The future of privacy
Volume 1
Private life and public policy
As the publisher of this work, Demos has an open access policy which enables anyone to access our content electronically without charge.

We want to encourage the circulation of our work as widely as possible without affecting the ownership of the copyright, which remains with the copyright holder.

Users are welcome to download, save, perform or distribute this work electronically or in any other format, including in foreign language translation without written permission subject to the conditions set out in the Demos open access licence which you can read here.

Please read and consider the full licence. The following are some of the conditions imposed by the licence:

- Demos and the author(s) are credited;
- The Demos website address (www.demos.co.uk) is published together with a copy of this policy statement in a prominent position;
- The text is not altered and is used in full (the use of extracts under existing fair usage rights is not affected by this condition);
- The work is not resold;
- A copy of the work or link to its use online is sent to the address below for our archive.

By downloading publications, you are confirming that you have read and accepted the terms of the Demos open access licence.

Copyright Department
Demos
Elizabeth House
39 York Road
London SE1 7NQ
United Kingdom

copyright@demos.co.uk

You are welcome to ask for permission to use this work for purposes other than those covered by the Demos open access licence.

Demos gratefully acknowledges the work of Lawrence Lessig and Creative Commons which inspired our approach to copyright. The Demos circulation licence is adapted from the 'attribution/no derivatives/non-commercial' version of the Creative Commons licence.

To find out more about Creative Commons licences go to www.creativecommons.org
Demos

Demos is an independent think tank committed to radical thinking on the long-term problems facing the UK and other advanced industrial societies.

It aims to develop ideas – both theoretical and practical – to help shape the politics of the twenty first century, and to improve the breadth and quality of political debate.

Demos publishes books and a regular journal and undertakes substantial empirical and policy oriented research projects. Demos is a registered charity.

In all its work Demos brings together people from a wide range of backgrounds in business, academia, government, the voluntary sector and the media to share and cross-fertilise ideas and experiences.

For further information and subscription details please contact:

Demos
9 Bridewell Place
London EC4V 6AP

Telephone: 0171 353 4479
Facsimile: 0171 353 4481
email: mail@demos.co.uk
web site: www.demos.co.uk
Other related publications by Demos:

On the Cards: Privacy, identity and trust in the age of smart technologies (Perri 6)

Democracy in the Digital Age (Roger, Lord Freeman)

Access Denied? Preventing information exclusion (Danny Kruger)

NetState: Creating electronic government (Perri 6)

Business ethics (Sheena Carmichael)
Perri 6 is Director of Policy and Research at Demos and was previously Lecturer in European Social Policy at the University of Bath. His recent publications include *Holistic government* (Demos), *Escaping poverty: from safety nets to networks of opportunity* (Demos), *Bringing it all together: a vision for the future of London governance* (with Gerry Stoker, Association of London Government, London), *The substance of youth: the place of drugs in young people’s lives* (with Ben Jupp, Helen Perry and Kristen Lasky, Joseph Rowntree Foundation, York), *The contract culture in public services: studies from Britain, Europe and the USA* (ed. with Jeremy Kendall, Ashgate, Aldershot), *Liberty, charity and politics: non-profit law and freedom of speech* (with Anita Randon, Dartmouth, Aldershot) and *Delivering welfare: repositioning non-profit and cooperative action in western European welfare states* (ed. with Isabel Vidal, CIES, Barcelona). His current work includes studies on the future of government, public policy and risk, social capital and deliberate efforts to change cultures.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface and acknowledgements</td>
<td>ix</td>
</tr>
<tr>
<td>Summary</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>12</td>
</tr>
<tr>
<td>Notes</td>
<td>18</td>
</tr>
<tr>
<td><strong>PART 1 PRIVATE LIFE</strong></td>
<td></td>
</tr>
<tr>
<td>1. Origins</td>
<td>21</td>
</tr>
<tr>
<td>2. Risks</td>
<td>32</td>
</tr>
<tr>
<td>3. Values</td>
<td>45</td>
</tr>
<tr>
<td>4. Traditions</td>
<td>51</td>
</tr>
<tr>
<td>Notes for Part 1</td>
<td>70</td>
</tr>
<tr>
<td><strong>PART 2 DRIVERS OF CHANGE</strong></td>
<td></td>
</tr>
<tr>
<td>5. Introduction: the drivers of change</td>
<td>81</td>
</tr>
<tr>
<td>6. Cultures and privacy</td>
<td>84</td>
</tr>
<tr>
<td>7. The business of personal information</td>
<td>107</td>
</tr>
<tr>
<td>8. Information technologies</td>
<td>128</td>
</tr>
<tr>
<td>9. Information age government</td>
<td>163</td>
</tr>
<tr>
<td>Chapter</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>10. The regulatory capacity of government</td>
<td>186</td>
</tr>
<tr>
<td>11. The media and the personal</td>
<td>215</td>
</tr>
<tr>
<td>Notes for Part 2</td>
<td>241</td>
</tr>
<tr>
<td><strong>PART 3 FUTURES OF PRIVACY AND PRIVATE LIFE</strong></td>
<td></td>
</tr>
<tr>
<td>12. Toward futures for privacy</td>
<td>257</td>
</tr>
<tr>
<td>13. Standard scenarios</td>
<td>260</td>
</tr>
<tr>
<td>14. Alternative ways of constructing scenarios</td>
<td>269</td>
</tr>
<tr>
<td>15. Cultures and the future of privacy</td>
<td>278</td>
</tr>
<tr>
<td>Notes for Part 3</td>
<td>301</td>
</tr>
<tr>
<td><strong>PART 4 PRIVACY, POLICY CONFLICTS AND VIABLE POLICY</strong></td>
<td></td>
</tr>
<tr>
<td>16. Viability and conflicts over privacy</td>
<td>311</td>
</tr>
<tr>
<td>17. Freedom of speech and freedom of the media</td>
<td>319</td>
</tr>
<tr>
<td>18. Public accountability of public servants and people in public life</td>
<td>341</td>
</tr>
<tr>
<td>19. Data protection in business and government</td>
<td>360</td>
</tr>
<tr>
<td>20. Privacy and the distribution of risk</td>
<td>381</td>
</tr>
<tr>
<td>21. Institutions for coping with cultural conflict and influencing cultural change</td>
<td>387</td>
</tr>
<tr>
<td>22. Privacy in information policy and information ethics: the policy process</td>
<td>401</td>
</tr>
<tr>
<td>23. Conclusion</td>
<td>405</td>
</tr>
<tr>
<td>Notes for part 4</td>
<td>411</td>
</tr>
<tr>
<td>Glossary</td>
<td>418</td>
</tr>
</tbody>
</table>
Preface and acknowledgements

In this book, I have tried to use the case study of privacy and private life to illustrate and make tractable some difficult issues about politics, culture, risk and social change. The book attempts to use the case study of privacy and private life to innovate on several fronts at once.

First, it offers, I hope, to the community concerned with the possibilities for privacy and private life in the new information economy, some new tools for thinking about these problems and some distinctive specific policy recommendations.

Second, in bringing together many of the themes that I typically apply to problems of public policy, it serves to provide a toolkit for the policy sciences. In particular, by bringing to bear ideas from risk perception and risk management, together with understanding the nature of trust (which is given more attention in Volume 2) and the embedding of policy problems in cultures, it offers a style of policy analysis that is quite distinct from the conventional cost-benefit, economistic, programme evaluation oriented that dominates standard textbooks on the policy sciences.¹

Third, it seeks to develop what I call here ‘cultural dynamics’ as an approach from general social science applied to the discipline of thinking about possible futures known as scenario building, using cultural theory.

Fourth, I hope that the book is a contribution to a certain kind of political theory. One problem in particular that runs through this book...
I take to be a central fault line around which societies in the developed world are shaped. This is the continuing, and perhaps growing, tension between the impulses of economic liberalisation, with its commitments to removing constraints upon trade and exchange, and of political liberalism, with its impulse to construct and then protect a conception of individual or family life from unfettered openness to trade or governance. Surely there never was a golden age characterised by what some writers call ‘classical liberalism’, in which these two fundamental impulses were reconciled harmoniously in a simple, clear and non-arbitrarily defined system of quasi-natural, liberal, civil and property rights comprising the whole of the law. Indeed, it seems that the more we understand the history of how individuality, private life, property rights and the idea of an economic interest have developed, the more they seem contingent upon particular social configurations of cultures, conceptions of risk and order, patterns of social networks and the shifting vicissitudes of power.

The literature on privacy is vast – spanning law and comparative law, jurisprudence, moral and political philosophy, history, anthropology, sociology, social network analysis, psychology, social research methodology, economics, marketing, public administration, a variety of technological and engineering disciplines ranging from computing science and mathematical cryptography through to architecture, from town planning to materials science – and then reaches into more esoteric disciplines such as therapy, psychodynamics and the design of gardens. And that ignores the daily stream of often excellent and thoughtful journalistic material. For anyone to pretend to have conducted a comprehensive literature review on privacy would be ridiculous. Such a review would take a team of researchers many years; it would be out of date well before it was complete; and much of the effort expended would probably not be worthwhile. It would be more absurd still to claim to have conducted even an adequate review in the course of what has become an eighteen-month programme of work and I make so such claim here. I have set myself no more ambitious an aim than ‘just enough scholarship’ to have at least a reasonable idea of the main debates in each of the areas which the book addresses and to
stimulate my own thinking. Moreover, as will be clear from Part 2 of
this volume and from Volume 2, much of the research time has been
devoted to expert interviews, focus groups and surveys rather than
wholly expended on library based work.

The book will, I hope, stand or fall on the strength of its argumenta-
tion rather than on the length of its list of references, and finally on the
hope that its merit is in part to bring to bear on the subject of privacy
ideas from literature that are not usually the principal concern of pri-
vacy scholars. For those who seek good literature reviews, there are
several to which their attention is directed.²

The research carried out for this study has been financially sup-
ported by the Economic and Social Research Council (ESRC) and by
IBM UK plc. The main body of research was backed by the ESRC.³ In
addition, both organisations jointly supported a series of seminars at
which some initial findings and scenarios were presented.

In a project of this nature, I am indebted to many people and the
charge of responsibility for my errors and misunderstandings cannot
be levelled at any of them. My first debts are to my collaborators in the
research process.

During his time at Demos, Adrian Fletcher, now of KPMG, collabor-
ated with me in the design of the focus group schedules, conducted
the focus groups, worked with me on the initial interview schedules
and then conducted the interviews with business and technology lead-
ers; he produced detailed reports, helped with the design of the survey
questions and generated with some initial syntheses of the interview
material; and he started the work of organising the drivers of change
for the scenario building work.

Kristen Lasky, now at the Kennedy School of Government at
Harvard, carried out the detailed statistical analysis of the survey data
with great flair and understanding. Rachel Jupp conducted a number of
telephone interviews with experts and gathered large quantities of grey
literature and other materials from which I have worked. Ian Christie
has been a most supportive editor. Lindsay Nash handled the design,
copy and proof editing. Jamie Coulthard organised the ‘Virtually Social’
seminar and provided me with valuable material; Matthew Ward and
Siân Gibson also gathered some material, while George Lawson and Tom Hampson helped with scanning the press.

The project advisory group provided invaluable guidance, support and comment on draft instrumentation and interim reports. The members of the group were Anne Hinde of the Office of the Data Protection Registrar (now to be the Data Protection Commissioner), seconded to the Home Office, Alan Hedges who is an independent researcher, Charles Raab of the University of Edinburgh and Melanie Howard of the Future Foundation.

The experts interviewed on various issues gave their time and knowledge freely. They were Dr Anthony Furness of the Department of Physics and Electronics at Keele University; Dennis Piggott, Head of Customer Database Management at NatWest Bank; Mark Patron, Managing Director of Claritas; Stephen Taylor, Marketing Controller at Safeway; Sarah Tanburn, Director of Strategy and Information at Hertfordshire County Council; John Watson, Data Security Officer of the Metropolitan Police; Ian White, Director of Social Services at Hertfordshire County Council; Chris Wynne-Davies in Corporate Affairs at BT; Dr Marek Rejman-Greene in Knowledge Management Research at the BT Martlesham Heath Research Laboratories; Professor Vivian Nathanson of the British Medical Association; Dr Frank Hickman, Managing Principal of Unisys. Telephone interviews were conducted with Peter Horroway, Inner London Probation Services; Jon Bright, Crime Concern; Louise Ayriss, Chartered Institute of Housing; Hillary Kitchin, Local Government Information Unit; Nigel Hickson, Department of Trade and industry; Christine Hine, CRICT, Brunel University; Martin Bartle, Direct Marketing Association; Christian Anderson, The Economist.

Janet Dewes of MORI Field and Tab organised the recruitment of participants in the series of focus groups that we ran around the country. Stephen Welch and Scott Wallace (then) of MORI provided assistance in the design of the survey questions and organised the administration in the MORI Omnibus survey between 6 and 9 June 1997. They provided an initial data report as well as data for additional analyses.
The following people took part in a Demos ‘Virtually Social’ seminar at IBM in February 1997 at which a briefing paper was presented, containing initial findings: Orit Azaz, The Common Sense; Tony Baker, Association of British Insurers; Claire Birks, IBM UK; Professor Ruth Chadwick, University of Central Lancashire; Dr Heather Draper, University of Birmingham; John Drummond, Integrity Works; Angela Edward, Institute of Personnel and Development; Anne Hinde, Office of the Data Protection Registrar and Home Office; Charlie Leadbeater, Demos; Jo Lenaghan, Institute for Public Policy Research; Dr Helen Margetts, Birkbeck College; Christopher Millard, Clifford Chance; Colin Muid, then of the Central Information Technology Unit, Cabinet Office; Professor Charles Oppenheim, then of De Montfort University and now Loughborough University; Dr Charles Raab, Edinburgh University; Geoff Robinson, then of IBM; Dr Simon Rogerson, De Montfort University; Thaer Sabri, Mondex; Sarah Spencer, Institute for Public Policy Research; Ian White, Hertfordshire Country Council.

I am also grateful to Tim Whitaker of the ESRC, Claire Birks of IBM UK, Colin Muid (then) of the Central Information Technology Unit, Cabinet Office; Professor John Goddard of the University of Newcastle; Oliver Morton (then) of Wired UK; Bob Tyrrell formerly of the Henley Centre for Forecasting; and Francis Aldhouse, Deputy Data Protection Registrar (shortly to become Deputy Data Protection Commissioner), who formed the advisory group for the Demos ‘Virtually Social’ series of Information Society seminars.

In addition, for their comments and suggestions at various stages of the research, I am grateful to Dr Ross Anderson of the University of Cambridge, Sarah Tanburn of Hertfordshire County Council, John Browning of Wired, Debbie Porter, Geoff Mulgan and Claire Brown.

Francis Aldhouse, Charles Raab, Adrian Fletcher, Ian Hargreaves, Ian Christie and Ben Jupp all read part or all of the manuscript and gave me invaluable comments.

Privacy is so widely ranging and protean a concern in modern societies that some of these individuals naturally wondered from time to time what their professional concerns had to do with those of the others.
None of these individuals can be held responsible for my opinions, errors or conclusions. Consistently with the principle of respecting privacy, I have taken care not to identify the sources of any of our focus group participants or survey respondents and none of the material from the expert interviewees is attributed; the text has been written in such a way as to ensure that no inference can be made about which statements were made by which expert interviewees: indeed, most of the material came from more than one source.
Summary

Coming to terms with the explosion of personal information

1. Computers, data warehousing, high speed networks and smart cards now make it possible to produce and manipulate personal information about everything from shopping patterns to genetic make-up and criminal records on an unprecedented scale. This poses huge challenges to the traditional conceptions of how to protect personal privacy.

2. However, fatalism that new technologies and the economics of the information age will inevitably mean the end of privacy is mistaken. Cheap new technologies are now available that could be used to buttress privacy more than ever before. Moreover, the fact that we continue to care about privacy means that governments will continue to try to prevent abuses of personal information; and that market forces will encourage businesses to prove their trustworthiness. So while there will be strong pressures to share personal information across the public sector, and substantial incentives for private firms to trade in data concerning their customers or employees, there will also be countervailing pressures on all organisations to demonstrate their respect for personal privacy.
The meaning of privacy

3. The meaning of privacy is changing. In the emerging information economy, privacy will not primarily mean preventing organisations and other people from knowing about us. Instead, it will be founded on securing organisations’ commitment to principles about what shall and, crucially, shall not be done with those data. Privacy cannot be an absolute right, but will remain a centrally important value.

4. Privacy can best be understood as a protection against certain kinds of risks – risks of injustice through such things as unfair inference, risks of loss of control over personal information, and risks of indignity through exposure and embarrassment.

Futures


6. The other conventional assumption about the future of privacy – that there will be a market in privacy, in which we will each pay for the level of privacy that we want – is also misguided. Since no one – not even businesses using personal information for database marketing – can know what the future value of personal information really is, it is almost impossible to price it sensibly. Moreover, Europeans continue to demand regulatory protection beyond that offered by contract law.

7. Each of these visions misunderstand the complex cultural dynamics reshaping privacy. As alternatives to these one-dimensional accounts of the future, this book uses a more complex set of methods to map out the driving forces
likely to shape privacy, and the potentially viable settlements between the continuing demand for privacy and the claims of business and government to override them. These are set out in Part 3.

8. Key forces shaping the future of privacy will include the importance of consumers’ trust in the handling of personal information by commercial organisations, the extent of integration within government and strategic alliance building in business that involves the sharing of personal information.

9. However, in any society, the place of privacy depends less on technologies and organisational arrangements than on cultures – how people think and feel about privacy and how they value it. These cultures have changed radically in the past and will continue to change in the future in ways that cannot now be predicted with certainty. Any viable strategy for privacy needs to be designed to cope with a range of different possible ways in which cultures of privacy could evolve.

Policy and principle

10. The book proposes a series of considerations for governments, business and the media in responding to the new pressures on privacy.

11. Greater public literacy with regard to privacy will become increasingly important. People will increasingly need to be able to make judgements about the trade-offs between privacy and other goods.

12. All organisations will need to invest more in the future in proving their trustworthiness. This will be essential both for private companies and for public agencies using and communicating personal data. A range of different tools for building trust are set out in this volume and its companion. These include voluntary kitemarking schemes on compliance with privacy standards, use of anonymous ways of
identifying people in databases, codes of practices on matching of data, and staff training in information ethics.

13. Governments will need to take care to ensure that the laws governing privacy do not become irrelevant. For example, if they seek to prohibit encryption technologies for which there is substantial demand, or try to insist that individuals and businesses deposit their decryption keys where law enforcement agencies can gain access to them, such laws will almost certainly be circumvented.

14. For the media, the idea of public interest that has hitherto been the principal test of when privacy can be set aside, is too vague for the new challenges emerging around privacy. Instead, the media should be given a special duty of scrutiny, subject to specific authorisations to collect and use information in ways that other agencies may not.

Recommendations

Privacy and the media

1. There should be no further extension of the criminal law in this area.

2. The following principles should inform the decisions of the Press Complaints Commission and the Broadcasting Standards Council in privacy cases and should inform the efforts of the appeal courts to reconcile the European Convention on Human Rights provisions on media freedom and on privacy with each other and with the English law of breach of confidence. Only if the courts fail in this task should there be primary legislation in this area.

3. The news and current affairs media should be given a special duty of scrutiny in law. On demonstration of a reasonable basis of suspicion and the necessity for the use of the particular means for collecting information employed, this special duty would be a defence in cases of breach of confidence, trespass and stalking, but would not permit
breach of trades descriptions, defamation or libel, partisan bias or breach of quality threshold conditions in terrestrial broadcasting. Only under specific conditions would the duty permit impersonation or entrapment by journalists. The public interest test should be reinterpreted as a fourfold test on the application of the special duty of scrutiny, concerned with the threshold evidential conditions, the manner of data collection, the case for disclosure and the target of disclosure. Only where the special duty of scrutiny can be invoked should the news and current affairs media be exempt from the data protection duties of fair and lawful obtaining of data and of subject access.

4. Interim restraint injunctions should continue to be permitted in breach of confidence cases, but only subject to much tighter tests of seriousness, evidence, balance of public and private interest and efficacy, and only in the rarest cases on *ex parte* hearings: only the courts – and not the self-regulatory bodies – should have powers to make such orders.

5. The tort of trespass should be reviewed and the case for a new tort of unlawful invasive surveillance examined: the special duty of scrutiny would provide a defence for the media in such cases.

6. Public figures should be able to seek injunctive relief or damages against the media for violations of privacy through the self-regulatory bodies or the courts by way of breach of confidence only where any allegations made concern minor misdemeanours, failures or character flaws and where they have not sought the status of a public figure. Politicians should not have fewer privacy protections.

7. Matters which are not allegations but are claimed to be of public concern on the ground of ‘fair comment’ would only justify collection and disclosure of personal information without consent, thereby overriding privacy,
when an individual’s behaviour has affected many others adversely.

**Data protection in government and business**

8. There should be a specific data protection principle introduced to place duties on data controllers only to use true identities when absolutely necessary for the purpose of the transaction to be achieved and only to make true identities available to the fewest possible authorised persons who need to know them in order for the system to work effectively.

9. Data held for national security, pensions, payroll and accounts purposes should be notified to the Data Protection Commissioner.

10. There should be a specific right to erase excessive and irrelevant data.

11. Exemptions from subject access should be curtailed, leaving only:
   - data held by the police or other law enforcement agencies for the purpose of conducting criminal investigations, where and only where subject access could compromise the effectiveness of an investigation. The present exemption covers absolutely any database that might be held to be useful in preventing or detecting crime, and can cover many kinds of data where individuals can, without any harm to the enforcement of law and the detection of crime, have the right to know and perhaps challenge what is held about them
   - data held in reserve during the course of commercial negotiations for the purpose of making decisions on claims put in those negotiations
   - data subject to legal privilege, and
   - data held for research purposes only, where the research agency can show that it will, on completing analysis, anonymise the data.
12. There should be a specific right of independent subject access.
13. The ‘serious harm’ test in third party appeals against disclosures under freedom of information legislation should not be introduced: it should be sufficient to show that disclosure would violate data protection law.
14. Each industry and the public sector as a whole should, in three years, introduce detailed codes of practice on practical implementation measures of data protection agreed with the Data Protection Commissioner. These codes should cover the issues set out in Chapter 19.
15. If the industry fails to offer them voluntarily, legislation should be introduced to give consumers a right to purchase blank multi-functional smart cards and insist that a governmental or commercial application be placed on a card of their choice, as well as be allowed to decide for themselves which applications should co-reside.
16. Britain should encourage the European Union in services to negotiate at the World Trade Organisation to secure a multilateral treaty to secure global convergence towards best practice in data protection.

Electronic commerce and encryption

17. Proposals for a system of mandatory key escrow should be dropped.
18. There should be a clear and specific right for businesses and individuals to use encryption systems for any lawful purpose as they see fit.
19. Judicial warrants should be required for law enforcement agencies to secure access to the means of decryption.
20. A voluntary key escrow system should be facilitated in law.
21. A relatively permissive legal framework should be introduced for certification agencies, focusing mainly on the extent of liability upon the agency to third parties
relying on their certificates and ensuring that certificates are only issued with active consent.

**Police powers**

22. A comprehensive code of privacy practice, integrated with the generic public sector code, should be introduced for all police records and agreed with the Data Protection Commissioner.

23. Judicial warrants should be required for law enforcement agencies to engage in interception of communications, entry to premises and the use of surveillance devices. On this basis, data obtained should be admissible evidence in court cases.

**Insurance**

24. Insurance companies should provide proposers in writing with details of all the kinds of information that will be considered relevant in setting premiums, in particular: of the kinds of genetic information, if any, that will be considered relevant; of the kinds of inferences that will be drawn from that information; of the inferences that may acceptably be drawn from any unwillingness by a proposer to provide certain kinds of information; and of the breadth of the risk pools into which individuals for whom insurance is accepted will be placed.

**Recruitment into employment**

25. The Confederation of British Industry, the Federation of Small Businesses and the Institute of Personnel Directors should develop, agree and jointly publish a comprehensive code of practice on the kinds of personal information, including any genetic information, that may be asked for and taken into account at the point of recruitment for the main
categories of employment; on the kinds of inference that it is acceptable to draw from that information; and on the inferences that may acceptably be drawn from any unwillingness by a candidate to provide certain kinds of information.

