in health and

benefit systems, are all among the technological settings and contexts for this research into privacy protection.

Moreover, Government proposals for the electronic delivery of public services and information to the citizen, including the rationalisation of government information processes for this purpose and the enhancement of an open, democratic polity, likewise depend upon controlling potential misuse of personal data that are collected, processed and communicated in the public sector. The Government expects data protection to play a crucial part in this reassurance, and the further crystallisation of its plans in the next few years are likely to feature privacy issues and ways to resolve problems.

These applications of new electronic technologies raise issues concerning the permissibility of extensive personal data-gathering, its effect upon social relations, and the rules that should govern these activities. Recent proposals and innovations have served to concentrate debate on these important issues and conflicts. Whilst real or supposed benefits to government efficiency, economic prosperity, lawfulness and citizen or customer satisfaction are acknowledged, the development and implementation of ICTs has for many years stimulated a concern for the maintenance of important human rights and values, amongst which privacy looms large. The 'chilling effect' of surveillance upon human interaction has long been recognised; if the 'virtual society' is perceived by people as amounting to the perfection of surveillance without appropriate safeguards, its promise will remain unfulfilled. Further technological advance in the age of the 'information superhighway' and the 'virtual society' will continue to construct this terrain for policy-making in regard to privacy protection, and for its academic study.

International harmonisation and national redevelopment of privacy protection rules occur just at a time of 'take-off' for many 'virtual society' developments mentioned above which gather and communicate a large amount of often sensitive personal data, and which themselves provide a particularly important rationale for reconsidering the issues, ends and means of privacy, identity and trust. The design and use of PETs, including public-key encryption and other techniques for personal identification, anonymisation and authentication, are among the proffered solutions for the problems of trust and privacy that accompany these departures. On the other hand, opinion is divided about the sufficiency of these technological solutions, but so, too, is it for the rest of the repertoire of solutions propounded by, or on behalf of, other interested parties. These include legal sanctions, voluntary codes of practice, adherence to agreed standards, the use of 'trusted third parties', and individual remedies. A mixture of strategies constitutes the present international and national policy agenda, but research into the coherence of the 'mix', and the value of each component, remains substantially to be done.

The implication of privacy in the collection, processing, use and communication of information about persons in and amongst many contexts of application has given rise to a search for practical measures of control. Since at least the 1960s 'computer age', this has been realised in many countries and internationally as a problem on the plane of

human rights, but also on the plane of commerce and public administration. In the latter dimension, it was considered that insufficient attention paid to public fears about new technologies would have a detrimental effect upon the development and exploitation of ICTs unless privacy protection could be brought to bear in the technologies themselves and in public policies and business practices. From that time originated the privacy or data protection laws, regulatory machinery, and self-regulatory practices that have been developed over the last twenty-five or more years. By now, a very large number of countries and lesser jurisdictions have 'legislated for privacy' through general or specific laws for data protection. The EU has built upon these foundations, and on the background of previous international conventions and agreements, in adopting a Directive to harmonise privacy protection in the context of the Single Market, and to exert influence over third countries' regulations.

These examples of legislative activity and the regulatory systems which it has shaped illustrate the response of governments to the question of privacy. However, there is ample room for scepticism about the efficacy of these measures, and about whether they leave important value issues as well as practical questions of implementation out of consideration. There is, on the one hand, a standard range of mechanisms and strategies that are employed in various ways in data protection systems, a conventional wisdom about the criteria to be used in assessing the acceptability, in terms of privacy, of technological innovations and business or governmental practices, and an established doctrine concerning the need to balance privacy against other objectives. On the other hand, such assumptions and procedures are severely tested by public policy departures and by social and economic practices in which electronic technologies open up new possibilities and often new dangers. Thus the systems of regulation and enforcement require, and have undergone, revisions, but there is a continuing need for fresh thinking and approaches in order to anticipate and resolve difficult conflicts arising between human rights and other values and interests, and in order to ground new ways of protecting privacy in a better understanding of regulatory relationships and criteria. The research project attempts to cast light on these matters by investigating the working of the system.