**Allegations of paedophilia**

26. The Local Government Association, the Chartered Institute of Housing, the British Association of Social Workers, the National Institute for Social Work, the Association of Chief Police Officers, the Association of Chief Officers of Probation and other relevant government and professional bodies should develop, agree and jointly publish a code of conduct on the handling of information concerning alleged paedophiles. In particular, the code should require that disclosure about risks to persons in the community (other than the immediate family of the alleged paedophile or victims’ families) should be undertaken against individuals living in that community previously convicted or otherwise, only when the following four conditions are met:

- Firstly, the evidence must be corroborated by independent witnesses with no prior or other reason for malice, must be internally consistent, credible and sufficiently detailed, and generally meet the usual civil law standard of ‘the balance of probabilities’.

- Secondly, the risk involved must indeed be catastrophic. That is, the individual must be one of the minority of paedophiles who represent a risk to children to which he or she is a stranger, and the risks involved should be of serious physical or mental abuse.

- Thirdly, the risk of a serious offence being committed must be high.
Fourthly, the recipients should be warned of the penalties they would themselves face for any victimisation of the individual.

Privacy risk literacy

27. The Data Protection Commissioner and the Central Office of Information should jointly conduct a public information programme, through national broadcast media but also through professional, industrial and governmental bodies, to inform the public about privacy risks in a way that encourages, not alarm and fatalism, but a confident and balanced proportioned sense of risk and strategic response.  
28. The Data Protection Commissioner should work with the Department for Education and Employment and with the school curriculum authorities to develop ways in which more balanced understanding of privacy risks can be encouraged through the use of relevant examples and materials across the curriculum, without confining coverage of privacy issues only to ‘civics’, ‘citizenship’ or ‘general studies’.

Deliberative institutions

29. The Data Protection Commissioner should work with the Confederation of British Industry, other industry umbrella bodies, the Federation of Small Businesses, the Office of Public Service, the Local Government Association, the National Health Service Executive, the Trades Union Congress, the National Consumer Council, the Consumers Association, Liberty and others to create a range of appropriate, often perhaps ad hoc and temporary deliberative institutional arrangements through which privacy risk issues and conflicts over privacy concerns can be negotiated and where lessons can be learned and disseminated.
Public sector audit

30. The National Audit Office and the Audit Commission, in addition to their existing roles in auditing the public sector for value for money and for effectiveness, should – working alongside the Data Protection Commissioner – offer (or manage the contracting-out of) third party audit of information ethics within the public sector that private auditors like that offered in private schemes such as Truste™.

Political accountability

31. The House of Commons should create a Select Committee on Information Policy, which would take over from the Home Affairs Select Committee oversight of data protection, from the Public Service Committee, oversight of information policy in the implementation of electronic government, and from the Trade and Industry Committee, issues affecting electronic commerce, digital signatures and encryption policy.

Data Protection Commissioner

32. In recognition of the government-wide application of data protection issues, the executive oversight of the Data Protection Commissioner should move from the Home Office to the Cabinet Office.
This book argues that privacy has a future, because we shall continue to value private life. Technology and the economics of information are not killing privacy: indeed, they can now be used to reinforce it. But they are reshaping the means by which it can be pursued. Laws, regulators and the paraphernalia of legal activity do not tell us what privacy is and why it matters. Rather, they are the symptoms of conflict about private life itself. For, as a society, we do not and cannot agree on what it is about private life and privacy that we value. But the disagreement is not between an infinite number of perspectives. There are a relatively small number of traditions that organise the values we attach to private life and that offer competing ideas about risk which underpin what ‘threat’ to privacy we recognise, consider unacceptable and are prepared to act upon or call for action by governments upon, and claims about the kind of protection we seek for it under the label of ‘privacy’.

Therefore, the futures of privacy depend on the ways in which our society attempts to handle and organise these conflicts of values and the ways in which we accommodate at least the principal traditions. We have choices about how we do that and the book sets out some of these. Finally, it offers specific recommendations for strategies for dealing with the conflicts between privacy and other kinds of values, which seek to find ways to at least partially accommodate the competing demands of these principal traditions.
This makes the argument much more controversial than perhaps this sounds. In particular, the book argues against those who consider that:

- nothing can be done about privacy because it is grand forces of technological development or economic change which determine outcomes rather than policy decisions or collective aspirations of societies; or if anything can be done voluntarily, it will be done by some technical fix such as encryption technology (*privacy fatalists, technological determinists*)

- culture is of no great or independent importance, and policy design should be a matter of alignment with economic and technological forces (*reductionists*)

- the framework of risk perception, assessment and management is inappropriate in this area because we are not concerned here with probabilities of fatalities or physical damage to people (*risk purists*)

- some grand, once-for-all philosophical reconciliation is possible to which most reasonable people will sign up (*committed liberals, communitarians, etc*)

- the idea of privacy can be eliminated or reduced to its constituent parts, leaving issues affecting the media, issues affecting database marketing in business, and issues about what information should be provided before life assurance is granted as separate problems (*privacy fragmenters*).

A common fatalism runs through both the more complacent and gushing technological and business literature and also the despairing tone of privacy activists writing about ‘threats’ to privacy. Both groups see the fragile instruments of legal regulation as pitifully inadequate to resist the advancing hordes of surveillance technologies, but simply align their respective romanticisms with different sides in this conflict.
I do not accept this apocalyptic vision. In this common ground between the romantic civil libertarians and the complacent technological determinists there are some fundamental misreadings of how societies and their governance work. Firstly, the conception of regulation with which many of them imagine privacy regulators are working is simply inappropriate and wrongly transferred from other industries and fields. Privacy regulation is a quite different kind of activity in strategy and goal from regulating the prices of monopoly utilities. Secondly, there are privacy enhancing as much as privacy undermining technologies and many others that can be put to either use. Thirdly, there are real conflicts of values within business, within government and within the public at large that have not been settled once and for all about privacy – and everything we know about the dynamics of cultural and social change suggests that they are never settled once and for all.

We need to revise fundamentally the common conception of what is distinctive about what is variously called the information society, the information age or informational capitalism. Usually, this means the age of the computer instead of the abacus, the pocket calculator, the pen and the filing cabinet, or the age when computers are connected by modems or other forms of telephony. This understanding of the age in terms of the business and home hardware is quite inadequate. For the printing press, the publishing firm, the calculator, actuarial tables, double entry book-keeping were all information technologies for earlier ‘information ages’, just as writing and literacy were before them. Moving from hardware to content does not help. Simply to point to the scale on which volumes of ‘bits’ flow today says nothing distinctive about our society, for large volumes of financial information, contracts, engineering and actuarial information, literature, personal mail, and many other kinds of information have been accumulated, traded and moved around the globe for centuries.

Instead, this book argues that what is distinctive about informational capitalism is that personal information has become the basic fuel on which modern business and government run and that the systematic accumulation, warehousing, processing, analysis, targeting,
matching, manipulation and use of personal information is producing new forms of government and business; most importantly, that what people in the age of informational capitalism mean by and value in private life is changing. It follows that privacy cannot be measured by the quantity of other people’s and organisations’ ignorance about us, but only in the extent of their acceptance and commitment to certain principles about the use of this information.

As yet we are only beginning to understand these new meanings – and they are plural – of private life that compete for our loyalty and commitment. The most important shaper of the future of privacy is neither the capacity of national governmental regulators to enforce a set of information processing practices nor the development of ether data collection, analysis, matching, mining and warehousing or even security technologies. Rather, it is the kind of private life we want, and what we care about in the experience and conduct of private living, that will shape the future of privacy.

The aim of the book’s argument is the improvement of public policy. In in the final part, I set out some specified and detailed recommendations. The test that I argue public policy must submit itself to, in this field as in many others, is one of cultural viability. By cultural viability, I understand the following. A strategy in business or an overall direction for policy in government is culturally viable if it is sufficiently robust against shocks from many plausible configurations of the principal cultures of privacy, as they change their importance, make coalitions or come into conflict with each other.

Therefore, the first step in understanding viability is to understand cultural dynamics. A public policy or a business strategy is not culturally viable if it makes the overly simple assumptions of the technological determinists and despairing romantic civil libertarians that only one cultural formation of private life is possible in the age of informational capitalism. I shall argue that the most robustly culturally viable strategy for the foreseeable medium term future (for the present purposes, to 2010) is one which finds ways to appeal in some measure to each to the different cultural biases which make up our fractured and rival conceptions of private life, and which attempts to enable them to
form coalitions where possible and to resist shocks from sudden resistance and assault unexpected cultural change when necessary.

By stressing the idea that what we value in private life is the heart of the issue, I mean to assert the integrity of the idea of privacy. Many writers have gone out of their way to cast doubt on the idea that there is an coherent common thread running through the variety of contexts and claims in which privacy is reasonably invoked. However, I argue that the risks in the name of which privacy is claimed against belong together in an important sense. Privacy claims fight the same kinds of enemies on the same sorts of ground for closely related reasons. True, different cultures of private life place the emphasis on different risks within the group of risks but these traditions recognise each other as claiming the same turf. And that turf may as well be called private life.

The first part begins with a schematic history of private life and grounds the origins of contemporary ideas about privacy firmly in the changing mentalités of private life. Next, the idea of privacy is presented as a set of related risks, together with a classified organisation of the range of privacy risks which seem to attract most concern today. It then goes on to explore what it is that we value so much in private life that claims for its protection under the label of ‘privacy’ come to have such resonance. The main rival cultures’ long standing political currents of thought about the place of private life are traced in the Chapter 4.

Part 2 is devoted to describing some of the principal forces that are reshaping the scope for privacy and private life today.

The third part attempts to use the materials developed in the second in order to think ahead, and to identify some possible futures or scenarios for private life and privacy in about ten or twelve years from now. Any responsible attempt to derive recommendations for public policy must try to test its prescriptions by considering their performance in the context of imaginable futures. This is the heart of the test of cultural viability. The aim is certainly not to predict the future: there are plenty of forecasts and the only thing that we know about them for sure is that they are wrong. These scenarios are offered instead as ways
of thinking through risks, opportunities, preferences and possibilities. The purpose is to use possible futures as chess players and military strategies do, as a kind of risk assessment, and consider how strategies may operate in those contexts. It ought to be considered more remarkable than it is that democratic political parties and governments seem – at least in public – to do so little of this.

In the fourth and final part of the book, I turn to the challenges that this presents for public policy, at both the national and the supranational levels. Chapter 16 defines and introduces the main conflicts between privacy and other claims, values, rights and duties, which together form the public policy dilemmas about the protection of private life. Subsequent chapters deal with conflicts between privacy and media freedom; the accountability of people in public life; issues of the distribution of risk; the conflict between economic and political liberty surrounding business use of personal information; data protection; law enforcement and claims of right by business and individuals to use cryptography; issues that bring together privacy concerns with questions about how risk should be distributed between different individuals and groups in society; and finally dilemmas of issues of public education about privacy risks.

Volume 2 presents and analyses in some detail a new survey of public attitudes on privacy undertaken in the course of the research for this book. The survey aimed to identify, for the first time in Britain just why people trust certain kinds of organisations with their personal information and exactly what risks individuals trust these organisations not to expose them to in handling information about them. Understanding the reasons and tasks for trust in personal data handling will be an increasingly central part of business strategy in many fields and, in Volume 2, a number of specific implications are drawn out from the strategies of leading business and government agencies handling information about individuals.
Notes

1. For an example of such a standard text – which, I should add, does what it does well, rigorously and usefully – see Dunn WN, 1994, *Public policy analysis: an introduction*, Prentice-Hall, Englewood Cliffs, New Jersey. The problem is with what it does not set out to do, which, I argue, comprises much of the interest and difficulty of the policy sciences.


3. Research project grant R000221949.

Part 1
Private life
1 Origins

Privacy is one of the major flashpoints of political, industrial and cultural conflict of our times. The controversies over the role of the paparazzi in the death of Diana, Princess of Wales, the bitter battles in Congress over the US administration’s attempts to keep control of encryption, the eruptions of protests on the Internet against Lotus and Microsoft for what were felt to be privacy violations – all are symptoms of this conflict. At the heart of the issue is the growing capacity of business, government and media to gather, manipulate and disclose personal information on an industrial scale. Inevitably, at the end of a century dominated by struggles against totalitarian states by individuals seeking the refuge of private life, the shades of Orwell and Koestler\(^1\) are invoked in the context of growing government capacity for surveillance and dataveillance.\(^2\) The task for this book is to explore where this concern has come from, where it might lead, what it comes into conflict with and what can be done with these tensions.

Any exploration of possible futures for privacy must begin with an effort to understand how the value of privacy to people has changed over history and how it differs between societies.

Histories

Only in the late twentieth century has privacy become a central zone of cultural and political conflict. In the reaction against state surveillance
by totalitarian states in the post-war era, anxiety about privacy became widespread, not only in dystopian fiction such as Orwelли’s 1984 but in reality. It was on privacy grounds that challenges were brought in Britain against the continuation of the identity card scheme in peacetime. The advent of the mainframe computer brought new concerns. Data protection laws of various kinds spread throughout the developed world during the 1970s. The OECD and the Council of Europe formally adopted guidelines at the beginning of the 1980s. Campaigns against census collections of personal information have welled up in Britain, the Netherlands and other countries at least once in every generation since the war. Surveys of public opinion (see Volume 2) have generally identified rising public concern about privacy risks. While in Europe once (and in the USA largely still today) this concern was focused principally towards government, now it is directed towards the activities of executive government and business alike. Privacy concern appears to be at least as high as in the 1980s, if not slightly higher.

Certainly, it seems to be relatively recently and mainly in the developed world that societies have explicitly given attention to efforts to protect private life from various kinds of intrusion. But this fact alone tells us little. In fact, some of the values that today underpin our modern conception of privacy have been an implicit concern for much longer and on a much larger scale than was thought without leading to the recent rise in interest in privacy protection.

There are three themes that dominate the main histories of privacy. One explains the rising demand for privacy as a consequence of the development of a culture of individualism. The experience, self-consciousness, behaviour, social network position and role bearing of individuality is common to all human beings: individualism as a cultural formation stresses the value of individual liberty, autonomy, choice. Control is a more recent phenomenon variously dated from the Renaissance, the Enlightenment, or more recently still from the nineteenth century.

The second strain stresses urbanism and argues that, in agrarian societies, the proximity and mutual involvement of people in each
others’ lives makes the experience of privacy practically impossible and therefore not even thinkable, let alone desirable.\textsuperscript{7}

The third stresses the risk to privacy from the development of techniques for the collection, storage, selection, matching, analysis, disclosure and publication of information.\textsuperscript{8} None of these arguments is completely compelling, at least in the forms they are generally made.

**Individualism**

The individualism story of privacy has a chronological, geographical and logical problem. The chronological problem is that the demand for legal protection for privacy comes so very late in the day, long after the rise of individualism, whenever it actually started. The first legal decisions on privacy do not really appear until the very beginning of the twentieth century; the main constitutional commitments and international conventions offering some general protection are all phenomena of the second half of the twentieth century; and the main statutory interventions such as data protection legislation all appear in the last quarter of the twentieth century.\textsuperscript{9} Indeed, privacy has been a latecomer in the development of liberal constitutional or legislative rights for the individual and is still relatively insecurely grounded by comparison with eighteenth and nineteenth century efforts to buttress rights against arbitrary arrest, rights to freedom of conscience, association, speech and to vote for elected representatives.\textsuperscript{10}

The geographical problem is that in many conventional ways (limited labour market regulation, social insurance and so on), the most individualistic society on earth is surely the United States, which has as yet no general data protection law at federal level.\textsuperscript{11} Moreover, in the USA, individualist arguments about economic liberty are frequently deployed against proposals for data protection or press privacy law, on the grounds that these would present unacceptable interventions in freedom to trade using personal information.

The logical problem with the individualist history is that many claims to privacy cannot readily be reduced to claims of liberty and autonomy. The concerns of data protection and press privacy law are
not all about the power or right to make certain fundamental or important kinds of decision for oneself and carry them out without the obstruction of government coercive power. Rather, they tend more often to be about claims to *dignity*.¹²

**Urbanism**

The story about urbanism is not wholly satisfactory either. It does not follow from the unavailability of some experience in some society that at least some people in that society will not long for it, have no concept of it, see no purpose in it. Insofar as what is valued in privacy is a certain kind of experience or behaviour, then, presumably, we are concerned with solitude, which is certainly available – and positively valued by many religious and spiritually minded people – in agrarian societies.

**Informatics**

At first sight, the informatics story about privacy might appear to conform more suitably with the chronology of the rising demand for formal privacy protection, in that the large scale use of computers for professing personal information is a post-war development. But here again, there are serious chronological problems with this history.

To some extent, state surveillance of citizens and the collection, storage and analysis of information about individuals are as old as the state itself. The Sumerian state archives, Tacitus’s strictures against the networks of spies working for various Caesars, biblical complaints against Herod’s census, assorted peasants’ revolts against tax assessment in mediaeval times all reflect concern about the surveillance capacities of the state, long before the era of George Orwell. While there has certainly been a great increase in the volumes of personal data collected by government in the last two centuries, it is not the case that the advent of the computer in the 1970s represented a fundamental change in the nature of government surveillance.

Previous historical enhancements in capacities for collecting, storing, analysing, moving and sharing information do not seem to have given rise to strong privacy concerns. Printing represented a step
change in collection and storage capacity, yet the objections to printing seem to have been based on quite different grounds. While there were late nineteenth century privacy concerns about press photography, they were hardly the most salient ones about that technology. If the theory were correct, one would have expected that telegraphy, morse code, telephony, the typewriter and the reorganisation of business and government that they brought about would have provoked a major storm of privacy activism but this was not the case. In general, objections to technological development are rarely based on privacy grounds but mostly on fears of the loss of traditional jobs.

Although none of these is an adequate explanation of why privacy came to be so salient so late, individualism, urbanism and informatics no doubt all play a role in the gradual rise of concern about privacy.

But the inadequacy of the informatics history does suggest very strongly that one important hypothesis about the future of privacy should be rejected, namely that of technological determinism – the idea that developing information and communication technologies will determine the possibility, thinkability and desirability of privacy. Of course, information and communications technologies are centrally important in the context in which we seek privacy, in the ways which we can seek to define, protect and develop it. But they do not determine in any simple way our conception of human dignity and what we want for private life.

Secondly, to understand privacy it is important that we focus at least as much on the the history of the experience and behaviour of private life as on history of claims to rights to privacy. For this is what each of the three standard histories fail to take account of.

**Private life and modernity**

A full explanation of the rise of privacy concern must, this book argues, base itself on historic changes in cultures of what is valued and perceived to be at risk in private life and, in particular, in the rise during the later Enlightenment of a liberal culture which eventually fractured in the twentieth century, particularly sharply in the post-war era.
In later chapters, this understanding of cultural formations will be developed more fully. However, at this stage, some points about the historical role of the idea of private life are necessary.

While the experience of private life is not only a feature of modern societies, as anthropologists working in many technologically simpler societies can attest, modernity has made a number of major transformations of the experience and behaviours of private life.

The idea of interiority can be traced back to pre-modern origins, not least in the classical Athenian idea of the examined life, and later the Hellenistic and early Christian debates about the merits of the contemplative life. However, with the advent of mass reading alone and in silence, following the spread of printing during the Reformation, came among many people an intensification of interest in the interior life as the site of personal piety. In the eighteenth century, the romantics brought a huge reorganisation of interiority among the literate classes. In the more rugged outdoor romantic sensibility, solitude became at once a private experience of nature and a private consciousness of a supposedly authentic self, by contrast with the inauthenticity of the debased selfhood of diurnal sociability – a current of thought revived briefly in twentieth century existentialist ideas.

However, long before interiority came to be opposed, in the romantic age, to the intrusion of the inauthentic, it was felt to be opposed rather to a rival but equally authentic discipline or regime of life. Interiority was a course to be followed, with its own standards of behaviour, norms. Far from being a space in which one did or thought as one pleased, at least before Rousseau’s *Rêveries*, the interior life was generally thought of as a demanding and disciplined programme, whether in its religious forms or in the near secular self-exploration of Montaigne. Moreover, interiority was at least as much a public stance of individualism against the weight of social tradition and authority as it was absorption in a sphere of life specifically created as private.

More specifically, when the interiority or intimacy or space for family life or personal development is violated, what is violated has not generally been regarded as personal liberty. In general, what has been
feared has been loss of honour, or, nowadays, of dignity, or the invasion and corruption of the integrity of a sphere of life seen as ‘personal’. As we shall see, there are some risks to privacy that do represent injustice and even infringement of liberty. However, the reduction of privacy – as in the US litigation on abortion – to considerations of liberty has the effect of downgrading the status of claims to human dignity, and hollowing out the complex currents of moral sensibility that make up concerns about privacy.

The connection between privacy and dignity can be seen in the development in modernity of manners, of politesse and civility. At least since the Renaissance, behaviours and bodily habits once considered acceptable and normal in public first became coarse and boorish at court, then among the middle class and finally even in private. The exhibition of bodily functions in public, in particular, gradually came to be seen as matter of pollution and taboo, by bringing bodily matter into an inappropriate place, to which privacy is the proper disciplinary response. The causes of this process are complex. Certainly it has something to do with the rising power of centralised, relatively sedentary rather than peripatetic monarchy, leading to the absolutist strategy of centralising noble life in royal palaces rather than in the countryside or allowing freebooting military activity.

Secondly, the rise of powerful mercantile and trading classes in many parts of Europe was important. Gradually, a public conception of personal dignity became transmuted into a private discipline of bourgeois dignity in private life. As military and later courtly honour became bourgeois dignity, it became more individualised. Only at the beginning of the French Revolution was the idea of family honour, as something that any family member can besmirch for the whole dynasty, formally debated and rejected in favour of a wholly and explicitly individual notion of personal standing. Gradually, the pietistic and later romantic commitment to interiority enabled the emergence of a conception of honour but not so much around display as around integrity. In the nineteenth century, the workerist tradition began to demand a recognition of dignity in labour itself, more on the basis of integrity than public display, which over time merged with
more middle class ideas until, with the turn of the century, the idea of the respectable working class emerged with a particular claim to dignity in private life.

The design of the modern home, with differentiation between rooms according to a conception of the differing degrees of privacy or publicity of the activities intended to be conducted in each, dates largely from the eighteenth century and did not become a mass phenomenon until the industrial age. In the mid to late nineteenth century, the demand for privacy of family life may have increased as expectations of the nourishment from family life rose temporarily at least among some sections of the middle class, perhaps in reaction against what were seen as the excesses of the romantic age.

Privacy is, therefore, by the early twentieth century as much a construction of shame and embarrassment at relatively ordinary behaviours that only became unacceptable in public, let alone in private, in modern times. Indeed, the availability of individually private space within the home did not become a mass experience in Europe until the late nineteenth and early twentieth centuries, when several key developments became the norm for most people. Home and work became finally and completely separated for most males, leaving married women and dependent daughters confined to a space now become private; a room of one's own became a common expectation and the division of functions of rooms became settled; home became a place where one acts as spectator in a private space on the rest of life, through the intrusion into the home of media such as radio, television and the personal computer; and paternal authority ceased to order the home and the whole of family life.

The rise of the ideal and aspiration of the individual person as a character or personality, of which the greatest symptom is the growth of the novel of character from the eighteenth through to the twentieth centuries, has been accompanied by a growth in the idea of education as the making of character and the Freudian conception of the solving of problems as the integration of private character. In this ‘intimate society,’ in which the impersonal is feared above all, it becomes natural to conceive of life as a search for private or intimate meaning.
and experience, in which a personal project is the defining feature of character and self-discovery and self-expression are respectively the paedagogical and public forms of private life.22

It is therefore one of the ironies of twentieth century history that it should have offered people in the developed world at once greater expectations of privacy than ever before and presented them with greater capacities for what came to be experienced as intrusion into that privacy from outside the family than were ever previously possible.

One signature of this twentieth century conflict is the rise of confessionalism and display at the same time as privacy. Politicians often wallow in the act of baring their souls. We in turn expect them to demonstrate ever more of their private lives in order to convince us that they are not hypocrites, that they live lives like our own and they are willing to submit to a public accountability which we ourselves would be horrified by and yet which we remain envious of and fascinated by. Celebrities live by a kind of striptease of their own privacy. Some quite ordinary individuals long for the chance to divulge their private life to newspapers or in a court. The display of the private body is often (and not only for younger people) a commitment of lifestyle.23 Yet these are essentially activities that are parasitic upon privacy. For if everyone told or showed all routinely, these behaviours would lose all their frisson.

Private life has been set about with detailed prescriptions and codes of how intimacy, family life, maturation and lifestyle are to be conducted, even when not directly under scrutiny. However, it has not been principally conceived and conducted in modernity as a space behind which what would be scandalous is tolerated and agreed to be hidden, but as a discipline or regime through which social life is conducted. Some of the principal definers of private life have, therefore, always been what we might call style counsellors – those who professionally peddle through advertising, newspapers, broadcasting, literature and arts, the current range of norms and standards for lifestyles, personal expression, manners, taste in clothes or home furnishings. Style, in this sense has become increasingly important as personal styles have been branded, catalogued, marketed and segmented by
business in the effort at once to monitor and target tastes, and also to persuade the adoption of tastes and certain associated disciplines of what to do in private. Prophets thundered for centuries against the corruptions of luxury and civic privatism that they considered style counsellors to propagate, and there are still – although muted – voices of asceticism. Private life is always subject to the disciplines of public style and morality.

At the same time as private space in the home has been assembled, modern societies have built a new series of social roles and identity around private and personal life, reinforced through the disciplines of the media. Privacy has become, in the twentieth century, a zone of private life. For there are newspapers, magazines, broadcast programmes, Internet sites, which relentlessly counsel us with what styles to manage our personal finances, our sex ‘lives’, our behaviour as parents, friends, consumers. This disciplining of private life has made of it the sensitive, the personal and yet the stylistically accountable experience that it has become. Failure to achieve the standards imagined and prescribed by the modern style counsellors is felt by many to be a risk to modern dignity.

Claims to rights to privacy emerged first in connection with the prurience of the press about private life and later in connection with the growing surveillance capacities of the state and, more recently, of business. Before the late nineteenth century, aspirations for individual privacy were vaguely imagined as being more to do with liberty against familial and particularly parental authority than against formal external institutions and organisations. At least in the twentieth century, it has proved difficult to ground claims of rights and duties on considerations other than personal liberty and either distributive, retributive or procedural justice. Dignity, although important to most people in every society, is not well articulated in moral languages that stress only rights and justice. This has left privacy claims that were really and fundamentally about a modern conception of human dignity ever more enmeshed with those ideas, even though only a relatively small number of privacy risks are directly concerned with injustice.
In order to understand how it became so difficult to frame claims of duties and rights in terms of dignity, the next two chapters explore the relationship between the different things that are valued in privacy. The argument proceeds in three stages. Firstly (Chapter 2), we look at the things perceived as threats or risks, where appreciation of what is valued is often most clearly elicited. Secondly (Chapter 3), we look at these values directly. Finally, (Chapter 4), these values are in turn organised by a small number of central but rival traditions of political thought. Through these traditions, the idea of privacy has been framed, articulated and expressed in the moral and political arena since early modern times.
Types of privacy concerns

Privacy, it has rightly been lamented, cannot be defined very satisfactorily. One can offer very general definitions, such as that presented by one of the principal texts in the field:

The claim of individuals, groups or institutions to determine for themselves when, how and to what extent, information about them is communicated to others.26

Such definitions have the merit of honesty: they do not pretend to be able to settle any of the hard questions about how important such claims are, when and how they can be protected, when privacy claims trump other claims in cases of legal or moral conflict. Definitions only take us so far: we also need a better characterisation of privacy.

One can identify some of the key interests that people have in privacy, as another classic of the field did, in a list of rights claimed to:

- provide individual autonomy
- be left alone
- have a private life
- control information about oneself
- limit accessibility
have exclusive control of access to private realms
minimise intrusiveness
expect confidentiality
enjoy solitude
enjoy intimacy
enjoy anonymity
enjoy reserve
enjoy secrecy.

Unfortunately, this kind of list is lacking in structure, has many overlaps and gives little guidance about the weight of such putative rights. Indeed, to build the concept of a right into the characterisation of privacy may already be premature.

Another approach is to consider specific contexts in which claims arise in which the concept of ‘the private’ is raised. One can distinguish between:

- people who do not hold public office
- organisations that are not state or government owned
- facts known either only to one or a small number of people, or activities carried out in seclusion, or either facts or activities that have a limited impact or effect
- issues or behaviour that are not a (legitimate) matter of scrutiny by any authorised others (such as companies with whom one has a contract, executive government or the courts or the media)
- places to which access may (legitimately) be denied to others, except in specific legally authorised circumstances
- property that is subject to largely unrestricted personal property rights
- interests of specific individuals, groups, organisations, industry or identities.28

The brackets around the appearances of the idea of legitimacy in connection with privacy are to stress that there are undoubtedly
many claims to privacy that do not prove justifiable and therefore legitimate.

A common response to this problem is to distinguish privacy issues arising in connection with personal information from those dealing with physical access to bodies and places and from those concerned with autonomy in the making of decisions about certain choices in life. One leading writer suggests that it is better to offer a definition of personal information and then to consider in practical contexts when it is reasonable to protect claims to withhold such information from others. Personal information is defined as consisting of:

Those facts, communications, or opinions which relate to the individual, and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict their collection, use or circulation.

Privacy then appears as but one kind of claim for reasonable withholding, alongside the law of discovery, the law of privilege in the solicitor-client relationship, police and regulatory powers of investigation and seizure, civil rights to silence or not to incriminate oneself and so on. Alternatively, privacy can be seen as a special case of the wider class of fiduciary – that is duty bound beyond the requirements of voluntary contract – relationships of loyalty and confidentiality.

These are all useful initial characterisations of privacy interests and concerns. However, they share a common limitation: in defining privacy positively, they can serve to obscure the negative role of privacy as a claim for protection against risk.

The premise of our argument is that the concept of privacy is usually advanced as a claim for protection against a series of risks; for understanding this, the literature on risk perception, risk cultures, risk assessment and risk management offer useful tools. This enables us to see the history, cultures, conflicts and sustainable futures of privacy in a quite distinctive light. In the next section, the conception of the key
privacy risks will be introduced and, in subsequent chapters, the literatures on risk cultures will be applied, to offer a distinctive interpretation of where ideas about risk can be situated in contemporary cultures.

**Privacy through the lens of risk**

No one could ever have complete control over the information about themselves that is created in the hand of others: what people make a mental note about as they see us in the street; what they jot down in their diaries or letters; what they record about each transaction with us are all matters over which we have rather limited control. The coercive power of the state to assess liability for and collect taxes on income, purchases (VAT), general wealth (for example, inheritance and capital gains) or particular assets (cars) or even behaviour (pollution taxes), its schemes of registration for births, marriages and deaths, conducting censuses, and so on all represent major abridgements of any putative right to control what is known about us. In any literal sense, a ‘right not to be known about’ would be enforceable only by a completely self-sufficient hermit. It is therefore very difficult to define privacy as ‘informational self-ownership’, if by that one understands the idea of normal property rights to control personal information about oneself which is in the hands of other people.

Nevertheless, most people share a basic sense that there is a zone of private life that deserves some kind of protection, about which we have some kinds of claim to influence how far others can come to know about us or even rule out certain things, if we wish to. In short, people share – although in differing degrees about different issues – a sense that there are certain *risks to privacy* that are worth being concerned about.

The main risks with which most individuals are concerned can be grouped under three headings.

**Risks of injustice**

The first group covers those privacy risks that mainly concern possibilities of injustice. Businesses may want to use personal information for
purposes quite other than those for which it was collected and to disclose it to other businesses even though the individuals concerned have not consented to such disclosures. The consequence of such data matching may be that inferences are made about individuals which are quite incorrect and lead to treatment, denial of service or refusal to grant entitlement that is unjust. I shall call such cases ‘unjust inferences’.

- **Significant inaccuracy**: while trivial inaccuracies of spelling do not usually lead to injustice even relatively minor mistakes can lead to cases of mistaken identity resulting in unjust treatment. Typically, much more significant are inaccuracies concerning facts about individuals circumstances that may lead to unjust treatment.

- **Unjust inference**, or the risk that, by collecting personal data or by linking two or more sets of personal information that were originally collected for very different purposes, incorrect inferences may be drawn. In consequence, unjust decisions made about entitlement to service or treatment.

- **Function creep**, or the risk that, data collected for one purpose will gradually be used for others, to which the subjects have not consented.

- **Reversal of the presumption of innocence**, or, where data matching is conducted in order to detect or minimise crime, non-entitlement, fraud, moral hazard or adverse selection, the risk that systems for handling personal data can readily become a means of using ‘red alert characteristics’ of individuals – ethnicity, use of cash where credit card would be expected, national origin, place of residence – as the basis for ‘categorical suspicion’. In other words, service or entitlement is denied on the basis of suspicion of abuse based on inferences, very often incorrect, from behaviour that can be undertaken quite innocently. This can have the effect of reversing the presumption of innocence until guilt is proven.
Risks to personal control over collection of personal information

Whereas the first group is concerned with the use of data, the second group includes those concerned with possibilities of loss of control over the procedures by which personal information is collected and created. For example, the collection of e-mail addresses from everyone who ‘visits’ many World Wide Web sites (part of a cluster of practices known revealingly as ‘data capture’) without the knowledge of the person concerned is now a widespread practice and one of which many Internet users are probably unaware.

- **Excessive or unjustified surveillance** or the capacity of business or government agencies to trace and profile one’s behaviour, attitudes, communications, speech, networks and so on, when those organisations have neither a valid need nor a valid right to do so. Many cases of the collection of what are conventionally regarded as ‘sensitive’ data are cases of this kind, where they are not necessary for the purpose of the transaction with the individual.

- **Collection of data without the consent of the subject** in contexts where there is no obvious reason (such as the need to levy mandatory taxation or subject firms to mandatory regulation) to set aside the need for consent.

- **Denial of access to the means of protecting oneself from any of these risks**, such as the right to acquire and use strong cryptography and other security procedures at least partly to protect confidentiality.

Risks to dignity by exposure or embarrassment

The third group covers exposure and disclosure, in which what is principally at stake is the dignity and reputation of the subject by way of some shame or embarrassment. Dignity concerns arise in connection with being subjected to surveillance where this is not considered necessary for the carrying on of ordinary and legitimate business or
governance and, secondly, where that surveillance has costs upon the individual, who is constrained from doing things that might be beneficial to themselves or others. This is not normally the issue in respect of criminal activity, where we normally override considerations of privacy to allow for proper and legitimate investigation. More often, privacy risks about dignity arise in respect of ordinary but 'personal' activity or experience. The best understood examples of this group are those occurring in connection with press intrusion and also in cases of routine police surveillance of persons against whom no reasonable suspicion has been established.

- **Absence of transparency**, or the risk that personal information will be disclosed, exchanged and used in decisions about treatment or access to resources and services, where one does not know of the existence, content, accuracy or authority for collection and use of that information.

- **Physical intrusion into space** defined as private or observation and collection of information about behaviour defined as private even though conducted in a physically public place.

- **Absence of anonymity**, or the capacity of business or government agencies to connect information about behaviour or attitudes to someone’s true identity, when those organisations have no valid need or right to know the person’s true identity to carry out their legitimate activities.

- **Unnecessary or unjustified disclosure or disclosure without consent**, or the risk that organisations – including the press and media – holding personal information about someone will disclose it to other agencies, either without that person’s consent or where consent is not actually required.

It is worth making two points about how this classification of risks relates to the conventional data protection principles. First, what data protection lawyers know as fair obtaining and processing of personal information is a response to the risks of unjust inference, function
creep, excessive collection, collection without consent and reversal of the presumption of innocence, to the extent that data protection law is designed to protect against them. Second, an understanding of privacy risks that sees dignity as being at least as important as liberty and justice makes it clear that issues of security and lawfulness in data protection are as much matters of privacy as are fair obtaining and processing.

Each of these types of risk may lead to others. Unjust inference can be the occasion that causes physical intrusion and vice versa. Injustice can lead to loss of dignity and vice versa. While it is true that injustice, loss of control and indignity are not the same thing and that people place different emphases within this group of risks, they are closely related and have a sufficiently significant common core of concerns. They are risks about the spheres of personal space and personal identity in description, which together make up the twentieth century conception of private life and deserve to be treated together. The privacy issues raised by the physical intrusion of press photographers and by the manipulations of data banks on customers and potential customers by large corporations, and on citizens, taxpayers, claimants and litigants by government, are sufficiently similar for us to resist those who argue that, because there are different types of risks involved, the generic concept of privacy should be dissolved into its constituent parts.33

Throughout this book, I shall return to these classifications of types of risk, as we explore the risks that particular forces and factors expose us to or partially protect us from and in considering policy recommendations.

Situating privacy in the world of risks

Looking at privacy through the lens of risk perception, assessment and management can be a fruitful exercise because the taxonomies in those fields can help us to understand just what kinds of risks we are dealing with in privacy.

Summarising three decades of research in risk perception, Ortwin Renn distinguishes the following intuitive biases in how we view risk.34
By comparison with many of the risks that conventional risk perception, assessment and management scholarship concerns itself with, the harm from violations of privacy tend to be chronic rather than acute\textsuperscript{35} – there are relatively few fatalities and serious injuries. As a result, the mental availability of privacy risks for many people is low: that is to say, the concern is latent, low level and background rather than immediate, save in particular transactions, relationships or situations when dealing with certain organisations about which a person of a given cultural outlook has suspicions. The more acute risks are those of physical intrusion, reversal of the presumption of innocence, unjust inference and denial of the means of self-protection. Nevertheless, harms arising from privacy violations can become acute: for example, if unjust inference leads of the unjust denial of services to which someone would otherwise be entitled, acute harm can follow.

Occasional scandals such as outrageous press intrusions into privacy or government mistakes about individual identity leading to the wrong parent’s children being taken into care, may have an anchoring effect or some people, leading them to overestimate risks to themselves

<table>
<thead>
<tr>
<th>Bias</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>events that come to people’s mind immediately are rated as more probable than events that are less mentally available.</td>
</tr>
<tr>
<td>Anchoring effect</td>
<td>probabilities are adjusted to the information available or the perceived significance of the information.</td>
</tr>
<tr>
<td>Representativeness</td>
<td>singular events experienced in person or associated with properties of an event are regarded as more typical than information based on frequencies.</td>
</tr>
<tr>
<td>Avoidance of cognitive dissonance</td>
<td>information that challenges perceived probabilities that are already part of a belief system will either ignored or downplayed.</td>
</tr>
</tbody>
</table>
or others and in extreme cases may be taken as representative. Volume 2 explores the question of what might be going on when people report that they trust organisations with personal information, in situations where they regularly deal or perhaps have little choice but to deal with that organisation. In cases such as trust in personal information handling by family medical doctors, there is some evidence that people may persuade themselves that they trust because the psychological discomfort of not trusting someone whom you need to resort to, is too great. This is a spillover effect from esteem to trust. However, it is not clear from the data reported in Volume 2 that this effect can be traced through all the cases studied there.

Renn goes on, after summarising findings from risk psychology, to offer the following classification of images through which risks are classified and seen by individuals.

As we shall see, there are different cultural traditions about private life and privacy that bring to bear different images about particular

---

**Figure 2** Images of risk in public perception

<table>
<thead>
<tr>
<th>Images</th>
<th>Key elements of content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending danger</td>
<td>Artificial risk source; large catastrophic potential; inequitable risk-benefit distribution</td>
</tr>
<tr>
<td>(Damocles’ sword)</td>
<td></td>
</tr>
<tr>
<td>Slow killers</td>
<td>(Artificial) ingredient in food, water, air; delayed effects, non-catastrophic; contingent on information rather than experience; quest for deterministic risk management; strong incentive for seeking someone to blame</td>
</tr>
<tr>
<td>(Pandora’s box)</td>
<td></td>
</tr>
<tr>
<td>Cost-benefit ratio</td>
<td>Confined to monetary gains and losses; orientation towards variance of distribution rather than expected value; asymmetry between risks and gains; dominance of probabilistic thinking;</td>
</tr>
<tr>
<td>(Athena’s scale)</td>
<td></td>
</tr>
<tr>
<td>Avocational thrill</td>
<td>Personal control over degree of risk; personal skills necessary to master; voluntary activity; non-catastrophic consequences</td>
</tr>
<tr>
<td>(Hercules’ image)</td>
<td></td>
</tr>
</tbody>
</table>
privacy risks. Although the classification has some limitations, the main survey research on how people think about privacy risks – reviewed in detail in Volume 2 – suggests that people can be divided into three broad groups:\footnote{36}

- **Unconcerned about privacy**: willing to provide to or allow collection of personal information by organisations.
- **Privacy pragmatists**: willing to make explicit trade-offs, in which personal information is provided or allowed to be collected in return for specific benefits, such as enhancements of service, personalised service, discounts and so on.
- **Privacy fundamentalists**: unwilling to provide personal information except in situations over which they have a high degree of control over the users and uses of that information.

One would therefore expect that privacy pragmatists would tend to adopt either the *cost-benefit ratio* view of privacy risks, at least in dealing with commercial organisations and perhaps also with some public bodies; that privacy fundamentalists would see privacy risks either as *pending dangers* or else, in Renn’s terms, as *slow killers*. There have been several surveys of Internet users which find that privacy is one of the top concerns among that group.\footnote{37} This may reflect, for example, a widespread culture among them that privacy violations take the form of something analogous to *slow killers*. However, this classification of risk perceptions does not really deal effectively with the ‘unconcerned’: this may not be a weakness after all if, as is suggested in Volume 2, there are fewer of the truly unconcerned than some of the survey evidence suggests.

In the middle years of the twentieth century, government privacy violations provoked a response among some cultural traditions rather like that associated with *slow killers*: government was blamed, some associated the advent of the welfare state with totalitarianism, means tests were regarded as intrusive and in the 1950s the legal basis of
Britain’s continued wartime paper identity card was challenged. Similarly, when the press physically intrudes upon the privacy of either those of the famous believed to be decent and deserving (the way that many saw Diana, Princess of Wales) or else ordinary people seen to be caught up in a media story in which they are blameless (children of politicians or film stars who are hounded by press photographers), the same kind of reaction can follow. However, there are clearly many of those who are regularly in the news who look upon press invasions of privacy through the colder eyes of cost-benefit ratio calculations and there may be some other celebrities who perhaps even court publicity and who regard risking occasional intrusions on their privacy as part of what Renn calls the avocational thrill.

Unlike the risks of fatalities and morbidity usually studied by risk scholars, privacy risks are not usually ones in which there are major differences of understanding between the public and scientific experts, for rarely do experts in personal data management offer risk assessments on the principal privacy risks. If there was a scientific discipline which could offer quantitative risk assessments in the field of privacy, it would presumably be that of organisational and management researchers but they rarely undertake such studies – not least because there are few clients other than national privacy regulators.

Those who take the view of risk in which perception is merely irrational deviation from the proper calculation of objective probabilities of objective harms and should not be the basis of public policy will consider that this leaves the understanding of privacy risks in a parlous state. However, it may also have certain advantages in this context. There is fundamental disagreement about whether privacy violations should count as risks of harm at all. Some law enforcers and others of an authority-centred cast of mind, as well as newspaper editors and direct marketers who start from a position of the priority of economic liberty for their businesses, take the view that privacy is something to which individuals are not entitled or at least that it is overridden by other rights and duties. Given such radical disagreements between the leading traditions of thought about privacy and private life, it is not clear that the development of better quantitative scientific assessments
of the probability of particular privacy-related behaviours would in fact help settle any of the basic theoretical and political issues. It may be to the advantage of the field that these hard questions must be handled directly, by assessing the ethical, political and philosophical assumptions underlying these traditions.
Ideas and values of private life

When societies go through fundamental transformations, conceptions of how far the private life of individuals, households and families are rightly known and accountable to the disciplines of the wider society and of how far that private life should be protected from this scrutiny do change and compete with each other.

The globalising society of the developed world is in such a period of fundamental change now that much is accepted by people with widely differing views about what kind of change is under way – to a digital age, an information age, high or later modernity, post-modernity, post-industrial society, risk society and so on. Yet, unlike other periods of great transformation, our globalising society is not particularly fertile in ideas about how private life will relate to public life. Following both the collapse of socialism and the widespread intellectual and political retreat from radical economistic individualism, our moral language is strangely impoverished and leaves us with limited understanding of what kind of private life is now on offer, what we want for it and what kind of public scrutiny we find acceptable.

Whenever moral sensibility becomes impoverished, not only is there questioning and debate about private life but fatalism also spreads. Today, there is a widespread if shallow resignation that private life is now so completely mapped by marketing managers and public officials that individuals can hope for little or no control over privacy.
Privacy, many people have come at least on occasion to say, is now something only to be achieved when institutions are inefficient and fragmented and that even then it offers but a temporary and unstable niche in the interstices of social domination by information, soon to be swept away by modernisation. In fact, for very few people is fatalism the only or even the dominant attitude to privacy. Rather, it has become an easily accessible part of the repertoire of values, even if it does not run very deep. As the evidence presented in Volume 2 shows, many people who hold firmly to certain values in private life and privacy also display some fatalist attitudes. The danger is that what is now a veneer may begin to corrupt what lies beneath.

Because the ideas of private life are intimately connected with our conceptions of liberty, justice, human dignity, individuality and family life, as well as our ideas about the scope and limits of organised power, this attenuation of moral language and fatalism matters enormously. What we now value in private life and how far it should be protected and against what are not side issues. On the contrary, these questions go to the heart of those matters, universally acknowledged to be central ones for our society – about business power and business ethics in a global economy, about the nature and scope of government, about what education and learning should prepare us for, about the claims, obligations and accountabilities we can legitimately and effectively place upon individuals and institutions.

For many purposes, we have come to imagine privacy to be practically identical with liberty. In particular, it has come to characterise privacy as the ‘right to be left alone’, with the implicit assumption that we are left alone to do as we please. In the United States, even decisions about whether or not to abort an unwanted child are now debated, represented and litigated in terms of privacy. What is not your business is mine – in the senses of property, control and choice. Privacy is often described as the sphere where choices are not publicly accountable. Respecting someone’s private life then becomes a matter of maintaining ignorance or at least maintaining confidentiality and refraining from disclosure to others or publication if ignorance has already been surrendered. It is but a short step from here to a conception of privacy
as a set of claims about procedures in the handling of information of certain kinds about individuals.

Business and government have developed more and more sophisticated ways – from closed circuit television through press intrusions to ‘loyalty’ card schemes that connect every purchase to an identity to build up profiles – in which to roll back the frontiers of public ignorance about private choice, style and consumption. Thus we have grown accustomed to the idea that private life is little more than a pattern of consumption that may be routinely mapped and disclosed by marketers or the media. Because we have few other conceptions of what privacy is and what it is for, so many have become at least partly fatalistic about its preservation.

Mapping what is valued in privacy

What a society really values when it uses the vocabularies of privacy will change over time, as different kinds of private life and private experience become possible, thinkable, desirable or considered base.

Certainly, there is no single thing that any society will value in privacy: societies are too complex to agree on fundamental values. Nevertheless, it is not helpful to divide up privacy into ‘informational’ and ‘other’ kinds supposedly too vague to be worth thinking about clearly, as some writers seem to suggest, or to decompose it into a series of other claims to do with general liberty, property rights, rights to reputation, claims to be free from annoying interruption in the course of ordinary activity, and so on.

Private experience in almost any complex society spans the range from interior life (which often takes the behavioural form of solitude or, adversely, loneliness) to intimacy, personal development, family and personal social identity or distinctiveness. Because privacy is a social as well as a solitary matter, certain social roles are associated with each of these privacy experiences. For these experiences of private life to be possible, and to become valued, societies have to organise themselves in particular ways. The experience of private life is not valued if it is experienced as deprivation – if solitude is little more than
loneliness and isolation, if intimacy is enforced in shotgun weddings or total institutions. The revolt of the private – such as those made by religious pietists, by eighteenth and nineteenth century romantics, or by early twentieth century feminists (Woolf’s A room of one’s own) – only become possible when a positive experience of privacy has become thinkable and available.