Any study of the 'virtual society' must therefore now consider whether the technological developments of the 1990s and beyond will affect the parameters of privacy in ways that make existing protections obsolete. There is already a good deal of reconsideration underway in practitioner communities concerning the implications of new ICTs for privacy, and concerning the implications of perhaps outdated protections for the further exploitation of ICTs. In the balance lies the ability of individuals to protect their own privacy, and thus control their identities, and/or to have these protected for them by some combination of strategies that include law, regulation, voluntary self-regulation, trusted third parties, cryptography and other security devices. The extent of that ability will powerfully shape popular trust in the 'virtual society' to bring the supposed commercial, public-service and democratic or communitarian benefits that its proponents claim. The terms under which the collection, processing and communication of personal

information are consented to, made transparent, and subjected to controls will form part of the context within which people judge whether they feel as secure in virtual communication as they do in face-to-face interaction.

### Research Questions

The research is concerned to understand attitudes, roles, relationships and practices. Thus it enquires into the way in which the privacy issues thrown up by emerging electronic technologies and their application in a variety of fields and sectors are being conceived of by policy-makers, regulators, users, and other participants in terms of the risks that are posed and the possible ways of safeguarding against them. Some research questions are about how policies towards the use of technologies that have consequences for privacy are formed, and how regulatory approaches and activities are deployed. Other questions seek to understand what data-using participants in a variety of sectors do to protect the privacy of customers or citizens - e.g., how they comply with external regulations and devise systems and rules for self-regulation. Questions are asked about whether they consider existing strategies for data protection to be adequate, and what other measures or combinations, including technological solutions, might be thought useful in redesigning the system of privacy protection. Research questions are also particularly concerned with understanding how, when and why participants engage in relationships across fields and roles in order to influence, implement or inhibit policies and practices for data protection, and how these interdependencies or tensions in effect arbitrate the quality and level of privacy protection afforded to the public. Another main research question concerns how these networks have been affected by the late-1990s revision of the law and system, and by the part played by the EU and other international players.

Further, the research enquires how far, and in what ways, participants perceive issues concerning equity, risk, democracy and trust to be important considerations in their approach to privacy protection, whether these values and criteria are thought to have a part to play, and how their recognition might affect activities and relationships. Related to this are questions about how the idea of a balance between privacy and other aims or values is thought about by participants who have different interests in the use and control of electronic technologies, whether it is considered to remain a valuable cornerstone of a regulatory system in the context of technologically related changes in the use of personal data, and what criteria or rules might replace the balancing philosophy as a guide to policy- and decision-making.

These are the main dimensions of the research questions. Inherent in them is an attempt to explain similarities and differences across technologies, fields and sectors, and across different roles played by interested parties in the data protection system. The project focuses upon the current and possible future application of theory to policy and practice in a much clearer way than in previous writing. It is believed that the research will break new ground in a subject that has been mainly studied within legal or technological frameworks.

## Data Collection and Analysis

The main research method is semi-structured interviews with leading participants in the processes and systems discussed above. The Central Information Technology Unit (Cabinet Office, Office of Public Service) is willing to provide and facilitate interview access within central government. The Office of the Information Commissioner and the Consumers' Association have also agreed similar access to their staff as well as facilitating contacts with policy-makers and data users. The local government sector will be approached with this aim.

Most of the interviews will follow a common set of questions derived from the main research questions, but within each variations are designed to reflect the different contexts and roles of the interviewees, as well as open-endedness to explore other avenues. About 100 one-hour interviews are envisaged; they will be tape-recorded, transcribed and analysed in relation to the main research themes and questions. Consideration is being given to the use of a package for qualitative data analysis (e.g., Hypersoft, The Ethnograph, NUD-IST). Interviewees will be selected according to their actual or presumed centrality to decision-making and policy-formation in a variety of organisations and fields drawn from the contexts outlined above. Some sectors of increasing technological intensity, and in which particularly sensitive personal data are used will receive more attention: these include direct marketing, the financial industry, health and other public services, and policing. Interviewees include British government and agency officials and politicians, EU and officials in other European organisations, regulatory officials, officials in trade associations, business organisations, consultancies and legal firms, technology developers, consumer and pressure organisations, and service providers. Most of the British interviews will be in London and environs. The EU interviews will be mainly in Brussels and Strasbourg. Charles Raab will conduct the majority of the interviews. He has already cultivated and maintained a large number of contacts in the networks of practitioner and policy communities in earlier work in this area.