What is sought may be the opportunity to explore these experiences or to undertake these roles in private life, without some kind of intrusion, or without being subject to the surveillance of others, or with the confidence that others will respect one’s (family’s) desire that secrecy about certain things be maintained. Secondly, what is sought may be a certain respect, recognition or tolerance for the status of experiences and behaviours conducted as part of private life, even if known about by others and occasionally disclosed by them. Thirdly, what is sought may be some accountability or recompense against others who default on some claim for unintruded or respected private life.

Just as privacy is a social behaviour, so it is as often behaviour in the open, not in seclusion. Many things that we often consider to be part of private life are done in physically public places. Holidays, shopping, eating meals and even working can all be matters in which we seek an absence of surveillance or intrusion or about which we seek respect and recognition as activities deserving private status. The risks that we perceive to private life in these contexts are often as much to do with exposure of the ordinary rather than the extraordinary – of ordinary activities of which only certain kinds of display are taboo, such as sex, death and wealth.

In other cases, it is not so much exposure per se that is feared as the reduction, coarsening, trivialisation and vulgarisation of private life through private experience and behaviour being recorded, classified, enumerated, analysed and divulged in a prescribed format. ‘I’m not just a bar code’ is a common complaint. In such situations the assertion of privacy is concerned with the experience of being classified according to the institutions of governance, business, religion or philanthropy. For when we value privacy, we just as often flee from anonymity as we seek it. At best, anonymity is a means of securing
some kinds of privacy by hiding us in a much larger crowd already classified and in other cases it may be the very means of demeaning private life that we dislike most.

We seek privacy in our own identity and in immediate relationships but also in transactions – for example, when we express concern about the collection and use of information about us by firms and government bodies.

A straightforward way of bringing together these things that are valued in privacy is offered in Figure 3, which gives examples of the kinds of social practice that sustain these experiences of private life. The figure moves from the most solitary practices of privacy on the left to the most social and even exhibitionist forms of privacy assertion on the right. The first row gives examples of the kinds of physical and social space claimed for private life and behaviour at each level; the second gives cases of the kinds of recognition, support or norms and

<table>
<thead>
<tr>
<th>Values</th>
<th>means of securing privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>value of privacy</td>
</tr>
</tbody>
</table>

**Figure 3  Examples of practices that sustain the key values of privacy**

<table>
<thead>
<tr>
<th>Value of privacy means of securing privacy</th>
<th>Interiority</th>
<th>Intimacy</th>
<th>Family</th>
<th>Material environment</th>
<th>Social distinctiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>private life in seclusion</td>
<td>the cell</td>
<td>niche</td>
<td>havens in the home, etc</td>
<td>lace curtains toleration</td>
<td></td>
</tr>
<tr>
<td>relationship, identity</td>
<td>tables in restaurants</td>
<td>respect, toleranc</td>
<td>norms of conversation, questioning, etc</td>
<td>lifestyle eccentricity sub-culture</td>
<td></td>
</tr>
<tr>
<td>assertion of selfhood</td>
<td></td>
<td></td>
<td></td>
<td>for control over classification</td>
<td></td>
</tr>
<tr>
<td>against classification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>private life in public public transaction, contract</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>assertion of selfhood</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>for control over classification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Accountability, redress and recompense    | breaking off relationships ostracism | confrontation |

This page is covered by the Demos open access licence. Some rights reserved. Full details of licence conditions are available at www.demos.co.uk/openaccess
institutions that are claimed in order for privacy to be sustained at each level; the third is concerned with the ways in which broadly liberal societies can – short of going to the law – try to hold accountable those individuals who seek privacy at each of these levels, and in turn with the everyday strategies that individuals whose privacy is violated can use to counter these violations. Thus, for example, we may sue in tort, use rights under data protection legislation or simply shun a business or individual that we consider has violated our privacy.

Firstly, privacy is as much a matter of social role as of a sphere of individual control and choice. Secondly, the enemies of and risks to privacy are numerous, as are the strategies by which individuals can hold their enemies accountable. Thirdly, privacy is a sphere in which people resist and seek control over the institutions by which their tastes, behaviours, experiences and roles are classified, as much as over the fact of others’ knowledge about them. In this sense, it is central to an understanding of what we value in privacy and private life that we see dignity as being as much at issue as liberty or justice.
Values do not come singly; they are organised into clusters or cultures.\textsuperscript{48} By this, I do not mean that politicians and intellectuals organise values into tidy groups for their own purposes. Rather, I mean that around these clusters, \textit{lived} cultures develop, in which daily life develops, social networks form, through which media work, by which conversations are organised and aspirations are formed. Traditions of thought, in the sense that I am concerned with here, are not just intellectual constructions but currents of mundane, demotic sensibility.

In this chapter, I distinguish four main traditions of thought or currents of political sensibility which have sought to articulate what is and is not possible or valuable about private life. They also offer different ideas of why some aspects of it should be protected against certain kinds of risks, what should be protected and how. More than this, they shape the way in which people’s recognition, fear and experience of the privacy risks amplify some and attenuate others. This means that traditions in effect teach us how to feel about privacy.\textsuperscript{49} Moreover, each is as much a culture of what \textit{loyalty} means as a culture of which privacy risks matter: the notion of a culture of privacy cannot be understood except in connection with the idea of a culture of loyalty.

\textbf{Currents of political sensibility}

The first is the civic republican tradition, and it can be traced from the ancient stoics through the ‘country’ party in seventeenth century...
England to revolutionary America with its concern for the virtuous citizenry on which the republic would be built.\textsuperscript{50} The austere disciplines of privacy are, in this tradition, bound to a conception of a community as one in which virtue is achieved primarily by the private discipline on both interests and passions.\textsuperscript{51} For, on this view, no invisible hand can coordinate private interests, no system of political intermediation can coordinate private factions, interests and passions, without the private cultivation of what the Adam Smith of the \textit{Theory of moral sentiments} called ‘the man within the breast’ or what Freud would later call the superego and processes of sublimation. Modern conservatism and ethical socialism, even in their more hierarchical and authority-focused forms, have followed the civic republican outlook on the provisional separation between public and private and the formative disciplining of private life rather than seeking to enforce a strict separation of spheres into one of authority and one of liberty.\textsuperscript{52}

This tradition stresses the dimension of privacy which is concerned principally with relationships. Intimacy and family life are regarded as the important aspects of private life and to be protected from market forces and politics mainly in order to enable this world of relationships to play its formative role.\textsuperscript{53} The more individualistic privacy concerns such as the need for solitude and interiority and for personal distinctiveness in social identity are not denied, but not given emphasis either. For in this tradition, privacy is the necessary sphere in which a person’s civic virtues are developed. The fundamental concern of the tradition is with the development of such stoic virtues of private behaviour as dignity, reserve, control and civility.

Friendship and sympathy with particular fellow citizens are emphasised and society is seen as a web or network of such intimate ties that make up a particular community and, ideally, a virtuous civic one. Friendship is an important model of private life for this tradition, for with friendship comes the primary duty of loyalty. The duty of confidentiality and secrecy about the private life of friends is grounded in a duty of personal loyalty. With the rise of the joint stock company, this model of the loyalty of friends was transferred to the corporate self and became the fiduciary duty of commercial confidentiality. That is
to say, in this tradition, loyalty to company is based upon an enduring relationship.

In general, in this tradition, only the very strong considerations of virtue can be recognised as overriding the fiduciary character of the loyalty relationship. Private life is the place where citizens are made, where civic virtue is both nurtured and steeled, and where a discipline of civilised reflection, self-control and peace is exemplified, learned and handed on to children. Privacy is then a place of lifelong self-pedagogy in virtue, as well as of inculcation of children in the personal style of virtue. While the veil of privacy over the family may be broken in order to enforce laws – privacy is no more a defence against violence or other serious crime in this tradition than in any other – the tradition fears the consequences of too frequent or drastic a breach of the private realm on the grounds that only there can virtue be inculcated.\textsuperscript{54}

Indeed, in this tradition, unless privacy is disciplined, and the desires educated in this fashion, the tradition fears corruption by private vices such as luxury, sloth, avarice – or the vices of private consumption and public apathy or ‘civic privatism’. The tradition seeks a proper, duty bound, balance of private autonomy and public virtue.\textsuperscript{55}

The second tradition articulating privacy is the liberal one.\textsuperscript{56} It can be traced from the romantic emphasis on the authentic self experienced self-consciously in solitude. This culture seeks liberty in privacy – indeed, hardly distinguishes between the two ideas – rather than discipline or dignity. Individuality rather than family or intimacy, is the moral and experiential basis of its conception of privacy. Personal development is considered important, even at the expense of family obligation. It sees privacy as a space for self-exploration and the formulation of a personal conception of the good rather than the practice of a given style of virtue. For this second tradition, the fiduciary duty of loyalty to a company or organisation is essentially contractual and enforceable only to the extent that the contract, with its compensation in remuneration, provides for it and rewards it. Moreover, where some higher duty – such as the duty of honesty and integrity owed to oneself – conflicts with it, it may be set aside and disclosures such as ‘whistleblowing’ may be justified.
It is not ironic but entirely natural that a tradition that begins with the romantic assertion of personal emotional freedom should also become a tradition which asserts personal economic freedom and privacy as something that is traded in transaction and contract. The tradition draws on the conceit of a neutral system that coordinates and brokers between private interests both in markets and in pluralistic politics.

In the liberal tradition, claims to privacy are often framed as matters of rights. True, such claims can be overridden when greater rights are at stake but in the liberal tradition privacy represents at the very least a strong presumption in favour of a protected realm of individually chosen activity and experience. Indeed, insofar as the liberal tradition makes use of the concept of dignity, it consists mainly in the respect for others as the bearers of rights with the capacity to exercise them.57

These two traditions do not exhaust the political cultures in which competing ideas about privacy have been developed. In particular, I want to draw attention to two other strains which are much less well articulated by political philosophers and thinkers, but which do represent important strands of popular culture.

The third strain can be found in many radical movements and in many kinds of institutions dedicated to the pursuit of spiritual and political goals. In this tradition, the private generally is suspect, although some moderates can find some instrumental value in it for the protection of their own movement or sect. Privacy claims can be seen as provisional ones (that is, ones that may be overridden in certain circumstances) to a certain unaccountability. This tradition places great stress on the duty of individuals to hold their lives accountable to the public judgement of the movement or the citizenry. The idea is that the responsibility of a life lived under the glare of publicity, criticism from fellow citizens and accountability of one’s life to this is the correlative of the ideals of solidarity and mutuality. The slogan of this tradition has been ‘the personal is political’. Institutions have been developed to give expression to this commitment, ranging from the public confession (‘self-criticism’ in the worst Maoist and Stalinist forms) and the denunciation (in Jacobin times) to, in milder times,
the consciousness raising group with its more supportively critical disciplines for mutual accountability. The private is considered to be the factional, the selfish or self-interested, that which is lacking in public spirit or the obligation to altruism. The secrecy of private life is to be subject to public scrutiny, precisely because the motives of individuals cannot be trusted.

Perhaps the most generic label which can be offered for this tradition is that of ‘egalitarianism’. Nevertheless, it is worth noting the extent to which it flourishes, in enclaves and sects, where the levels of activism, commitment and willingness to subject one’s life to politically guided public scrutiny can best be sustained. Moreover, its conception of membership of the public, to which private life and privacy are to be subordinated, is typically built upon the model of association, even when it is extended to given or ascribed identities such as citizenship of a nation, womanhood, a certain secular orientation or ethnicity.

It shares with civic republicanism the conception that what is private is subject to accountability but differs in that it places wholly in the public realm, the paedagogic, developmental, moral and interpersonal values and disciplines. It shares with liberalism a commitment to a model of life that is extrapolated from the condition of a transaction entered upon voluntarily but differs in its rejection of the idea of the private as a sphere of personal and accountable choice. Liberty, in the egalitarian tradition, is a matter of the collective freedom of the enlightened from domination by private power, not that of the individual from public power. Unlike civic republicans for whom loyalty is a discipline of friendship and unlike liberals for whom loyalty is a contractually basic responsibility, egalitarians see loyalty as principally the duty of the individual to be accountable to the community (which may be the sect, movement, society or national state) to which they owe a duty of political obligation.

Since the demise of the Jacobin and radical Marxist traditions such as Maoism, the most common political milieu in which the egalitarian rejection of privacy has been articulated is that of some varieties of radical feminism.58 In this tradition, the idea of the private as a sphere is rejected for the probability that what it would protect behind walls
of rights to privacy is likely to be abusive behaviour by men against women.\textsuperscript{59}

Within the feminist egalitarian tradition of privacy arises a second critique, particularly of civic republican and liberal conceptions of privacy. The argument focuses, as we might expect, on the social implications of the protection of privacy. It claims that the liberal and civic republican willingness to tolerate certain kinds of lifestyles or activities (for example, homosexuality) conducted in private devalues them, and deprives them of equality with other more widely accepted lifestyles that may attract the subsidy of the taxpayer (such as marriage or child rearing), and that toleration in private robs the chosen lifestyle of its value by denying it public expression and the right of public challenge.\textsuperscript{60}

There are moderate varieties of egalitarian culture, which value a measure of privacy at least as a protection for a movement or a sect, or at least are prepared to make common cause on occasion with political liberals when they fear that the accountability to which civic republicans would subject them would also threaten their movement or culture.

The fourth tradition sees the chances for privacy, however much or however little one might desire it, as very limited. It stresses the inevitability of large scale surveillance by public and private powers and the ratchet effect by which such powers gradually assemble ever more comprehensive and intrusive means to profile, understand and, if necessary, discipline private life. Indeed, in its purest form, private life is itself the construction of such power, deliberately engineered through brands and television images, for the most effective distribution of externally given ideas.

For ordinary people who follow these ideas, this tradition can best be described as fatalism. While perhaps its purest and most nihilistic form may be found in some of the writings of Michel Foucault, many writers in this tradition exhibit an uneasy alliance of liberalism, civic republicanism and fatalism (Orwell’s later work). Like other forms of fatalism, this tradition is of little use to policy makers and activists but it is a temptation to which many people can occasionally succumb in the face of the power of modern data gathering systems.
If the liberal tradition has historically proved itself best able to make sense of the procedural character of some of these claims for protection against certain types of risk, it is perhaps the civic republican tradition that is best able to make sense of their focus on human dignity rather than on justice when each offers an explanation of what is valued in the idea of control over the sphere of personal information collected and used by others about oneself.

While liberalism has sought a monopoly on the articulation of concerns of justice, justice is but one part of fairness, and each of the three main active cultures embodies and articulates a distinct conception of what is fair. While liberals may reduce it to considerations of liberty and justice, and egalitarians see fairness as a collective and distributive matter, civic republicans see fairness as a matter of the degree of civic obligation that one's position requires.

Civic republicans, liberals and even egalitarians value something different in private life: choice, consumption and eccentricity for liberals; family, formation and citizen making for civic republicans; shared, open, politically equal life free from the commodifications of the market for moderate egalitarians. However, those who are not wholly and consistently fatalistic about privacy often agree on certain risks and certain demands for protection, even if they disagree about the goals they pursue with these risk perceptions and claims for protection. We can conveniently describe those measures on which non-fatalists agree as 'robust' by saying that they make reasonable sense across each of the traditions. Nevertheless, even within the group of risks that all the main traditions, at least in the moderate forms, agree upon, there are differences of emphasis. Liberals tend, as we shall see, to stress risks that affect justice and liberty and to be concerned with procedural questions. Civic republicans tend to place their emphasis on risks that endanger dignity and on substantive questions.

It should be clear from this way of classifying the traditions that no simple 'left' and 'right' classification could ever have properly represented our cultural attitudes to privacy and private life. On the subject of privacy, there are civic republicans of the left and right, with their typically contrasting views on state and market power; liberals who
see it as a sphere of liberty and take quite contradictory positions on the classic left-right debates about the trade-offs between economic and political liberty; and egalitarians of ‘the personal is political’ viewpoint who are enthusiastic about state power as a source of protection and others who are deeply anxious about it as a threat. Perhaps some people still imagine that any debate of real importance in politics can either be described in left-right terms (for instance, proportion of gross domestic product that should go through public expenditure) or else will prove extremely disruptive for a nation (for example, divisions in the UK over membership of the single European currency). This book will argue that privacy comes into quite a different category – of issues of great but diffuse importance which cannot be fitted onto a left-right spectrum but which will not prove utterly intractable.

Perhaps the best way to understand the relationship of these traditions to one another is to conceive of the intellectual and cultural space they occupy as capable of being mapped on two fundamental dimensions. No human society can sustain itself without operating some clear settlement between the conflicting impulses that the poles on each axis represent. The first dimension is that which places a tradition according to the way in which it sees social relationships. At one extreme, a culture sees relations as (at least ideally) voluntarily entered into – contracts, transactions, membership of associations, and the like. At the other, it sees social relationships as essentially given, inherited, ascribed matters such as stock social identities and roles, relationships to family or the state in which one was born and from which one cannot (in the ordinary way of things) opt out. The second dimension is the extent to which the tradition considers that individual or family autonomy should (at least ideally) be held accountable to some public, collective or social unit or whole – fellow movement members, fellow citizens, even future generations. (Of course, it is possible to believe that basic social relations ought to be voluntary, but are not – as Rousseau lamented, ‘Man is born free but is everywhere in chains’. However, someone with a cultural bias for believing that something ought to be the case will often find that this perspective colours their entire world view, including that which is the case.)
If we divide this space into segments representing the zones where models of voluntary and involuntary conceptions of social relations and relatively accountable and unaccountable conceptions of individual autonomy dominate, then each of the four traditions that I have described falls clearly within a separate quadrant in Figure 4. Civic republicans see social relations as subjected to discipline, but do not necessarily insist on the accountability to the group, while egalitarians take both views. Liberals take a voluntarist view of human relations and see individuals as free to truck and barter with their privacy without the need to account. Fatalists on the other hand see life as dominated by involuntary social facts, yet feel no moral authority behind the brute fact of their accountability.

**Figure 4** Situating the privacy traditions
However, there are some hybrid forms shown in the figure. Such hybrids or coalitions are not usually stable over longer periods, for instance, privacy social movement activists with a ‘privacy fundamentalist’ slant. The privacy unconcerned are essentially liberal pragmatists who will sell their privacy cheaply, while conventional authoritarian law enforcement views occupy the opposite extreme. One of the pleasing ironies of the figure is that it clearly illustrates the way in which diagonal opposites often understand one another authoritarian civic republicans would be happy governing a society of the privacy unconcerned, just as radical egalitarians often turn fatalist about privacy.

Moreover, the figure shows that we can place, at least roughly, the ideas of particular thinkers, writers, movements and politics about privacy within the matrix, showing their relationships to the four principal traditions.

Those familiar with cultural theory will recognise Figure 4 as a variant of the ‘grid-group’ classification of cultures developed by anthropologist Mary Douglas and political scientist Aaron Wildavsky. Grid is the dimension of social order by rule and role, while group is the dimension of commitment to individual autonomy or collective group life. Cross-tabulating the two and distinguishing high and low segments on each dimension yields the matrix presented in Figure 5. The four ways of life or cultural biases thus identified are, cultural theory argues, the principal stable forms held together by mutual repulsion and mutual dependence in ever shifting realignments and reconfigurations.

Civic republicans and egalitarians both think of privacy as a ‘sphere’ or distinct field of social life. The difference between them is that the former value it and the latter regard it with suspicion, but they share a common conception of the private as a form or way of social life. The low group cultures of fatalism and liberalism, however, see privacy as a series of disjointed facts, issues, places, properties or experiences. The two low grid cultures disagree over whether it is possible for individuals to secure any control over access to these discrete phenomena. In particular, the disagreements between civic republicans and egalitarians
centre on different valuations of traditional family life as the sphere of private life. Fatalists and egalitarians (on the negative or ‘dissenting’ diagonal) share a view of private life as a struggle over public accountability for random private experiences, while liberals and civic republicans (on the ‘power’ diagonal) share a view of private life as something to be managed. Therefore, the differences between the traditions boil down to their fundamentally different conceptions of private life, as illustrated in Figure 6.

Drawing on the work of Douglas on such classifications, we can see more clearly how some processes of change in political culture of privacy might work. I began by stressing the particular salience of the civic republican and liberal traditions. Cultural theory predicts that
this is what would be expected, because these traditions, on this diagonal, articulate currents of sensibility that enable the organisation of power while fatalism and egalitarianism, on the other diagonal, are less salient because they are essentially reactive and dissenting cultures, less able to articulate sensibilities that make for sustained social power.\textsuperscript{66}

The key point here is these are not merely intellectual traditions, but ways of life, which are implicit in the ways in which ordinary people live their lives and think about their private life. The intellectual traditions both articulate and influence ordinary life. In short, these traditions reflect mundane cultures. This point is central to the argument of the book, as it explores privacy and private life in the setting of cultural dynamics. Part three sets out the understanding of cultures on which the specific argument about privacy and private life will rest.

More importantly, for all the tensions and incompatibilities between these cultural traditions, cultural theory suggests that, over
the longer term, there will be in any society some people who will, on any major issue or social problem, appear in each quadrant of the matrix. Certainly, no society, the theory argues, that comprises people with only one or two of these cultures is sustainable. Any attempt at permanent domination by any one of them is likely to fail, although settlements on the positive diagonal will be more likely to sustain themselves for longer periods, given a fair economic and institutional wind. In particular, purely egalitarian projects have proven unsustainable over the long run, except in very closed social systems – usually religious and denominational in character – which are extraordinarily flexible to changing conditions in the wider society.

The theory therefore suggests that sustainable projects require temporary settlements between people with different cultural outlooks, and continuing institutional dialogue between the traditions – or at least between civic republicanism, egalitarianism and liberalism, since fatalism generally proves to be a wholly reactive and institutionally uncreative tradition.67

One merit of thinking in these terms which may be immediately apparent is that it helps to understand just what cultural problems there are in organising social movements around privacy. Revealingly, many privacy activists exhibit an unsteady compromise between the despairing style of the fatalist when they rail against the rise of technologies of surveillance, the egalitarian’s conceptions of social movement organisation and the demand for protection of rights of the radical political liberal.68 The mismatch between the organising style of a social movement and the content of its particular claim is a serious tension and one that typically makes it harder for activists to use resources of cultural identity to overcome problems of collective action.69 Thus privacy movements may sustain themselves for the duration of a campaign around an identity card proposal or a census but find it hard to institutionalise themselves in the way that interest groups, whose ideology and organising style are aligned in, say, hierarchy, such as farmers or doctors, can. For coalitions along the diagonals are much more likely to remain stable for a period than are alliances along the horizontal of the diagram.
In the next section, I discuss some of the recent history of this dialogue.

The triumph of liberalism

In Britain and North America, we know something about the distribution of the public across this classification. Volume 2 provides the detail. In general, we find that – depending on the questions asked and the measures used – no more than 15 per cent subscribe to views that can be called ‘privacy fundamentalist’. About the same or fewer claim to be unconcerned (although in practice many of these turn out to be fatalists). The majority are privacy pragmatists. Privacy pragmatists, willing to trade personal information for other benefits, exhibit the liberal conception of privacy as a counter to be traded. This domination reflects the more general triumph of liberal ideas. However, these standard categories developed in the course of empirical work on privacy attitudes are – Figures 4 and 6 suggest – not necessarily the only ones that matter. As histories of privacy and private life show, cultures of expectation and commitment can change, even rather quickly in later modernity. It is therefore worth exploring just how and why the liberal tradition came to triumph over the others, in order to understand some of the dynamics of political culture that could, in future, bring other traditions in new forms, once again to the fore.

It is now a matter of historical consensus that the civic republican tradition was eclipsed by the liberal tradition during the nineteenth century in much of Western Europe and North America. The reasons for this are complex, often specific to conditions in particular countries and well documented. We can distinguish several kinds of forces – political, familial, organisational and governmental.

In societies such as England, France and the USA, the civic republican tradition and, with it, its specific conception of the role of private life, died slowly and hard. The history of bourgeois family life in all three societies in the nineteenth century shows that the liberal conception could not define family and household manners until the twentieth century. Nevertheless, the intimate link between the nuclearisation
of the industrial family and the political articulation of bourgeois and middle class aspirations through liberalism gradually narrowed the space for a more dignity-centred conception of private life and privacy. Nevertheless, the revolt of young men against paternal authority ran through the late eighteenth and nineteenth century and became such a standard trope in literature was naturally expressed in languages of privacy that stressed a liberty-centred conception of privacy in family relationships, rather than the ascribed fiduciary duty of loyalty that informed civic republican thought about the family.

Moreover, the rise of the joint stock company, the modern charity and the new incorporated forms of public organisation in the great period of innovation in organisational form in nineteenth century was a process of which the liberal tradition seemed, at least at the time, to provide a better account than the civic republican one. For the instrumental character of the company, the charity, the local authority, the cooperative seemed, to a culture imbued with utilitarian ideas, quite different in character from the relatively non-instrumental nature of family relationships and friendship. The transfer of the moral language of a fiduciary relationship from ascribed and intimate relationships to a realm of financial transactions seemed, to the nineteenth century mind, inappropriate. Indeed, only in the late twentieth century has the law of contract become imbued by judges with implied fiduciary relationships of privacy and loyalty (for example, by implying duties of care or duties to disclose possible conflicts of interest or even duties to disclose personal information about clients to third parties into contracts) and even now this is the subject of vigorous contestation in liberal thought.71

Finally, the liberal tradition seemed to offer a clearer guide to the moral and political principles by which citizens should engage with the state in the period of its greatest expansion in surveillance capacity. For the rise of systematic surveillance has been the most important enhancement of the capacity of the state and business organisations to make decisions about individuals and in some measure to exercise control over them in the allocation of entitlements, privileges and risks. Liberalism was able to express well not only the restlessness and
resistance of individuals to that control but also latterly the claim of business organisations to the economic liberty of the right to engage in large scale data collections about individuals. Liberalism therefore provided a language, albeit one with internal tensions, in which these struggles could be described as ones of conflicting claims to liberty and justice.

**The fracturing of liberalism**

However, as cultural theory would lead us to expect, excessive reliance on any single cultural bias has had the effect of undermining the viability of the way of life that cultural bias fosters. And so it has been with liberalism. To be sure, liberalism’s triumph has been a contingent affair, in which it has come to dominate but never wholly to supplant the commitment to order and civility that civic republicanism engenders, the social solidarit that egalitarians traditions can furnish nor even the necessary scepticism that a moderate dose of fatalism can afford to a society. Had it done so. Western societies would have collapsed as surely as did the overly egalitarian Second World of communism or some overly individualist societies studied by anthropologists.

The fate that liberalism has suffered has been that it has fractured, some say irretrievably, into distinct political and economic forms. Political liberalism, with its commitment to individual rights buttressed with constitutional and juridical protection and its conception of orderly political competition that tames faction into manageable interest groups, seems – at least to economic liberals – to be well on the way to civic republicanism.72 Indeed, we can see John Stuart Mill as the fount of modern political liberalism, seeking to protect from public regulation a sphere of private conduct, grounded wholly in principles of liberty to the point where it is hardly a distinct value from that of freedom.73

Economic liberalism celebrates deregulated markets, entrepreneurship, individual responsibility, risktaking and the most minimal role for the law consistent with the existence of a system of exchangeable property rights. To political liberals this seems to leave the way clear
for private hierarchies to emerge: these will crush individualism, leaving the devastated cultural plains of fatalism at least as readily as traditional hierarchical conceptions of society offered by more collectivist civic republicans.\textsuperscript{74} Today, the emergence of political liberalism represents an important complicating factor in the grid-group schema. For it represents a key and relatively durable alliance on the part of liberal individualism with moderate forms of egalitarianism and civic republicanism.

Political liberalism has taken up the cause of an individualistic version of the human rights case about privacy and pitched the case as much against business as against executive and regulatory government. It has been relatively successful at least in Europe in making the case for regulatory capacity to enforce individuals’ claims for control over personal information. Meanwhile, economic liberalism has grown suspicious of the expansion of the claims of human rights in a great many directions, not only in connection with welfare rights,\textsuperscript{75} but also in respect of economic regulation, including data protection. In short, the impulse of political liberalism has moved closer to the civic republican conception of a protected sphere of private life and also towards the egalitarian idea of enforceable rights for those informationally disadvantaged by government and business.

For all its earlier roots, this fracturing of political and economic liberalism was cemented in the post-war era when Hayek and Popper’s ideas confronted the rising alliance of egalitarianism with a political liberalism that led to the many international conventions and constitutions that sought to buttress richer and more expensive conceptions of individual rights against taxpayers than the ones economic liberals believed were compatible with liberty. This rise and fracture of liberalism serves better to explain the rise to prominence in the post-war period of privacy concerns than any of the theories canvassed in Chapter 1.

Meanwhile, in the 1980s when economic neo-liberals had perhaps more influence over governments than they do today, the economic liberal case was pitched mainly at much larger targets. The undercurrent of principled dislike of data protection, alongside anti-trust law and a
variety of other forms of regulation of business activity has continued and can be heard in some business circles in discussions of the implementation of the 1995 European Directive on data protection.

In some large part, the modern debate about the future of privacy is now a product of this fracture. The model of private life that political liberalism has installed, economic liberalism now proposes to remove, leaving us to wonder whether there are other conceptions of private life and privacy that are viable in the age of informational capitalism.

The continuing tension

Indeed, the liberal conception of privacy and private life has not been completely dominant and, at times, it has struggled to make sense of the experience of private life in modern times. The impulse has not abated among most people for the protection of private dignity against the disclosure of personal information in situations where liberty and justice are not principally at risk.

Concern about press intrusion, for example, remains – as recent revisions to the UK Press Complaints Commission code show – rooted firmly in worries about loss of dignity. Rising demands for data protection, even within the United States (which has so long resisted any general legislation at federal level) is often a response to a perception of risks to dignity as much to risks to liberty or of injustice. It is interesting that the often more impassioned debate about press privacy has been addressed to a more substantive conception of the specific kinds of behaviour deemed to be deserving of protection in the name of privacy, yet this is fundamentally concerned with dignity rather than liberty. Meanwhile, the less salient and often apparently more technical debate about data protection has been concerned principally with procedural issues about how personal data may be handled and the circumstances under which certain kinds of disclosures may be permitted, without making great efforts to define the nature of the private. This more neutral, procedural conception of privacy has a more natural home in the liberal tradition. In practice, of course, this perception of data protection as procedural is not wholly accurate, for
the fair obtaining and processing rule (see Chapter 10) provides a basis for privacy regulation to examine the substantive intentions of someone using personal information.

Both left and right have reasserted classical civic conceptions of the family as an arena of obligation and virtue and, within business, trust, long term relationships and fiduciary duties of loyalty are now given more emphasis than ever before. Indeed, in contemporary political thought, there is now a high profile stand-off between a resurgent civic republican tradition, often allied to some species of communitarianism and liberalism.

The very fact that neither the liberal nor the civic republican sensibilities alone cannot make sense of all the values shaping private life in modernity suggests that any satisfactory account of what, in modernity, we value in privacy must encompass both, while recognising the inescapable tension between them and the fact that no settlement can be permanent. Only with such a model can we expect to think coherently about the likely futures for private life and the demands for institutionalisation of the means of its protection against various kinds of risks.

Finally, it should be clear from this analysis that no study of the concept of privacy will yield answers to the questions of just which kinds of claims to privacy (if any) can be justified and which kinds of behaviour (if any) conducted in private, however morally reprehensible or culturally disapproved of, should nevertheless remain beyond the scope of social or public or political scrutiny. The challenge for ethical enquiry and policy making – and therefore for the third and fourth parts of this study – is to consider whether the idea of cultural viability will lead us in a direction which affords practical recommendations for coping with and legislating for privacy.
Notes for Part 1


7. This view of agrarian societies is a long standing one in social thought, going back at least to Tönnies, certainly to the romantics and perhaps as far back as antiquity.


11. The 1974 Privacy Act is federal legislation but relates only to government. There are specific pieces of legislation concerning medical records and personal video loan data and, recently, the Federal Trade Commission has hinted that it is willing in principle to use its powers to prosecute as unfair and deceptive trade practices certain categories of privacy violation. However, ‘full frontal’ attempts to get comprehensive federal privacy legislation affecting the business through Congress and the White House have always failed.


31. This is the way in which it is treated in some law tests, for example, Foster C, Wynn T and Ainley N, 1996, *Disclosure and confidentiality: a practitioner's guide*, FT Law and Tax, London.


52. For example, Scruton R, 1980, The meaning of conservatism, Penguin, Harmondsworth, says 'in order to maintain and assert its power, the state must concern itself first not with private but with public things. It is within the public world as the nation state determines it that the consolations of privacy must be sought ... But what does [the right of privacy] amount to when unprotected by the state? Nothing … This Anglosaxon privacy which we esteem is in fact nothing more than the public order, seen from within.' [my emphasis]. In the context of a book devoted to arguing the limits of liberty and the duties of citizens while emphasising the importance of cultivating virtues, this last statement encapsulates crisply and powerfully how much of modern conservative thought on private life owes to civic republican ideas.


54. One of the leading advocates of this view in modern times was Hannah Arendt, who argued that the private sphere needs to be distinguished
carefully from the encroaching development of the social or the public, for whom the private sphere is indeed the place in which the virtue of citizenship are learned, and for whom one key element in the essence of totalitarianism is the erosion of the private sphere as part of a strategy for the corruption of citizenship: Arendt H, 1958, *The human condition*, University of Chicago Press, Chicago. For a discussion of Arendt’s conception of private life, see Boling P, 1996, *Privacy and the politics of the intimate life*, Cornell University Press, Ithaca, New York, ch. 3. Boling’s gloss on Arendt’s view is as follows: ‘Private life is a place to recoup one’s forces so that one can go back to the active and draining participation of a citizen in public life.’


60. This has long been an argument put by gay and lesbian movements about such ‘quarantine’ restrictions on the abolition of the criminalisation of anal sex, where it takes place ‘between consenting adults in private’. See for example, Boling P, 1996, *Privacy and the politics of the intimate life*, Cornell University Press, Ithaca, New York, 104–5.

61. Robustness concepts originate in the world of operations research and the analysis of decision making and strategy and especially scenario building, where they are used as measures of the extent to which strategies are rational under various alternative scenarios: see Rosenhead J, 1989, ‘Robustness analysis: keeping your options open’ and ‘Robustness to the first degree’ in Rosenhead J, ed, *Rational analysis for a problematic world: problem structuring methods for complexity, uncertainty and conflict*, Wiley, London. More recently, they have been used in conjunction with scenario building using the grid-group matrix of cultural theory, of which previous chapters have offered an adaptation: Thompson M, 1997, ‘Cultural theory and integrated assessment’, *Environmental Modelling and*
Assessment, 2, 139–150. It is this approach that will be followed here.

62. For example, I have argued in the notes above that Habermas on the quasi-liberal left and Scruton on the authoritarian conservative right share a common tradition in their conception of private life.


74. It was this tension between economic and political liberalism that preoccupied me in two of 6 P and Randon A, 1995, Liberty, charity and politics: nonprofit law and freedom of speech, Dartmouth Publishing, Aldershot.


Part 2
Drivers of change
In the next few years, the prospects for individual privacy could be transformed completely. Conventionally summed up in the phase ‘the information society’, forces in business, technology and the changing nature of government are making the ownership, control and use of personal information – as well as other kinds of information – more important than in any previous stage in human history. The volume of information processing, the networks through which information flows, the power that it enables some organisations to assemble and wield, the transformation of work and the lack of work that these trends have wrought are widely held to be key characteristics of a distinctive form of near global political economy that has emerged since the 1970s. This part will argue that the scale of corporate and governmental collection and manipulation of personal data – and not just computerisation or a general shift towards information processing of all kinds – is the defining characteristic of a developed information society today. However, for all its epochal importance, it does not follow that the technology or economics of informational capitalism will determine the future of privacy. Both allow space for several possible future developments.

These changes may deepen the risks of violations of privacy. But they may also bring new means of securing and enforcing privacy. If this view is accepted, then it seems reasonable to expect that the maturing of this new political economy will have impacts upon privacy as powerful as its infancy did.
The future of privacy

The purpose of this part of the book is briefly to describe and explore the likely impacts of the principal forces that are likely to reshape the meaning of privacy in the next phase of the information age; to explore the changing balance of privacy risks, as classified in Part 1, presented in each area; and also to explore the meaning of some of the key trends for the balance of the four privacy cultures set out in Part 1.

In this part, I describe the main drivers of change. Chapter 6 addresses changes in people's understanding, cultures and values that influence their attitudes to privacy, the value they place upon it and the purposes for which they seek it. New data from a survey conducted in the course of this research programme is briefly presented, but more details are provided in the Volume 2.

Chapter 7 turns to the economic forces that put a premium on personal information in business and executive government and looks at the implications for the dynamics of business competition. The changing shape of privacy risks is explored in a number of the key industries of informational capitalism.

Chapter 8 deals with developments in information and communications technology and the treatment and processing of personal information.

Chapter 9 is devoted to the implications of the new trends in the role, organisation and culture of executive government as a user of personal information in managing public services for privacy.

In Chapter 10, the focus shifts from public services and technologies towards the regulatory role of government and the changing legal, economic and organisational capacity of government to regulate collections and flows of personal information. Problems of jurisdiction arising from ever greater transnational flows of information are discussed; the often bitterly fought debate about government control of the use by businesses and individuals of strong cryptography is reviewed. The findings are brought together in the conclusion.

Finally, Chapter 11 is devoted to the issues of privacy raised by the media and the conflict between freedom of the media and privacy claims.
This part is based on the triangulation of several research methods, but principally on reviews of academic, policy and ‘grey’ literature together with interviews conducted with business leaders, technology experts and public officials. However, the chapter on cultures and values also draws upon new survey data, which is reported in full in Volume 2.
Many of those who have thought about the future for privacy believe that information and communications technologies – and those who control them, invest in their development and use them – will largely determine the future of privacy, if there is one. On this view, a study of the future of privacy is essentially a study of the social consequences of technological change. In this part of the book, I will argue that what people think and want are at least as important. The choices of technologies that businesses seek to develop, the ones that the public chooses to use and the ones that regulators encourage and discourage are all reflections of wider culture. Of course, cultures are not independent of economic and technological forces but the simple view shared by many admirers and critics of informational capitalism – that cultures are simply the effects of economic and technological forces – cannot be sustained. For business strategies, perceptions by businesses and governments of acceptable economic and technological risks, definitions of property rights and the ways in which technologies are introduced and used, are all in turn influenced by attitudes to the use of information among the public. The chapter uses the ideas of a stratum of culture called ‘culture of the material environment’, which comprises a much richer repertoire of values, sensibilities and commitments than simple ‘attitudes to technologies’.
Cultures and values
While this is not the place to review the vast literature on rival definitions of culture (Part 3 provides an overview of the understanding of the concept of culture with which this book works), it is useful to explain the range of issues dealt with in this chapter. The culture of the material environment, as I use the term here, is concerned with the physical artefacts of houses, tools, everyday objects and taste in their design and decoration. More cognitive levels of culture are occupied by symbols, norms, rules, habits, accepted and acceptable behaviours, rituals of everyday life and the like. These things are represented in myths, narratives, values, attitudes, perceptions of risk and danger (including risks to privacy), standards of excellence in culture of the material environment (‘high culture’) and social behaviour, and even ideologies and world views, such as the four traditions about private life and privacy identified in Part 1. Finally, all levels of culture are expressed and organised in particular social networks.

In this chapter, I begin with some aspects of culture of the material environment concerned with the physical separation or linkage of home and work, before moving on to more cognitive levels of culture. I conclude with a brief examination of what is known about trends affecting the relative influence of the four major cultural traditions of privacy identified earlier – civic republicanism, egalitarianism, liberalism and fatalism.

Cultures of private space: home and work
A room of one’s own, as Virginia Woolf called it, was a novel experience and claim not only for women at the beginning of the twentieth century but for most people. The division of the home into separate living and working space may have taken place in the Renaissance for great princes and merchants but it was not until the nineteenth century that the middle class began to organise their home lives in this way. The physical separation of home and work for the mass of the population came in the nineteenth century with the advent of industrial employment and, in late industrialising countries of continental
Europe, not until the last decades of that century and even the first decades of the twentieth.5

The geographical sequestration of home from the outside world became, in the middle class culture of late nineteenth century, the basis of a conception of privacy as a claim for protection against physical intrusion and being observed in one’s private property. Certainly, this idea informed the development of the American torts of violation of privacy6 and it continues to be an important element of general debates about privacy.7 It is fundamental to the modern conception of privacy as the claim for a sphere of life in which the state’s apparatus of crime control does not routinely subject individuals against whom no reasonable suspicion has been established to surveillance.8 Moreover, it continues to inform our debates about the ethics of the press in intruding into privacy as much as it did at the end of the last century – witness the furore following the death of Diana, Princess of Wales in 1997, regarding the behaviour of paparazzi photographers and the editors who used their work, and the subsequent revisions to the Press Complaints Commission code of practice.9

In contemporary culture of the material environment, the home is the archetypal private space. Thus far, the privacy culture of the material environment may have followed the economics of personal property ownership. However, it quickly outran it. Gradually, middle class culture has come to value and even expect similar protection – even to some extent for ‘celebrities’ – against surveillance and interruption in a wide range of other physical places, from ‘secluded’ beaches and mountain tops to certain outdoor parts of cities, and even public buildings such as libraries and public offices, to privately owned places open to the public such as gymnasia. This extension has led to the Press Complaints Commission code abandoning all efforts to define geographically, physically or in terms of property rights just what places count as private and to fall back on the idea of that some places carry with them (in our culture of the material environment of place) a ‘reasonable expectation of privacy’, in the sense, presumably, that one may be viewed there but not photographed or recorded.
Whether there is such a shared common sense about the place or expectation of privacy remains to be seen, but there are reasons to suspect that there is not. One would expect, for example, people whose basic cultural bias differs according to the fourfold classification offered in Part 1 to have quite different intuitions about what is a reasonable expectation. While liberals might look first to the property rights of the site, civic republicans would be more inclined to give weight to the particular purposes of the alleged violator and the extent to which they are proper and lawful purposes for the common good of the citizenry. Fatalists would not expect that property rights or media law would effectively protect any private sphere to which they might ideally aspire.

In the age of informational capitalism, the relationship between home and work is changing once again and this may put under renewed strain any settlement of what a ‘reasonable expectation of privacy’ might be that pertains to the particularities of place. The industrial age construction of home as the place that was free from the culture of the material environment of the workplace has been steadily eroded.

The advent of the telephone, the radio, later the television and more recently the modem have steadily brought more communications into the home and undermined the idea of home as a haven from the communication intensive world of work and public living. This could be still further eroded if there proves to be widespread demand for the kinds of technology that would make up the ‘smart home’ – in which embedded computers will communicate from the refrigerator to the car’s routing and navigation system so that, when passing a supermarket, the driver should be aware that supplies of milk are running low, which will control the switching on and off of lights and perhaps also control the ordering of home deliveries and the making of payments in the same way.\(^\text{10}\)

The growing proportion of the population who are elderly and with restricted mobility means that more face-to-face services such as social care, shopping and personal services like hairdressing are being delivered directly into the home, making home a less private space.
Since the early 1980s the lengthening of working hours for many of those of working age means that the demand for cleaning services in their homes from two earner households which are much lower down the income scale has increased for the first time in almost a century since domestic service went into decline.\(^{11}\)

Many more office workers can now work from home at least part-time than would ever have been possible in the age when office discipline depended on the kind of factory floor-type surveillance by managers of the typing pool. Rates of self-employment in the form of home working are rising, not only for office workers but also for a range of other activities: the ‘putting out system’ will not supplant factory based production, but will continue to occupy a secure niche in the economy of home and work. For these workers, homes are increasingly being designed or used in ways that must accommodate extended periods of work from home. Opera singers, lorry and taxi drivers, table waiting staff and oil drilling teams will always go out to work, but a substantial proportion of the workforce will use home as a semi-public place of work, increasingly using automated communication with the outside world and receiving services delivered directly.

It does not follow that home will cease to be associated with the value of privacy; still less that privacy will itself go into decline, as some commentators seem to imagine (‘Privacy is history – get over it’\(^{12}\)) – some gloomily (‘Britain is witnessing its last few years as a free society’\(^{13}\)), some more cheerily (‘[People on the net] will no longer feel uncomfortable being on display, since everyone around them is on display too’\(^{14}\)). The error in this view is the reduction of culture of the material environment simply to a question of the rate of adaptation or resistance in popular values and attitudes to the irresistible and independently determined march of information technology. Culture of the material environment is a far more complex matter. Where economic and technological change creates opportunities, expectations do not simply follow (although there are special cases where they do). Expectations and aspirations for privacy associated with the culture of the material environment in the home, however saturated with
information the home becomes, are embedded in the wider cultures of norms, symbols, myths, world views and social networks.

Knowledge and understanding

Perhaps the most fundamental cultural force is the way that people interpret their environment and the risks its present. Risks that remain poorly understood, or not seen as risks will, by definition, not show up as being either acceptable or unacceptable. New technologies that are adopted for efficiency of information processing can often disguise the volume of personal information processed and render opaque to citizens and consumers just what use is made of information about them. This is one of the most important encounters between technological development and culture of the material environment. For example, in our qualitative work it became clear that most participants initially had only a hazy idea of the detail in which their transactions with major retailers are collected and analysed when they join a loyalty card scheme.

Perhaps a more worrying example of complacency founded in ignorance is the widespread assumption that because of the confidentiality rule adopted by medical practitioners, patients' medical records are kept securely and that administrative staff in GP surgeries and hospitals, government officials handling payments within the National Health Service and others will always respect the privacy of medical data. In fact, manual medical records are alarmingly easy for the unscrupulous to acquire by simple bribery. Experts in medical data security remain deeply concerned about security for the NHS computer network NHS Net and about the increasing tendency of the NHS authorities to demand that payment systems should use the actual names of individual patients to track and identify costs and expenditures. Other problems of insecurity and lack of privacy in the system include the vulnerability of many of the smart card systems proposed or in use, both to physical tampering to retrieve data and to decryption using brute force.¹⁵

However, complacency is only one possible response to lack of understanding. There are also cases in which people may exaggerate
the risks to their privacy. For example, many people are extremely wary of providing their credit card details over the Internet in order to make a purchase, fearing interception and fraud. In practice, anyone sophisticated enough to intercept and decode a single e-mail message in order to extract and use a single credit card number is almost certainly a sufficiently sophisticated hacker to adopt the more efficient method of effecting unauthorised entry into the central database of a major bank and helping themselves to much larger numbers of credit card numbers and details. So far, there has been no case of criminal interception of a credit card number during the passage of a message across the Internet. Moreover, the vast bulk of individual credit card fraud takes place face to face when a credit card is handed over for payment in shops and restaurants or in muggings. The effect of this exaggerated perception of risk to privacy is to slow the rate of growth of electronic shopping.

Cultures of expectations about privacy grow up around the use of certain information technologies, which can be overturned in sudden shocks. For example, many Internet users were shocked to find that there are companies which analyse all postings to Usenet groups, record all postings by individuals and build up detailed profiles of everything that they said about themselves. Although Usenet group users know full well that there are many people who read their messages but never post any of their own (known as ‘lurkers’), the culture of expectations has grown up among many people that they are holding a small group conversation in private. This contrasts sharply with the culture of expectations about the insecurity of email to a single addressee containing a credit card number.

The aggregate effect of misplaced complacency and alarm is to encourage the development of a widespread but diffuse culture of fatalism about privacy risks. In our qualitative work, supported by a review of surveys of attitudes to privacy issues, we found a generalised belief that many organisations can, if they wish to, acquire personal information of almost any kind and that they often disclose it without consent. In such a climate, trust is fragile and efforts to manage one’s privacy risks and to develop information ethics for business and government remain impoverished.
The challenge, then, is to enable more effective learning throughout life about privacy risks and strategies for coping with them – an issue dealt with in Part 4 of this volume.