Opportunities for data collection, and for making contacts are also taken through attendance at practitioners' conferences and meetings in which researchers are able to participate, often as observers. Such is the nature of the policy networks in the technology and privacy field that, in the applicant's experience, these are extremely important occasions for holding highly informative conversations (sometimes off the record), gathering written materials, and occasionally for formal interviewing. Attending these gatherings, such as the annual international meetings of Privacy and Information Commissioners, and the conferences of the Privacy Laws and Business organisation and of pressure groups such as EPIC/Privacy International, are very efficient ways of contacting relevant practitioners and policy-makers in one location, of observing and participating in their discourse, and of disseminating research.

In addition, documents produced by governmental bodies, leading organisations and spokespersons are especially important. Among these are organisations' responses to a number of recent policy proposals and Green Papers in which technology-and-privacy issues, and regulation, have been uppermost. Documents are analysed in relation to the themes and research questions, and can be used to prepare for interviews as well as in conjunction with the analysis of completed transcripts. Mr. Raab already holds a considerable amount of documentary material from his previous work which has not been analysed with the proposed research focus in mind. This is selectively useful for providing some historical depth on attitudes, practices and relationships.

Published secondary sources are used in a conventional manner. These include opinion surveys conducted on the topic of privacy and public trust. If it seems warranted, and if access is granted, some use may be made of secondary analysis of existing survey data on public and business attitudes that may be made available by others. The 'think tank' DEMOS has provisionally agreed to allow access to public attitude data from their current research. Prospects of data access for secondary analysis are being discussed with other organisations such as the Future Foundation, the Henley Centre and Equifax. However, these attitude data are useful mainly for background purposes, and the project does not itself include the conduct of a survey.

#### Expected Outputs

It is expected that a book and a number of academic articles will result. The book will be aimed at a readership of academics and practitioners, and will cover the range of the project. The articles will be written for different readerships and submitted to appropriate journals. They are likely to start life as academic and non-academic conference papers. They will deal with theoretical issues, as illuminated by the research; and with practical and strategic issues investigated in the research, as illuminated by theory. They could be published as occasional working papers or as conference/discussion papers for research users; these might be placed on the Internet. One or two short articles are likely to be produced for dissemination to practitioners in consultants' newsletters.

A jointly-held invitation conference has been mooted with potential research users, which would be a vehicle for working papers. It is also possible to envisage some further international academic dissemination, based on existing close contacts with researchers on these topics in other countries where similar 'virtual society' issues arise, and where revisions of data protection systems are likewise in train. In particular, German, Dutch and Danish colleagues share many of these interests, as do Canadians and Americans. One probable dissemination event would be the annual meeting of the European Group of Public Administration's Permanent Study Group on Informatization in Public Administration, of which Mr. Raab is a member. He also intends to apply to direct a Workshop in the annual sessions of the European Consortium for Political Research. Collaborative research beyond the close of the project might well result from these activities; this has already been discussed with colleagues abroad.

The Office of the Information Commissioner has indicated strong interest in arranging a seminar or similar event in which strategic thinking can be developed for implementing privacy protection regarding new technological issues. Likewise, the Central Information Technology Unit (Cabinet Office, Office of Public Service) considers the research to be relevant to their plans for electronic service and information delivery, and will be able to engage collaboratively in dissemination and in involving other central government groups. Organisations in local government and in other public sectors will be approached regarding the use of results. DEMOS is interested in similar involvement, as the research dovetails with their technology and privacy work. The Consumers' Association is keenly interested in the results in relation to its policy activity, and can play a part in conferencing or other dissemination. The Centre for Computing and Social Responsibility at De Montfort University will lend their auspices, including an Internet site, for communicating results to user groups. Organisations involved in supplying consultancy, training and information about data protection especially to the business sector (Privacy Laws and Business, and Cap Gemini) have also expressed a willingness to assist access and dissemination. Overall, the potential value of the research to non-academic users may lie in stimulating greater understanding of how privacy and related values apply to 'virtual society' innovations in government and business, in suggesting new perspectives and criteria for that application, and in the collaborative exploration of privacy protection strategies.