**Perception of privacy risks**

We have few specific data on the questions of who worries about which privacy risks and why, and we have still less on how the pattern has changed over time. Most of the data we have – including the new data to be presented below – is concerned with trust, confidence or the dampening of worry and risk perception. This means that we have few general rankings by the public of the seriousness of the harms caused by different kinds of violations of privacy by comparison with other kinds of risk, nor clear estimates of relative probability or unacceptability.

Data of these kinds have been collected in the psychometric tradition on perceptions of risks, where the harms that respondents are asked to consider are fatality, injury or sickness, and where the usual and overly simple dimensions of analysis are questions about whether a risk is dreaded and whether it is known. Even in those fields, it is not clear that trends over time can be clearly discerned from the existing evidence. In the cultural theoretical tradition, a number of cross-sectional studies have been conducted on perceptions of a slightly wider range of risks, but none has examined privacy risks.

There is some evidence for rising general concern about the levels of collection of personal information. In at least some contexts (such as personal data held in association with benefit claims), people appear very concerned about disclosures to third parties in many and perhaps most situations. One survey found that a bare majority regarded it as a necessary evil that they should give personal information to companies, although younger people were less likely to accept this. The same study also found that younger people were more likely to be concerned about the implications of personal data processing by companies for the way in which they would be treated, while older people worried more about the quantity of the information and being ‘pigeon-holed.’ Roughly similarly sizeable minorities worry more about some parts of
government and about the private sector, but this does not explain much: there are wide variations within both sectors between trusted and untrusted organisations. Attitudes such as willingness to provide information and contentment with disclosure vary with the type of organisation, the purpose of the transaction and the nature of the information asked for or collected.

In general, the principal surveys on privacy suggest that as people age, they grow less trusting in companies’ and government’s handling of personal information. Younger, more affluent people, generally more consumeristic and individualistic in their outlook, seem more confident in their ability to manage their personal information to reduce their exposure to risk and to seek redress for violations. Majorities are aware of the existence of some kind of legislative protection and would, in principle, like to see it strengthened, but many are sceptical of its value and enforceability.

It is at least possible – and if true, it would be important – that the difference observed in the privacy survey data between older and young people’s risk perceptions may reflect a change over time, through generational replacement if no other causal mechanism, from a culture dominated by fear of large scale data collection and dataveillance towards one which fears unjust inference and treatment of individuals on the basis of data collected but not data collection and manipulation itself.

While there have been some data from newspaper commissioned surveys on attitudes to press privacy intrusion, they must be taken with a heavy pinch of salt. In answer to survey questions, people are willing to denounce egregious intrusions even though they will nevertheless enjoy reading the disclosures that result from them. Certainly, they rarely stop buying a newspaper which commits such violations even against admired celebrities.

Public trust in the handlers of personal information

The public seems to be quite discriminating in its distinctions between different types of organisations trusted with personal information and several surveys have developed rankings. Direct marketing, mail order
and credit reference companies, car dealers, home shopping companies, cable television companies and magazines are widely distrusted, while banks and building societies are quite highly trusted, as are travel and leisure companies.24 Doctors are the most highly trusted. In the public sector, the police attract less trust than many other agencies.25 On the other hand, there is some evidence that, at least for certain kinds of organisations, the more people deal with them, the more they trust them. This could mean that they genuinely learn to respect them or simply that they persuade themselves to trust them, warts and all, because it is psychologically difficult both to have to deal with an agency and to place no faith in it. These patterns appear to have been stable for some years.

In a survey conducted in the course of the present research, we explored the reasons why people trust organisations with personal information (‘reasons’), and the things that they trust these bodies to do or abstain from doing (‘tasks’) with their personal information. Respondents chose the two or three reasons or tasks that weighed most with them from a list. Full details are reported in Volume 2.

Figure 7 gives the principal reasons for trust by type of organisation and Figure 8 the principal tasks in the same format.

**Figure 7  Reasons for trusting organisations with personal information (%)**

<table>
<thead>
<tr>
<th>Organisation</th>
<th>Local councils</th>
<th>Central government</th>
<th>Banks</th>
<th>Supermarkets</th>
<th>Phone companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Law requires</td>
<td>63</td>
<td>67</td>
<td>62</td>
<td>41</td>
<td>55</td>
</tr>
<tr>
<td>Damage to reputation</td>
<td>38</td>
<td>33</td>
<td>47</td>
<td>47</td>
<td>47</td>
</tr>
<tr>
<td>Written agreement</td>
<td>34</td>
<td>35</td>
<td>39</td>
<td>22</td>
<td>30</td>
</tr>
<tr>
<td>Public commitment</td>
<td>19</td>
<td>17</td>
<td>17</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>Reliable staff</td>
<td>17</td>
<td>20</td>
<td>26</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Don’t know of problems</td>
<td>15</td>
<td>10</td>
<td>9</td>
<td>15</td>
<td>13</td>
</tr>
<tr>
<td>British/local</td>
<td>5</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>None of these</td>
<td>7</td>
<td>7</td>
<td>5</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>Don’t know</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>10</td>
<td>6</td>
</tr>
</tbody>
</table>

When we read these data in the context of our qualitative results which suggest that most people have little confidence in the efficacy of the law, the fact that so many feel they can place great reliance on little else does suggest that public trust is more fragile than commonly thought. Supermarket loyalty card schemes do not, on the evidence of the numbers picking ‘none of the above’ for these organisations, seem to have secured universal public trust. Turning to the tasks, banks are trusted on security more than any other organisation is trusted for any other task, supermarkets again perform poorly, and central government emerges with a tarnished reputation for disclosure.

We used two additional questions asking people to rank the organisations in order of trust to carry out specific tasks of different kinds (using the information only for the purposes told, and not making
judgements that might be right or wrong). Averaging the responses, we found the same ranking of the organisations in each case. In order to understand these data better, we derived two categories: a ‘high ranking truster’, someone who consistently ranked a certain organisation either first or second in both questions, and a ‘low ranking truster’, someone who consistently ranked that organisation fourth or fifth in both questions. Figure 9 shows the proportions of the sample falling into these categories for each organisation type and the gap between the two categories as a coarse measure of the relative balance of trust. It is interesting to note that the two categories of public body do not come out worst, as some people expected.

**Trade-offs between privacy and other risks**

Between three fifths and three quarters of the population of most developed societies for which we have data claim to be ‘privacy pragmatists’. That is, they are willing, at least to some extent, to trade off the provision of personal information, and even the protection against certain privacy risks, in return for other benefits, or protection against other risks. About 10 or 12 per cent are ‘privacy fundamentalists’, generally unwilling to offer such information unless they are compelled to, and about another 10 or 15 per cent report themselves unconcerned

### Figure 9  Numbers of high and low ranking trusters, and the gap between them

<table>
<thead>
<tr>
<th>Organisation</th>
<th>High ranking trusters</th>
<th>Low ranking trusters</th>
<th>Difference (high ranking percentage minus low)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local councils</td>
<td>398(20%)</td>
<td>400(20%)</td>
<td>0%</td>
</tr>
<tr>
<td>Central government</td>
<td>661(33%)</td>
<td>361(18%)</td>
<td>15%</td>
</tr>
<tr>
<td>Banks</td>
<td>1075(53%)</td>
<td>206(10%)</td>
<td>43%</td>
</tr>
<tr>
<td>Supermarkets</td>
<td>277(14%)</td>
<td>812(40%)</td>
<td>-26%</td>
</tr>
<tr>
<td>Phone companies</td>
<td>519(26%)</td>
<td>661(33%)</td>
<td>-7%</td>
</tr>
</tbody>
</table>

with privacy. Relatively small numbers have no opinion at all. Qualitative research suggests, however, that the more they come to understand about the range of risks they face in their everyday lives, the more privacy pragmatists are concerned about privacy.

In the context of shopping, privacy pragmatists may be willing to provide at least some kinds of personal information in return for a more personalised service, for cash benefits or discounts and targeted relevant promotions. In other contexts, there seems to be a trend toward greater public willingness to accept surveillance and dataveillance where they believe that, in return, they can expect protection against risks they rank as more severe than the abrogations of privacy protection involved. So, for example, closed circuit television or video cameras in shopping centres, housing estates, streets, parts of offices and the like have been largely accepted in many parts of the country, with significant proportions of local populations reporting in surveys that they are content with these arrangements.

This trend seems to fall in line with the trend toward rising concern about law and order, detected in recent years in the British Social Attitudes Survey data. There have been increases in the proportions reporting themselves willing to see, in the case of a person without a criminal record who is the subject of a tip-off, police action in surveillance (majorities), detention and even (although still quite small minorities) telephone tapping and interception and opening of mail. Similarly, a growing majority seems content to support a national identity card scheme. Electronic tagging of convicted persons arouses surprisingly little protest. More alarming for liberals who consider that the erosion of the presumption of innocence is the start of a slippery slope that leads to widespread police violations of privacy, only a small majority still supports the idea that it is worse to convict an innocent person than to let a guilty person go free.

**Privacy and ideas of fairness in the distribution of risk**

Arguments for privacy have always been closely connected with, and often dependent upon, wider ethical debates. In particular, privacy has
become linked to the *distribution of risk* in relationships or transactions, where an individual might behave in ways that could harm the interests of the other party in such a relationship: this is known as ‘moral hazard’. In recent years, these debates have become more complex and are discussed extensively in the media, legislatures, science and technology circles and in business. Privacy claims have close links with ideas of:

- *obligation* and *duties of care* to others (for example, to provide at least some kinds of personal information about oneself to others in certain types of situation, such as disclosing some genetic information about oneself to relatives whose health plans might be affected by knowing it)
- *fairness* or *solidarity in the distribution of risk*, bearing the costs of responding to certain harms (for example, in arguments that personal information of certain types should not be created or known to certain kinds of individual or organisation – typically, employers and insurers – because of the ways they will use it, and perhaps be bound by other kinds of duties to the disadvantage of those individuals); that is to say, it is not easy to distinguish privacy issues from issues of unfair discrimination, and many campaign groups in these fields do in fact argue that there is no distinction between privacy violation and unfair discrimination
- the *minimising of certain catastrophic risks* (for example, in arguments that there are risks of undeserved outcomes so catastrophic for some individuals that their avoidance is imperative and justifies violations of privacy rights – and perhaps even injustice – in the making of inferences from that personal information).

There are urgent policy debates and concerns running through contemporary culture on risk of each of these kinds. I shall consider three cases raising different ethical and policy problems:

- the creation, ownership, and knowledge of *genetic information*
the institutions that surround the relationship between employer and potential employees at the point of recruitment

the principles that govern information yielding suspicion or about convictions for the sexual abuse of children, or paedophilia.

In general, egalitarians and some moderate civic republicans tend to take the view that these are privacy issues, while liberals and other civic republicans tend to deny that these issues have anything to do with privacy.

**Genetic information**

Some have argued that a right to self-determination and autonomy implies the right to veto the creation of, for example, genetic information about themselves, if they wish to do so – the so-called ‘right not to know’ is extended into a claim for a right that no one should know. However, others would argue that where a parent, for example, may carry a gene for a certain disease that their own children and grandchildren may carry, they are under a duty to find out – a ‘duty to know’ – whether they do indeed carry that gene, and inform their own adult children if they do, because that knowledge will be important in helping those adult children make decisions about having children of their own. Such a duty to know would presumably also imply a duty to disclose, at least to family members such as children who may also carry or be at risk of disease, in such circumstances.

The US Congress recently debated proposed legislation that would have limited the right of life and health care insurance companies to insist on the provision of certain kinds of genetic information as a precondition either for the granting of cover or the setting of a premium. Some 22 states already have such legislation and the American Civil Liberties Union campaigns actively for its adoption at federal level. The argument for a strong claim of privacy against the creation or retention of such data amounted, in effect, to a claim that the private insurance sector should be compelled, behind such a veil of ignorance,
to run partial risk pooling between its clients. Presumably, this meant that, without such an overriding consideration, insurers would be obliged – in the course of their duty to be actuarially fair or contractually fair to each proposer – to use that information to discriminate against people who are considered genetically highly likely to suffer from certain diseases or conditions. Naturally, concerned about moral hazard and concerned for the desire of many of their clients not to bear risks for others, insurers resisted such legislation.34

Liberals might reply to these egalitarian arguments that this is not a privacy issue at all, or that there is a privacy case here but it is overridden by other claims of contractual fairness, or else that privacy as dignity may be a relevant consideration but cannot of itself require such huge policy changes in distributive justice. Liberals consider that privacy claims cannot be sufficiently strong to mandate large scale private sector risk pooling in life and health insurance, even if that were to rule out the emergence of a genetic underclass of uninsurable people unable to secure mortgages or other benefits covered by life insurance. Nor, they argue, can privacy claims require social policy initiatives funded by taxpayers in some way to compensate such genetically unlucky persons.

However, other privacy issues are raised by genetic information in the insurance context. For there are also important risks of unjust inference, such as where conditional genetic statements may be mistakenly read as unconditional statements; where probabilities may be wrongly over-estimated; where the chances of avoiding the environmental triggers are estimated too low; or where genetic risks are wrongly overestimated for particular ‘racial’ groups. Genetic information is not, in principle, different from other kinds of medical information. Indeed, much of the ordinary information on any individual’s medical record is already genetic in character, inasmuch as it relates to facts about people who are genetically influenced or determined, although it may not be expressed formally in terms of the presence of particular genes or characteristics of chromosomes. For example, details of the cause of death of one’s grandparents and parents can provide important genetic information even though it does not take
the form of genomic strings and requires no tissue analysis to obtain it. Moreover, it is important to recognise that most genetic information does not take the form of simple ‘on/off’ statements about the presence or absence of genes ‘for’ single gene diseases, where the presence of the gene means a 100 per cent probability of contracting the disease (and even information that is of that kind does not tell one when in the life course most diseases like Huntington’s Chorea will be contracted). Most genetic information is multigenetic and takes the conditional form of expressing relationships between environmental triggers and ranges of probability of contracting certain conditions. Indeed, many genes ‘for’ certain diseases – in the sense that if the individual experiences certain things their chances of contracting the condition are increased – are also genes ‘for’ beneficial things such as memory, speech, agility or other things. In this sense, there remain insurable risks here rather than uninsurable certainties and it would be an unjust inference from the crude presence of certain genetic features in most complex multigenetic stochastic, environmentally triggered conditions to deny insurance or even to make it available only at prohibitively high premiums.

Taking these points seriously has led one advisory body to the British government to urge the industry that actuarially fair risk assessments using data from genetic tests often cannot, in the present state of knowledge, be made with any confidence.35 There have been reports from the USA of cases where incorrect inference has led to behaviours that seem unjust; for example, in one reported case, employers have insisted on a test for sickle cell trait, even though its relationship with sickle cell anaemia and actual illness is much less than that of a surefire predictor.

**Employers and recruitment**

Employers have long had the right, at the point of recruitment, to reduce their risk in hiring by making use of interviews, psychometric tests, medical examinations and references. In future, some employers may even require genetic information to be disclosed. However,
the tenor of the debate about how far employers may legitimately go in this has shifted recently.

Employers have long argued that they need to be protected at the point of recruitment against catastrophic risks, such as hiring individuals who may use their employment to further terrorism, industrial espionage for rivals, fraud, sabotage, sexual abuse of children, etc. Until relatively recently, organisations offering information about the political views and activities of individuals were sometimes used in Britain by employers checking out potential employees. However, they were often criticised for using unsubstantiated allegations, uncorroborated evidence, inaccurate and out-of-date information and for failing to distinguish between similarly named or addressed individuals.

Recent concerns about the probability that paedophiles are still in employment in child care services and the fact that only 5 per cent of paedophiles are ever convicted has led to new arguments being put forward by some directors of social services. They claim that the risks to children are so great that ‘soft evidence’ – that is, information about individuals from which inferences can be drawn but which does not have a high standard of proof – should suffice to justify decisions not to appoint or even to tip off other potential employers. For example, uncorroborated allegations of child abuse, and perhaps even being known to associate with known paedophiles are relatively soft data, because their accuracy is not known, or because they provide at best circumstantial evidence and at worst may describe behaviour that is wholly innocent.

There are, of course, problems in using information about employees to make inferences about the risks that employers face. Not everyone with a criminal record will re-offend; only a tiny proportion of those who commit crimes are ever convicted, so absence of a criminal record is a poor guide to risk. There are risks that unjust inferences will be drawn. Increasing sophistication at the point of recruitment will mean increasing intrusiveness. The only way in which individuals who do not wish to be subject to such profiling can evade it, is not to apply for jobs where employers operate these systems.

As many more individuals begin to carry smart cards – many of which will perhaps soon be multifunctional – from which detailed
databases are accessible, some employers may contemplate making it a routine part of recruitment procedures that they ask applicants for temporary use of their cards in order to undertake profiling and mining. Some employers may already conduct some data mining to construct profiles of applicants, without the applicants’ knowledge. Some privacy advocates argue that these sorts of data collection are unacceptable and violate the privacy of the employee. Moreover, they argue, if – which could be disputed – such methods do succeed in reducing the employer’s risks in hiring, such efficiency from the point of view of the employer may render some individuals wholly unemployable, creating inefficiency from the point of view of the society as a whole.

**Paedophilia**

The sexual abuse of children has become an issue of information ethics in other ways in the last few years. There have been publications listing names and addresses of convicted paedophiles in New Zealand, Australia and the UK. The justification for this ‘community disclosure’ has generally been that the scale of damage to children, the likelihood of re-offending and, at least in a minority of cases, the risks of ‘stranger danger’ are such that people have a right to know the whereabouts of paedophiles and to make judgements for themselves about how they wish to protect their children. Indeed, in one major British city, public housing managers who disclosed the address of, and information about, previous convictions about an individual to tenants anxious about ‘stranger danger’ to their children were dismissed. In a number of other authorities, housing managers have been put under great pressure to make judgements about requests for disclosure to tenants who believe that their children may be at risk. In such cases advice from police officers, social workers and other authorities may be contradictory, and the balance of privacy risks and risks to children may be very difficult to discern.

In each of these cases, then, privacy has become part of wider social policy debate about who should bear what risks in transactions where moral hazard is a possibility, and whether some trade-off
between efficiency from the organisational point of view should be sacrificed for some claimed wider social benefit.

**Privacy and ideological change: the shifting balance of the four key traditions**

How, then, are we to understand the broad direction of change in cultures of privacy? We have seen in developed societies over successive post-war generations a dramatic shift in attitudes away from attaching priority to basic physical, military and economic security and sustenance, towards attaching importance to matters of liberty, hedonism, and life fulfilment. Privacy can be, in its liberal and in some measure in its civic republican guise, a natural concomitant of these wider 'post-materialist' attitudes.

We can identify survey evidence for the existence of each of the four traditions. In terms of shopping, younger and more affluent people take a self-confident view of their own ability to manage the risks they face in transactions involving pressures to disclose personal information and appear to take a generally individualistic and liberal view of privacy as a store of value to be traded. In the context of law and order, for example, there appears to be a significant shift in the direction of the more authority centred and hierarchical values of the civic republican tradition. Nevertheless, despite these shifts, many people are confused and may use fatalistic attitudes, however shallowly held, to express this.

Evidence for a continuing egalitarian tradition about privacy is harder to find. Since the 1970s, egalitarianism of the kind that regards claims to private life with suspicion has been in general decline. The main social movements in which a suspicion of any claims of provisional accountability for individuals are still widely entertained are some of the more radical sections of the environmental movement, where personal green behaviour is expected as much as public action.

However, there are some signs in some of the social movements that have sprung up to protest against particular perceived privacy risks, such as national identity card schemes or privacy on the Internet, of a mix between the organisational style of classical egalitarian cultured...
social movements and the ideological content of a radical liberal outlook.

In recent decades privacy has rarely been central to any mainstream political party or ideology. It has generally been confined on the one hand to civil liberty pressure group politics and on the other to the bureaucratic politics of data regulation. Even the anti-collectivist upsurge in the late 1970s and early 1980s focused its energies on economic liberty and consumer sovereignty rather than on privacy. However, in the late 1980s and early 1990s there have been a steadily rising number of pressure group activists and high profile campaigns on issues of privacy, ranging from revolts against state identity card schemes in Australia, New Zealand and Britain to professional resistance to patient information management systems believed to endanger confidentiality in relations with clients among doctors.

Attitudes towards personal information processing and the distribution of risk in society may be moving slightly towards the civic republican position in such contexts as the effort to root out paedophilia. While there is widespread concern about the abuse of genetic information about individuals, it has not as yet become the subject of social movement activism on any scale in Britain, although it is more important in the USA where public health insurance is more limited. From most of the studies of younger people’s attitudes to the greater profiling and surveillance by employers, the prevailing view seems to be the liberal pragmatic one that they will accept it, provided that they are able to secure sufficient other benefits from the job.38

This picture of rising civic republicanism in crime related contexts but continuing tendency towards liberalism in more commercial contexts is better explained by the idea that the four traditions constitute, not fixed syndromes which structure and inform every encounter a person has with issues involving privacy and personal information, but a repertoire on which they will draw in different contexts and occasions, depending on the institutional pressures and perhaps on underlying general personal biases.39

It is not clear which one of two interpretations is the plausible one. One reading offers a picture of human nature and behaviour which is
not without problems, because it posits people who are consistent only within certain institutionally defined compartments called ‘contexts’. The ‘normal’ condition, considered across context, is, on this view, one of people as being chronically inconsistent. Presumably most people have the cognitive capacities to recognise, at least after the event, that their values are different in different settings, and to ask themselves why. This might be another case of limited rationality, like other cases identified in psychological research where the way in which substantively identical risks and opportunities are described leads people to make different decisions.40

The alternative reading is that people might be very sophisticated indeed and weigh up very carefully which of several options in their repertoire might be the most appropriate means of securing their utility function. However, this view seems a rather forced and heroic interpretation.

Moreover, each of these explanations seems plausible only when looking at the trends in the recent past. They make little sense of the much longer historical run, in which liberalism has eclipsed civic republicanism, leaving small enclaves of egalitarianism and a small number of outright fatalists about privacy but a diffuse scattering of some fatalist attitudes. Seen in this context, it seems to make more historical sense to propose a choice between two other readings.

In the first one, the trends toward a more civic republican and hierarchical bias in some contexts may be a short term eddy on the bigger and more steady stream to a trend towards more liberal cultures of privacy. In the second, liberalism and civic republicanism are reaching some kind of accommodation or coalition. This would not be wholly unexpected. Much of contemporary communitarian thought seeks just such an accommodation; such a goal is also sought by the British new Labour government and its counterparts elsewhere in the OECD, an in many theorists’ quest for a third way between social democracy and free market capitalism.41 Treaties across this diagonal are indeed much more likely, on theoretical grounds, to be stable and legitimate, than across that between fatalism and egalitarianism42 and have often been observed in the make up of mainstream centre-right politics.43
Conservatism, for example, reinvents itself afresh in every generation as a new kind of treaty between liberalism and civic republicanism, individualism and hierarchy, liberty and authority. In each generation, too, these treaties have come apart, but they have proven much more robust than coalitions between egalitarian movements of the articulate disaffected with the fatalistic and apathetic, which have been heavily subject to cyclical shifts of rising and dying away.\(^\text{44}\)

Whichever of these is the correct interpretation of the changing cultures of privacy, it will be important to trace its impact through the changing nature of geographically private and public space with which this chapter began. As the home ceases to be a haven or enclave and becomes more and more an open and communicating centre to which work, knowledge and disciplines are delivered automatically, both digitally and physically, throughout the life course, the traditional civic republican idea of privacy as a place of paedagogy for citizenship may be revived. Already, there have been plenty of calls for the revival of public space, but as a place where private activity can safely be undertaken – for which the public park is the best example.\(^\text{45}\) Many people report that what they value in the open spaces of parks is, paradoxically, the ability to be alone and behave as if in private, despite the fact that their security in doing so is guaranteed either by human surveillance from park keepers or wardens or else from technological surveillance in the form of closed circuit television.

Liberals, of course, have never needed to think of private property as something closed and defended, like the gated communities of Los Angeles. Yet it will involve a shift in the rhetoric and some well-entrenched styles of liberal culture to reach an accommodation with civic republicanism which accepts what some will see as an erosion of a culture of the privacy of private property.
7 The business of personal information

Informational capitalism is built on personal information, not computers

When commentators talk of the information society or the digital age, they are usually thinking too broadly or too narrowly. Too broadly, when the information society comes to stand for almost everything that is happening. Too narrowly, when information is thought of as the maturing and embedding of computing technologies, hardware and software in every aspect of work, organisational structure and culture, media power, city and regional economies, the arts, personal identity and life generally. Because financial services have been the field of greatest investment in information and communications technologies, the statistics on the flows of electronic investment on the global money, futures and stock markets have come to be used as the hallmark of the information society. Neither the technology nor the money flows capture how important to the new economy and the new model of government are the collection, manipulation, analysis and use in the targeting of services of personal information.

Increasingly, businesses are re-engineering to focus on efficient personal data handling and to design core competencies around identified behaviour of customers and potential customers. Organisations that once thought of themselves simply as trading in goods or services now think of themselves as also trading in information. For example, banks increasingly conceive of themselves as holding assets not only in
financial capital or investment skills and knowledge, but also in the
details about their account holders on the basis of which an individ-
ual’s or a company’s reputation can be constructed.

The basic relationship between the individual as consumer and cit-
izen with businesses and government is the holding of the individual
digital account. This records transactional behaviour with the organi-
sation itself or with third parties (as in the case of a bank account),
assets built up or liabilities incurred, problems brought (in the case of
any form of consultancy from medicine to law, counselling or employ-
ment advice), tastes and preferences, attitudes and contacts.

The personal account is not merely an efficient means of managing
files, but the basis of a political economy is geared to the individualisa-
tion of the provision of services and governance. In the public sector,
education and training are increasingly individualised as schools
move away from whole class approaches to teaching and introduce
individual home-school contract, and governments explore the idea of
the individual learning account for adult training. Individualised cal-
culation of entitlement to benefit is gradually replacing household
assessment. In pensions, it is widely expected that some form of per-
sonal second-tier pension may become compulsory in Britain as it has
in Chile, Singapore, Australia and elsewhere.54

While the computer has made the collation and maintenance of
accounts much easier, the fundamental difference that modern data-
base technology has made is that personal data on accounts are rou-
tinely and quickly compared, analysed, classified and searched. Accounts
of different kinds can swiftly be matched and compared. Data ware-
housing, matching, mining, manipulation, future projection using
modelling and forecasting techniques and data interpretation are now
the basis, not only of businesses that have long kept individual
accounts but of every kind of organisation. The expanding sectors of a
developed economy – financial services, direct marketing, call centre
work, every kind of retailing, mail order, leisure services, insurance,
pharmaceuticals, technology – all depend upon the ability to segment
their markets, to understand ever more exactly how individual end
users of their products use them, when, where, with what other products,
how they pay for them, what risks they do or can be predicted, what resources those end users possess or can be predicted to acquire. The transition from an industrially based to a service centred economy has been predicated on the increasing capacity to carry out this kind of personal profiling.

Geodemographic profiling tools are therefore emblematic of contemporary informational capitalism. Such tools process and present graphically in ‘decision ready’ form, huge quantities of matched and warehoused data on individuals, households and their characteristics. The very generality of these tools makes them applicable in a vast range of business and government contexts for the assessment of risk, desert and entitlement, and of targeting for worthwhile investment.

It is frequently said that in the information economy, the big returns are to information rather than to ‘other kinds’ of economic activity. In fact, this misdescribes the phenomenon. The point is that there are few ‘other’ kinds of activity, few industries that are not largely structured around personal information in their marketing, risk assessment, revenue collection and customer relations. Much of the worth and value of any modern manufacturing company now resides in, on the one hand, its stock and flow of personal data, and on the other, its skilled human capacity to analyse, manipulate and interpret those data rather than in the value of its physical capital plant, assets and inventory.

This is not say that the most profitable companies are the ones that produce the geodemographic profiling tools, either the ones that generate and sell the data content or even the ones that write the data warehousing software. As one would expect in a services economy, however ‘informated’, the most profitable are those that can use these tools to deliver the services to the greatest number of customers most effectively. In fact, the collection and production of information content is not particularly profitable, as any author of books like this one will attest. Business software has much smaller markets than software sold to individuals and is therefore much less profitable. In any case, the prices of both generic data content such as that embedded in most off-the-peg geodemographic profiling tools and of data analysis and decision making software is falling as these markets become more competitive, and
the effect is to squeeze profit margins. However, the analysis of personal information is a field in which there are substantial sums invested for research and development, as one would expect from something that today has as great a claim to be a ‘basic’ industry on both a national and a global basis as, say, agriculture, energy or medicine.

The structure of industries and the relationships between them increasingly depends on the development of business strategies based around the exploitation of proprietary data about individuals. Supermarkets are diversifying into retail banking, not only because they have other ways of earning revenues from expensive prime sites which conventional banks do not (hence the closure of many high street branches of banks), but also because they know a great deal about their customers’ preferences, transactions, and spending and have the software and data handling system in place for account management. New strategic alliances and diversifications reflect a new kind of business strategy, in which – unlike the model prevalent in the 1980s – focus on existing core competencies gives way to focus on the exploitation of a resource of personal information and a generic competence in customer service. Many of these new strategic alliances are emerging around the sharing of personal information, through joint loyalty card schemes. What the customer who takes such a card is agreeing to, is the disclosure of personal information about purchasing within the group and perhaps with any new companies which subsequently join.

Meanwhile, the historic affluence of developed societies is leading to rising expectations on the part of consumers about the quality, responsiveness, personalisation and relevance of services offered to them by both private and public sectors. But this comes at an informational price. Products can only be designed, tailored and targeted finely to individuals’ needs if those individuals’ needs are known to businesses. A majority of consumers are, as we have seen, privacy pragmatists, sophisticated enough to recognise that in order to enable suppliers to offer what they exact, they must themselves yield up more information about their behaviour, preferences, attitudes, connections and history.56

Public trust in these developments is not yet secured and, if it is not forthcoming, their commercial potential may be weakened; there is
also the risk of privacy social movements emerging to be publicly crit-
cical of the information ethics of some key business sectors, which
would in turn have damaging consequences for business reputations
and the strategy of data protectors. In the next section, I examine some
key risks – especially those of unjust inference and intrusion – in some
leading industries, while in the following section, I trace them through
a number of key business procedures.

Some basic general points run through this chapter. We can distin-
guish three kinds of unjust inference:

- inference based on inaccurate data
- inference based on accurate data but matched in ways that
  misleadingly suggest (but not strictly entail) a conclusion that
  is inaccurate
- inference based on accurate data and by a generally valid
  inductive argument that yields an inaccurate conclusion in a
  particular case.

The question of how best to reduce these risks turns into a choice
between two strategies. The first is to collect still more information
and to develop the personal profile to the point where unjust inference
is unlikely and the second is to make fewer inferences of any kind that
go beyond available data. In general, business prefers the former at
least as far as the costs of collection and analysis of data permit, while
data protection regulators prefer businesses to pursue the latter.

Privacy risks in some key information using industries
Different types of organisation in the public and private sectors pre-
sent different privacy risks and kinds of benefits to individuals in
return for providing some personal information.

Direct marketing and geodemographic profiling
Direct mail is the issue most commonly raised by survey respondents
without prompting when privacy issues are aired. Although many
consumers often find the unsolicited offers they receive of interest and useful, there are also significant numbers who feel that their privacy is violated, although the actual harms are trivial, by the ability of companies to know so much about them and the manner in which such information is acquired from other companies or government. In particular, any perceived inaccuracy in data held about individuals alerts people to the possibility of unjust treatment.\(^{58}\)

During the passage through the European Union’s legislative process of the 1995 Directive on data protection, the key concern about direct marketing was the issue of the demand from some of the privacy lobby for active, express consent to be secured from individuals before data could be collected and held about them. After extensive lobbying by the direct marketing industry, the Directive did not require this. Instead, in most cases, facilities for opting-out after being contacted, by means of mail, fax or email preference service, will suffice to comply with the legislation. Certainly, a requirement for prior active and express consent would probably have been unworkable and unenforceable, not least since the public sector makes available to the private sector so much identified or relatively readily identifiable data on individuals by way of electoral registers and anonymised census data which are analysed down to the street or even postcode level. For it was the publication of 1991 census data in commercially useable form in spring 1993 that provided the major boost to the increasing centrality of geodemographics to investment location decisions, stock and inventory management, database marketing, and general strategic management in the retail sector and now in many supply sectors.\(^{59}\) In many retail fields, of course, geodemographic data are combined with transaction data or data from customers collected by voluntary questionnaire, but these combined data sets, although perhaps not yet developed or used to their full profiling potential,\(^{60}\) are increasingly at the heart of information age capitalism.

The aspiration of many in the direct marketing industry is to achieve the ‘marketplace of one’, in which ‘redlining’ and unjust inference on the basis of assumptions made about people from certain
characteristics would no longer be a serious problem because most people would be given wholly individual treatment in decision making on entitlement to financial service, targeted only relevant promotions, and so on. It is not yet clear whether there will be declining marginal returns to this ever finer discrimination in markets. However, these strategies require the collection of very extensive and detailed identified data on individuals throughout the life course and this raises the hackles of many people. While being in receipt of ‘junk mail’ is not a particularly serious harm, some people – particularly older people – worry about the quantity of information held about them by direct marketers, and many more worry about the decisions made about their credit rating, insurance risk profile and so on, on the basis of such information.

Issues of intrusiveness also arise in connection with the kinds of questionnaire surveys conducted by direct marketers with people who have consented to fill them out. Standards of intrusiveness change over time: for example, fewer women now refuse to answer questions about the kind of sanitary products they prefer, but many are offended at being sent questionnaires on behalf of a dating agency. Promotions from lawyers are regarded as unacceptably intrusive if they are seen to follow a personal injury, not only because ‘ambulance chasing’ is regarded as unseemly but because many people resent the knowledge by commercial professionals about their private tragedies. Questions about political affiliation and views, ethnicity, religion, personal health and sexual habits are considered sensitive by many people and many direct marketing companies try to avoid asking them. Cold calling telephone marketing is still regarded as unacceptable to a majority of British people, although many Americans regard it as acceptable.

In marketing, there are issues of data accuracy that can bring about privacy risks, because they can lead not just to inappropriate offers but also to denial of service or even mistaken identity. When marketing data are used by credit reference and other financial services to target certain products, there are graver risks arising from inaccuracy or obsolescence of data.
Financial services

Banking, insurance, pensions and other financial services can raise a complex range of privacy and related issues. During the last recession, there was a spate of press criticism of the banking industry, focused on charges, not always well founded, of unjust inference – that is, of discriminating in the offer of loans and overdrafts and in the timing of decisions to call in loans with the effect of, firstly, cramping the capacity to grow and, secondly, of forcing difficulties and even bankruptcy in small businesses. Naturally, such charges were strongly supported by the small business lobby. In the insurance industry, as we have seen, risks of unjust inference may arise from the misinterpretation of genetic information.

The extent of concentration in financial services means that most of the large retail banks are now composed of quite large groups of companies offering a variety of financial services. This raises a difficult privacy issue for them in terms of the ethics of disclosure of personal information about individuals within the group. Should, for example, the insurance or pensions company within one of the big high street banking groups be able to access information about the history of transactions and balances on the cheque account? At present, pressure from the Data Protection Registrar (now to become the Data Protection Commissioner) and the privacy lobby has partially restricted this. In the case of some of the largest banks, the central business can see any of the subsidiaries’ data on an individual, but not vice versa.

The effect on the group of this approach is to make the privacy implications for the customer heavily dependent on the structure that the group’s management choose for themselves. So, if home loans are established as a separate but wholly owned subsidiary in one banking group while they are part of the central banking business in another, the disclosure rules will differ between the two banking groups. The worst consequence for the customer – perhaps not a particularly serious harm, but at most an inconvenience and a small loss of efficiency for the group – is that some customers may be irritated by having to provide certain sorts of information twice to companies within the
same group. Provided that customers understand the banking structure and provided that their expectations about when disclosure will be permitted and conducted or not follow that structure, customers may not be greatly disadvantaged. However, because the Office of the Data Protection Registrar takes a dim view of corporate restructuring to put activities into the central banking business, of which the principal benefit for the banking group is to enable disclosures, issues about the proper scope of privacy regulation and its impact on business structure are raised.

Moreover, in the case of banks it creates a tension between the basic impulses of the two sets of regulation under which they operate. The Financial Services Act puts great pressure on finance houses to know their customers’ needs and therefore their affairs in great detail. The Data Protection Act, however, by restricting disclosures within the group, requires some major divisions to seek either information afresh from customers – with the associated risks of error – or the customer’s explicit permission to collect data from elsewhere in the group, which can be a costly and time consuming communication when conducted on a large scale. But the importance of the cost of communicating with and asking customers for personal information should not be exaggerated. In many cases, asking customers for information can be a vital check on the accuracy or otherwise of data already held. Banks do, however, find that asking for permission for internal pooling of data does raise suspicions among many customers.

A much more important issue of disclosure is the relationship between individual banks and other financial services houses and the credit rating industry. The economics of the business mean that they are mutually dependent. Finance houses need the kinds of information that credit rating and reference agencies collect and analyse in order to make decisions on the risks they bear when considering whether to offer a loan, to accept a proposal for an insurance policy or accept a cheque account customer who may at some stage need an overdraft. On the other hand, the credit rating and reference agencies cannot assemble these kinds of data without the disclosures from the banks and finance houses that hold it. Consumers feel understandably
ambivalent about credit rating agencies. Few love them, but most accept that some system of risk assessment is essential to the viability of the banking system. A common compromise in the mainstream banking sector is for disclosure of defaults and other problems but not information about accounts operating normally.

The financial services industry must segment the population carefully in order to assess the risk that each individual or household presents of defaulting on a loan, of making a claim on an insurance policy, of needing to apply for an overdraft or of maintaining payments on a personal or pension plan. Therefore, banking and other financial services are increasingly dependent on database marketing. Moreover, because high value banking business is generally conducted with rich individuals and large businesses, the value to them of detailed information about less wealthy segments of the population is limited.

This raises the long standing question of whether the collection and analysis of ever more detailed individual level information by banks, insurance and pension companies will lead to the emergence of a class of people systematically excluded from opportunities to take out loans, acquire insurance or be offered pensions. While this is possible, it is also just as likely that such a group of customers denied service would prove to be a valuable business opportunity for other businesses willing to compete at this end of the market. Many people who incur debts in the first half of their lives prove, on a lifetime basis, to be profitable, and it is quite possible that in a more competitive and innovative insurance market, even those with certain higher genetically based risks of morbidity might prove profitable at lower level levels of premia. Already, there are conflicts between the marketing and risk assessment functions within the insurance industry on these issues.

Banks want to use sophisticated predictive models to forecast the probability of demand from individuals for different financial services and then to target specific promotions at those thought most likely to be interested. However, pressure from the Data Protection Registrar has discouraged them from using individual transaction data for this purpose and, for the present, the largest banks rely mainly on aggregate data. This issue raises one of the more difficult tensions within
the impulses towards respect for privacy. Many businesses dealing with individual customers would like banks to help them with their own risk management and marketing, by asking for information about the people with whom they deal. Most reputable banks will only disclose aggregate data on the general characteristics of the people with whom a business deals, but not individual data. This may in turn creates a problem for those businesses, seeking on the one hand to avoid unjust inference in database marketing by knowing more about their customer’s wishes and on the other being constrained by privacy rules to work with aggregates that bring risks of injustice if they use only aggregate data in decisions about entitlement.

Retail

The advent of the retail ‘loyalty card’ market has transformed the debate about privacy issues in the retail setting. Certainly, loyalty cards are not about loyalty – most people who have any at all have several cards, often from rival firms61 – but about the assembly of detailed transaction data on individuals in return for discounts, air miles, targeted promotions and other benefits.

How many customers have a clear understanding of the scale of information collected about them and analysed in the finest detail and subjected to sophisticated predictive modelling exercises on likely preferences and interests in other goods and services? While supermarket loyalty card managers generally take an optimistic view of their customers’ understanding, in our qualitative research we found many people ignorant or unclear about the scale of the information provided and about its value and few had any thought-out conception of whether the trade of information for discounts represented good value.

And indeed, there are risks of unjust inference here. Because a great deal can be inferred, rightly or wrongly, about a person’s lifestyle, tastes, health and behaviour from their regular purchase of, say, champagne, condoms, over-the-counter pharmaceuticals, there may be some concern about disclosure of such information to third parties, for whom such information about identifiable individuals could be
commercially valuable. Such concerns are mitigated where there is
competition rather than collaboration between major retailers in the
same retail sector that gives each one good commercial reasons not to
disclose. Likewise, it is not in the interests of retailers to disclose such
data to their suppliers further back in the chain, although they might
provide them with aggregate data on general demographic character-
istics. There is more cause for concern where, for example, customers
taking out a loyalty card scheme are not aware of the extent of disclo-
sures to apparently unrelated businesses who happen to be part of the
card scheme consortium.

Because of the same possibilities of sensitive inference leading to
some of the same problems within households thought to be raised by
itemised billing by telephone companies, supermarket loyalty card
scheme promotions generally avoid making much explicit reference to
consumers’ particular purchases. Many people find it alarming to be
reminded just how much data retailers hold on them. At least some
customers might be offended at the intrusiveness of the suggestion
that a supermarket might offer them on entry a draft weekly shopping
list based on their last year’s purchases. This application of the concept
of the ‘market of one’ is one for which not all customers are yet ready,
although this may change over time.

The largest loyalty schemes are run by the major supermarkets and
some retail petrol brands in association with large groups of other
firms. Because of the importance of acquiring detailed transactions
data on significant proportions of the population, it makes sense for
consortia of businesses to share such data. Some supermarkets have
entered into alliances with unrelated companies such as do-it-yourself
stores. Strategic alliances between apparently unrelated companies
who want to share personal data are increasingly the development
strategy in the retail sector for loyalty schemes. ShellSmart, the Total/
Marks and Spencer scheme and many others have proven relatively
successful.

These schemes raise important privacy issues, particularly where
existing databases of details on individual customers are pooled, for
this amounts to a change of purpose for which the data are collected.
The data protection principle which says that information must be collected only for a notified purpose is supplemented in the new legislation with increasing pressure to seek consent. This has become an issue in connection with the strategic alliance between Tesco and the Royal Bank of Scotland to offer personal finance products to Tesco ClubCard shoppers, some of whom have filed a complaint with the Data Protection Registrar about junk mail, and with Centrica, the gas supplier’s attempts to use its database for cross-marketing with strategic allies. While the costs of making contact individually with every customer on whom details are held, informing them of the change of purpose, offering them benefits from the pooled data scheme and offering them individual opt-out may be prohibitive, it seems unlikely at present that the Commissioner will compel any of the major schemes to do this. There are other ways in which customers can be informed of changes of purpose and given opportunities to exercise consent actively or passively. However, if such pooled data schemes do run into problems of consumer trust as a result of failing to bring consumers with them, data protection principles may need to be enforced.

The emergence of more strategic alliances and joint offers between supermarkets and banks and finance houses raises privacy related issues. Supermarkets are content in principle to sell most kinds of goods to any customer willing and able to pay. By contrast, many financial services are sold on the basis of selection by assessment of the risk that consumers present. The use of data collected for the first purpose to help make decisions about the second raises concerns. For example, should a collaboration between a supermarket and an insurance company to offer life insurance be permitted, using loyalty card data on alcohol and cigarette purchases in the supermarket in the course of the insurance risk assessment? Because this involves transfer of risk and denial of service in some cases, this is clearly different in kind from simple segmentation of customers in order to target offers to particular customers. At present, most reputable supermarkets would be chary about this and the Data Protection Commissioner would probably raise objections, but the debates will rumble on.
Finally, it is expected that there will be a growing demand for home shopping, initially for the growing numbers of elderly people, but gradually more widely. Few people enjoy queuing at checkout tills and most find the carrying of bulky homogeneous goods time consuming and awkward. Internet shopping and home delivery are therefore natural directions in which to expect the industry to move. Some supermarkets already offer fax based ordering and either personal collection or delivery services for which purchasing data are used to produce a draft personalised shopping list. There may be customers interested in home shopping but they will find it alarming that their purchasing patterns are analysed in this way.

**Telecommunications**

Telephone companies have introduced itemised billing in response to demand from many customers. However, in the early years of itemised billing, there were concerns expressed that the system meant that one spouse could no longer keep calls secret from the other, and that the privacy of teenagers to use the family telephone without parental supervision of numbers called was being removed. While it is difficult to have much sympathy with these relatively minor dignity concerns, there are good reasons why, for example, calls to certain legitimate helplines should perhaps not appear on bills if callers ask that they do not, since they may have good grounds for wishing other household members to remain ignorant of their use of these services; otherwise people may be exposed to the risk of denial of the means of self-protection. In some European countries, there is continuing pressure that full itemised billing should be discontinued and that, at the very least, full numbers called should not be printed on bills.

Telephone companies do analyse data on calls for other purposes. They clearly provide some support to the state security services and the police in call interception and presumably can also provide analysis of calls on request. Call data are analysed in efforts to track telephone fraudsters conducting three way calls to clone mobile telephone identities. For more commercial reasons, BT now analyses each
customer’s calls and offers them a list of their most frequently called numbers with a view to selling them their reduced rate Friends and Family facility.

There has also been a debate in the US and UK about telephone harassment and the now widely used offer by telephone companies of caller line identification (CLI: available widely for the last incoming call made by dialling 1471 in the UK) and caller display. Those who have been harassed greatly welcome this service, although some people dislike the fact that it enables those working in call centres to call up their details even before they have given their name or other details. BT reports that malicious call complaints have fallen since the introduction of such facilities. Nevertheless, there have been some objections on privacy grounds. Although it is hard to see just what valid privacy claim there can be which would protect someone’s anonymity to the person called, BT allows caller display and line identification to be overridden by the caller by dialling 141 prior to dialling the number: other companies allow recipients a facility of rejection of such anonymous calls.

**Privacy risks and business procedures**

In this section, I turn to some of the business procedures that raise concerns about privacy.

**Cross-marketing**

Cross-marketing of products raises some privacy issues. Here a company enters an arrangement with another one, with which it has no conflict of commercial interest, because each company markets the products of the other, or perhaps they will jointly develop a product exclusively for each other’s customers. They do so either for a payment, in barter for a similar service in return, or with joint risk bearing. The legality of the use of their own customer database for this purpose will depend heavily on the registered purpose for which those data have been collected – and for which it is assumed that those customers have consented to the collection and use of personal information. Moreover,
there are industries that have found more difficulty with the Data Protection Commissioner in targeting specific customers than in sending out a more expensive, untargeted promotion to all customers. Once again, there is a conflict between two privacy risks: one of unjust inference on the basis of insufficiently detailed profiling and the other of excessive knowledge.

More fundamentally, there is a conflict between the privacy impulse to ensure that personal information is used for the express and limited purpose for which it was collected, and the commercial imperative to innovate and to apply personal information to new purposes. Specifically, in an age of increasing importance in strategic alliances between businesses to develop new products, there is a perceived conflict between privacy concerns about disclosures and the commercial logic of alliances. Such conflicts can be resolved by seeking customers’ active or passive consent to an extension of the purpose for which data are held and used, and offering some kind of opt-out along the lines of preference services. However, this is costly and also risky, in that it may raise customers’ suspicions about the scale and purpose of data collections. On the other hand as more and more people can be contacted cheaply and quickly by digital means, the costs to business of this kind of customer consultation may fall.

**Data matching**

Matching records from different databases about the same individual is known as ‘data matching’. Whether a particular matching exercise raises serious privacy concerns depends on the context, the purpose, the type of information and the types of decision to be made using the matched data. For example, in the collection of any data, matching is part of the ‘data cleaning’ that is routinely undertaken, in order to test for inconsistencies. The selection of data for matching brings risks – firstly of inaccuracy, secondly of matching records against the wrong people, and thirdly of unjust inference because combinations of data may misleadingly suggest characteristics that people do not in fact possess.
However, when data are acquired commercially from other sources, even when the purposes for which the two data sets were collected are exactly similar except that the company or group intended to benefit from the collection (such as retailers’ buying each others’ transactions records on named customers), these disclosures are widely regarded as unacceptable violations of a duty of confidentiality between a company and its customers, however profitable the sale of the data may be.

**Cross-border flows**

The volume of personal information moving across frontiers is growing rapidly, along with the volume of cross-border trade, investment and communication generally. There are several types of cross-border flow:

- transfer to contractors (or within multinational companies) in other countries of volumes of data already collected from analysis, warehousing and mining
- transfer to contractors (or within multinational companies) in other countries of systems of data capture from transactions within a country
- transfer of single records or small numbers of records or less structured data embedded in international data communications of other kinds, such as e-mail messages
- transfer of data of any of the above kinds, from a source to a destination within a single country, by a means that routes the data through a third country, where the data is not used in any significant way before being shipped on.

The greatest privacy concern is generally about the first two types of transfer, where the source country may have tighter and stricter privacy controls on the use of personal data than the destination country. In particular, the European Directive and the 1998 implementing Act place restrictions on the transfer of data to countries outside the European Union where the destination country is deemed to have
a system of data protection that is ‘inadequate’. How this will be done is not yet clear: either a list of countries with protection generally deemed adequate, or a list of those deemed inadequate, could be published; transfers of ‘sensitive’ data could be subject to special case-by-case controls; a list of agreed basic protections could be published to which countries must conform (an EU working party has proposed the following list: purpose limitation, data quality and proportionality, transparency, security, subject access, some implementation and enforcement mechanism and so on); countries ratifying the Council of Europe Convention 108 could be deemed to qualify.63 However, the drafting of the Directive is in danger of catching the third and fourth kinds of transfer within its net.

Because the costs of data processing labour are much lower in many non-European countries (especially in India and south east Asia) and also because in some countries there are more skilled staff available, or because Japanese and US based multinationals need to centralise data outside Europe, the economic pressures to transfer data more freely are growing.

There are contractual solutions to the regulatory problem. For example, some US banks dealing with data from German subsidiaries have contracted to conduct data processing in the US to standards that meet German data protection legal requirements. However, unless the costs of such contracts can be reduced through the widespread availability of standard clauses, in countries outside the European Union, of training, software and management systems to make compliance with such arrangements affordable, there are limits to what can be expected from contractual solutions.

**Procedures for assuring people about risks:**

**codes of practice**

Finally, we turn to strategies used in many countries by information age businesses to offer some reassurance to customers and the wider public that the privacy risks they might fear are being kept to a minimum.
Sometimes, with the encouragement of data protection and privacy regulators, voluntary codes of practice are adopted on privacy issues. These codes tend to be incorporated into wider codes of practice on customer relations. They are certainly valuable if they are used in training and the design of data management systems, but little is known about compliance with voluntarily adopted codes. Some codes are adopted on behalf of an industry by a trade association and, in these cases, compliance depends on the extent to which members are willing to hand over authority for audit and monitoring to that association and its capacity to carry out these functions. One widely distributed code is a joint product of the British Bankers Association, the Building Societies Association and the Association for Payment Clearing Services. It guarantees customers an opportunity at least every three years to opt out of automatic marketing of further services and products. It also guarantees not to pass name and address data to other companies, even within a group, for marketing purposes but it reserves the right to cross-market other companies’ services to you. It also includes an undertaking to be ‘selective and careful’ when marketing to under eighteen year olds. The specific codes of practice for the press and broadcasters are discussed in Chapter 11.

Canada is rather further ahead than the UK in the development of standards for industry and company codes of practice; the federal standards bodies there have issued a model code. The code sets out ten principles, which are broadly similar to the UK legislation’s principles:

- organisations must designate individuals accountable for the organisation’s compliance
- purposes must be identified by the organisation or at the time of collection
- knowledge and consent are normally required for collection, use and disclosure
- collection must be limited to that which is necessary for the purpose, and fair and lawfully collected
- likewise, use and disclosure must be restricted to the purpose; information must only be kept as long necessary for it
○ information must be accurate, up-to-date and complete for the purpose
○ sensitive information should be subject to specific safeguards
○ organisations must provide information about their policies and practices on personal information
○ individuals should be told, on request, of the existence, use and disclosure of their personal information, given access to it and have the chance to challenge accuracy and completeness and secure appropriate corrections, and
○ individuals should have the right to bring challenges concerning compliance.

The Data Protection Registrar in the UK has published guidance on how companies and trade associations can develop their own codes of data matching, based on particular applications of the existing UK data protection legislation principles. Unlike Australia and New Zealand, the UK has no legislation governing the way that data matching should be controlled.

Goals of business with personal information

Business organisations seek above all else to influence the behaviour of consumers, in favour of buying their products once and many times again and, as a means to achieving this, they seek to change attitudes through branding. For this purpose, it cannot be denied by most thoughtful business people that they need to seek some measure of control over consumers. The language of ‘lock in’ that marketers use about their regular consumers exhibits the kind of control that business marketing and sales forces seek.

The fit between this kind of vocabulary and the classical vocabulary of liberal thought that has traditionally been used by those seeking to articulate business interests is sometimes uneasy. Traditional economic liberal discourse speaks of consumer preferences as given and takes them to be the forces that should drive economic action and to which supply should in the long run respond. For business strategists,
the key to success is to influence those preferences before, during and after the transaction: ‘lockin’ is the key.

In informational capitalism, it is easy to see how privacy has moved centre stage in business ethics, in the debates about the coherence of economic liberalism’s concern for free markets and political liberalism’s commitment to the protection of individual consumers and citizens. Privacy provides a vocabulary of risks in which the conflicts of the age can be discussed. The seepage of privacy concerns into other concerns about who should bear which risks in an economy is natural in a context in which personal information determines the balance of risk in any transaction and is thus the key to pricing.

In fact, issues of control and privacy in the transaction or relationship between consumer and business or between citizen and government are closely linked. Consumers and citizens have ways both individually and collectively of influencing the informational context of transactions and business often lacks the means wholly to control that context, not least because the information processing involved is still expensive. Businesses understand full well that public trust, individually and collectively, is critical to any strategy of bringing services to market, and information ethics play a key role in that. The politics of privacy condition the economics of trust, and that is why he simple argument that the economics of information determine the future or privacy must be firmly rejected.
Although it has become natural to many people to think that new technologies are bringing about the death of privacy, this is a quite misleading view. Technologies are now available that could, if more widely used, be used to buttress privacy as never before, if we choose to place our trust as consumers, our resources as investors, our authority as citizens in those organisations using them and if we can find a way to make those uses culturally viable. This chapter will argue against the widespread deterministic view that technology or, at any rate, the economics of technological development, dictates values in such fields as privacy and information ethics. The choices that are made about directions to pursue in research and development, and about the introduction and use of information technologies, are shaped by cultures of privacy and information ethics.

Certainly, the use of both new information and communications technologies has increased some privacy risks. As discussed in the previous chapter, data matching and mining, hacking and snooping are all techniques that can put our privacy at risk. But technological strategies can encounter cultural resistance in the form of alternative applications of the same technologies. New systems are emerging for securing information against unauthorised access and there are now efficient ways to conduct transactions which preserve anonymity. Naturally, the usual conflicts are emerging between liberals and civic republicans over their desirability. If the technological determinist theory were correct,
the main form that we would expect resistance to take would be Luddism, but in fact privacy enhancing technologies provide a powerful example of the use of informatics to serve culturally specified ends.

In this chapter, we review the implications for privacy risks and privacy cultures of trends in the design and the use of information technologies.

Technologies of data collection and surveillance
Forces exacerbating privacy risks include the rise of sophisticated techniques for database hacking, transmission interception, unannounced collection of visual information and other data, the increased capacity of storage devices to handle large databases, increased computing power in manipulation and network search. New information technologies can also provide new commercial rationales for surveillance and profiling of individuals.

Surveillance of physical space: closed circuit television
Closed circuit television (CCTV) is now widely used in public places including shopping centres, main urban streets, inside and outside major buildings, in lifts, on the many housing estates where tenants have demanded it and in many other areas. The purpose of CCTV is partly the detection of crime through the contemporaneous viewing by security staff in back offices of relayed video or subsequent analysis of video tapes following an incident. It has been actively promoted in government policy, including in the 1995 ‘CCTV Challenge Competition’ when the Home Office made available £15 million for bidding to put in place 10,000 additional cameras. Some voluntary agencies, such as Crime Concern, support further extension of CCTV schemes. Certainly, CCTV in public places has proven popular with the public, reflecting some of the shifts in public values towards a tougher stance in the trade-off between surveillance of the innocent and the apprehension of the guilty.

It may be that the key effect is to increase the feeling rather than the fact of security from crimes against property and the person. Indeed,
dummy cameras have been used in some places as a cheaper alternative to functioning video cameras in the hope of deterring crime. However, where the public have reservations about CCTV, they tend to be concerned with questions or doubts about operations rather than privacy or overall effectiveness. Is anyone watching? Is there still film in the camera? Will the quality of the video be sufficiently high to enable identification of a putative criminal filmed in the act? Will it simply displace crime to other neighbouring areas? Some surveys suggest that almost 30 per cent of the population put the presence of CCTV systems in their top three factors in making an area feel safer. In qualitative research, privacy concerns are usually low down on people’s list of concerns about such schemes.67

Civil liberties organisations have expressed concerns about risks of unjust inference from data taken from CCTV schemes. These include suspicion of movements that are quite innocent or wrongful attribution of behaviour or misidentification of individuals68 on the basis of poor quality pictures and hence the risk of reversal of the presumption of innocence. They also cover the absence of consent by individuals passing through an area subject to covert surveillance.69 There have been concerns about the security of the video footage collected. In one well-known case a commercial video, called Caught in the act!, was made by a Mr Barry Goulding in 1995 from sections taken from private security firms CCTV video footage without the consent of the individuals filmed and released for sale. People were shown making love in lifts, getting undressed in changing rooms and indulging in self-flagellation.70

Video data are now generally capable of being processed just as much as text can be and, therefore, most such data will fall under the revised definition of personal data embodied in the 1998 legislation. This will make unlawful certain disclosures, some cases of ‘retouching’ or ‘enhancement’ of film, and perhaps even reliance as evidence in court cases on video film that has been damaged through being played many times,71 and other misuses. The data protection principle that perhaps presents CCTV schemes with the greatest difficulty is that requiring adequacy and relevance without excess. In theory, schemes
that are poorly sited and targeted could fall foul of all three parts of the principle. A camera sited so as to look principally into a private home, even one rented from a local authority, would generally be considered to breach the principles on fair obtaining, design for legitimate purpose as well as the principle against excessive or irrelevant collections. There were unsuccessful efforts by civil liberties bodies to insert a clause into criminal justice legislation in 1994 to create a licensing scheme making it unlawful to use such systems for surveillance of private residential premises without consent.\(^7\)

The heavy involvement of local authorities, both in administering their own CCTV schemes on their own property and in granting planning permission for private firms, has led to extensive discussion within local government about the appropriate principles for their implementation, and guidelines have been developed, which have been broadly welcomed by the data protection authorities.\(^7\) The code covers such issues as application of data protection law, management, installation, siting, complaints, evaluation and audit liaison with the police and other agencies: it strongly counsels against the use of dummy cameras and also against the recording of conversations.

CCTV has been a politically chosen instrument in the pursuit of a particular policy of crime deterrence and detection and a particular strategy of reassurance to residents and investors in urban areas. There are countries that have made quite other choices, such as Scandinavia and Austria, where CCTV is used only in connection with police and military buildings and a few major public buildings through to be at risk of attack. The emergence of codes of practice and extensive debates about the ethics of such schemes has brought the debate about CCTV in Britain into a new phase. It is becoming part of the wider debate about information ethics and the tension between privacy claims and the claims of authority. Even during the decade in which CCTV has become a common feature, the cultural attitudes to CCTV and the use of the technology have changed. The fact that *Caught in the act!* became a scandal was in itself revealing of the scale of cultural division and change. Far from CCTV being an example of the technological determinist outlook that ‘if it can be done, it will be’, it reflects
instead the importance of culture as the context in which use and development and application are shaped, debated and resisted.

**Surveillance of physical space for other data capture: smart transport systems**

In the twenty first century, the information intensity of road and railway journeys will be steadily increased and the management of traffic in both will become increasingly similar. Today in much of the developed world, a driver pays for travelling on only a very few roads, makes distinct decisions at each stage of a journey about which route to take, decides at each moment how close to the car ahead to travel and is subject to no particular surveillance over how fast, how distantly from the next car or over which route she is driving. The advent of the ‘smart road’ will change all this. Drivers will purchase particular journeys in advance, on locking into the smart road management system, will hand over many decisions about the route, how close to nearby cars to travel, and so on to the computerised road management system, which will also manage all billing for road use perhaps through deducting value contactlessly from a smart card embedded on the windscreen. Large databases could easily be assembled describing typical journeys, including profiles of individuals’ journeys and presenting special offers targeted to users of particular journeys. In the event of a breakdown, the road management system could relay to a nearby garage of the driver’s choice, the car’s location, the registration number, perhaps even the name of the owner and advance payment for repairs, while the road management system would also shunt the defective car to a safe position while smoothly managing other cars to take its place. Again, such systems can be used for policing compliance with vehicle emissions laws. Some are now under trial in Germany, Britain, California and other states.

In Germany they have already raised serious privacy concerns. And in general, contactless technologies attract lower trust than contact based systems, because many people are not confident about data collection being limited to the stated purpose. For example, some people
feel that apart from collecting information necessary for charging for a particular journey only, these systems could be used to identify a pattern of journeys that a particular car takes over time or even to collect information from other smart cards in the car or on the persons travelling in it.

While privacy enhancing technologies could be built in relatively cheaply from the initial design, they are difficult and expensive to add later. The culture of many programmers and designers of such systems is one that does not look to privacy issues at an early stage: risks of abuse of privacy are not part of the design evaluation of many such technological developments. Not all the concerns about surveillance of journeys are defensible: itemised billing for journeys may bring risks for insurers to adulterers of being found out by their spouses but this is hardly the strongest ground on which objection might be raised. More important grounds for wanting privacy enhancing technologies built in to such schemes are the risks of unjust inference. An organisation can put together data about journeys with other information that might produce misleading inferences that could the basis for unjust treatment – for example, matching purchasing records with journey data could build up quite misleading profiles of individuals’ lifestyles. This is a particularly serious risk where the brief for such schemes is written in ways that encourage the flow (‘coordination’) of information from smart road systems to other agencies that might have an interest in it.

**Surveillance of cyberspace: covert data capture**

Software is now available that can, when an individual visits a World Wide Web site, identify the e-mail or IP address of the computer from which the individual is working, track the site from which they came, the way in which they move around a given site and where they go on to visit, collect other information on the contents of the hard disk including documents currently or recently opened. All this can take place unbeknown to the visitor to the site. Software for this kinds of capture is readily available commercially and is being used for routine
profiling of visitors. The commercial value of such information is potentially vast, if site owners and webmasters can use it to profile the kinds of people to whom they currently appeal.

There is widespread concern among the Internet community about these practices. While it is hard to be sure that Internet surveys of e-mail addresses are representative, so fast is the community growing and so hard is it to track people down digitally, recent surveys suggest that privacy – in this sense, of covert collection of data as one visits a web site and also more overt profiling of individuals by posting to Usenet groups – is one of the most important concerns for regular Internet users. A Boston Consulting Group study for Truste™ in March 1997 found that more than 70 per cent of respondents were more concerned about privacy on the Internet than about privacy in phone and mail communication; 41 per cent reported being asked to leave registration information as they visited sites; 60 per cent did not trust web merchants with personal information.

The same kinds of systems are already in use by law enforcement agencies to track users of sites of particular interest to paedophiles, terrorists, drug traffickers and the like. Again, there are risks of unjust inference here, because some visitors to these sites may be researchers, journalists, private investigators and others with a legitimate reason for pointing their browsers in these directions.

Attempts have been made to increase the openness with which data are collected. For example, the Open Profiling Standard, developed by Netscape, Firefly and Versign, is an attempt to create a standard for web capture that is more transparent to web site visitors in a situation where individuals have some choice over what information they wish to provide, what uses are made of it and what may be disclosed to others. The standard is intended to facilitate data mining but includes a consent control. There are several other such systems now in use on the Internet. The emerging issue with such profiling standards here may be that the default settings on the menu of choices may well be those that would permit disclosure: if most people do not check all the default settings, this could prove to be a highly manipulative way in which to secure the letter, but not the spirit, of consent.
Technologies of security
As forces offering partial protection by way of data security we can count the development of public key cryptography, new privacy enhancing technologies such as password and biometric authorisation and other kinds of security firewalls, and the capacity of individuals to use multiple identification codes in electronic communication across networks.

Public key cryptography
In a traditional or conventional system of encoding information, it is necessary for the person who encodes the data to be able to send to the recipient in some secure way, the means of decoding it, which are the same ‘key’. This is difficult to do, and if it were straightforward then, in many cases, it would be redundant to encode the data. This problem was solved in the 1950s with the development of public key cryptographic systems. In a public key system, data can be encrypted with one key which is kept private and secure by the sender (the ‘private key’) and divulged to no one, but can also be decrypted with the use of a second key which is available to the sender (the ‘public key’) but from which the private key cannot be deciphered. Clearly, if the private key is acquired, the system’s integrity is lost, but as long as the public key is held only by individuals trusted by the sender, public key cryptography systems can provide a greater measure of security than traditional ones.

Modern cryptographic systems are mathematically sufficiently complex that without possession of one of the keys, decryption can – at the moment – only be done using the ‘brute force method’ of instructing a computer to try every conceivable transformation until something works to produce a sensible message. This takes time, and is usually conducted using several processors (‘massive parallel attack’). However, where the key is relatively short, there are fewer conceivable transformations and the process is typically less time consuming. Therefore, in commercially sensitive and military settings, a security ‘arms race’ has opened up, with ever growing bit lengths of keys: 128 kilobytes is now common and many companies are using 256 Kb keys,
while 512 Kb and longer will soon be available commercially. At present, the time taken for encryption grows with key length, but with the increasing computing power of microchips in workstations and high performance personal computers, and with developments in cryptography itself using different and more efficient algorithms,\textsuperscript{76} this will probably be a less serious problem than it has been.

One interpretation of the duty imposed by the EU Data Protection Directive that electronic communications must be secure is that businesses and government agencies should, wherever possible, make use of some technique for encryption – although not necessarily a public key system. However, there are still countries within Europe, let alone others through which information might pass, in which strong cryptography is seen as a \textit{munition} that only law enforcement agencies, the military, some parts of civil government and specially authorised banks and financial institutions handling secure payments may legally use or possess.

In the USA, for many years the federal authorities have taken the view that strong encryption is a munition, to which access should be restricted to the military and state security forces and export of encryption systems is prohibited. In a now famous case, the federal authorities attempted to prosecute Phil Zimmerman, author of the PGP (‘pretty good privacy’) system, for illegal export. Although the case eventually did not proceed, the Internet community responded by circulating the algorithm on his behalf, inviting the US federal agencies to prosecute many thousands of people. Some people printed the programme code on T-shirts and wore them on flights from the USA in an effort both to protest against the prosecution and to invite the authorities to prosecute them.

The Clinton administration first proposed a settlement, in which encryption would be permitted, but the federal authorities would retain the means of decryption. This system, called ‘mandatory key escrow’, is defended on the grounds of the risks associated with criminal organisations, terrorists and others having access to cryptography and the need for assured interception.\textsuperscript{77} In this system, individuals and companies must deposit subject to a duty of care or ‘escrow’ their private
keys either directly with law enforcement authorities or else with licensed private agencies trusted by the law enforcement agencies to yield up keys for decryption should they deem it necessary in the interests of national security. At first, this was to be implemented in hardware, using the so-called ‘Clipper Chip’ which would become mandatory in all US-built computers. However, resistance from computer users, the Internet community and computer manufacturers fearful that sales outside the US would slump if customer believed they were buying a computer ‘with the FBI inside’, meant that the proposal was eventually shelved in favour of a mandatory key escrow proposal using trusted third parties. Congress and the administration have yet to agree on a federal scheme, although some states have passed laws requiring key escrow.

Already and in much greater quantities in the future, many products and services will have cryptography embedded in them, as a secure means of communicating between elements in a system. MasterCard and Visa have developed a secure electronic transactions (SET) environment intended for use in electronic commerce. Many encrypted messages are already sent between users of Lotus Notes without those users necessarily being aware that they are sending and receiving such messages. In future, cryptography will be embedded invisibly in the ways in which refrigerators, light switches and other appliances in smart homes and cars communicate with one another, and in many other everyday technologies. When cryptographic operations are carried out unknown to the user, markets in the supply of such systems will be much more competitive globally, and it will prove very difficult for national regulators to enforce prohibitions without damaging their own industries.

**Trusted third parties**

All this has given rise to a new kind of regulatory problem, which has in turn elicited some potential solutions.

Business and government agencies need to authenticate the identities and trustworthiness of individuals and other businesses with
which they deal over electronic networks. It has been proposed in a number of countries that private agencies might emerge to facilitate this.\textsuperscript{79} Often called trusted third parties (TTPs), they might carry out one or more of a number of different functions for which different legal frameworks would be required. Broadly, these functions are of two kinds. Firstly, there are a range of functions that TTPs could carry out which would facilitate the growth of electronic commerce, either in more or in less privacy enhancing ways. Secondly, there are functions that relate to technical systems for maintaining confidentiality, integrity and security of information systems and data by individuals. These have to be traded off against the demands of law enforcement agencies for access to information if it becomes necessary in the course of criminal investigations or counter-terrorist operations. The main functions put forward for trusted third parties are given below.

**Facilitating electronic commerce**

- *Certifying identity:* providing certificates that an individual or business using a certain identifier – a digital signature, electronic pseudonym or ‘nym’,\textsuperscript{80} a biometric or other device that can be transmitted electronically – is indeed a particular client; or, in a privacy enhancing form, that someone presenting such-and-such a nym is indeed a client; some certificates will be worth more than others, depending on the level of checking undertaken, the integrity of the certification process and the handling of the certificate itself, and there are dangers that some people may be misled into relying on certificates that are in fact worth rather little.

- *Certifying other facts about their clients:* for example, that they have transacted with an individual or business in the past; that the previous transaction was completed satisfactorily; that the certificated individual or business is subject to
the jurisdiction of a certain national legal system or part of a larger company; once again, disclosure of true identity is not necessary for such certificates to have value.

- Certifying entitlement to certain services: in effect, this is what banks and credit rating agencies do for retailers at present, but they and other kinds of TTP could offer this service across a wider range of contexts; alternatively, certificates could be issued that would attest that the client possesses certain characteristics that would suffice for entitlement to service, for example is aged over eighteen or lives in a country in which access to strong cryptography is legal; of particular interest for the preservation of privacy, such certificates need not display the true identity of the client, but simply attach the assertion of entitlement conditions to the nym.

Facilitating risk management in encryption and facilitating law enforcement over private use of strong cryptography

- Holding private keys for decryption in escrow for individuals and businesses, in case the depositor needs access to a duplicate copy, in case law enforcement agencies secure a warrant for the release of the keys, or perhaps to enable them to advertise the fact that they have escrowed their keys as an indication that they are law-abiding and trustworthy.

- Providing key management services such as key recovery but without themselves holding private keys; while key escrow systems require the prior deposit of keys with an agency, there are now key management systems allowing recovery both by the client and by law enforcement agencies; TTPs could, for example, hold details of certain security procedures that could be used to access keys without themselves ever carrying out those procedures.
An intense debate about the nature of the national, regional and global legal and institutional framework for TTPs has opened up in the late 1990s. The proposals from the Department of Trade and Industry under the British Conservative government on 20 March 1997 are for a licensing framework that provides primarily TTPs that will provide for mandatory key escrow. Those proposals were condemned by many industry bodies and most civil liberties groups. At the time of writing, it is not yet known what the policy of the Labour government will be, although there have been suggestions that the old Conservative policy might be revived but, so far, an announcement has been delayed and consultation extended. The United States government has put forward proposals that, if accepted by Congress, would permit unlicensed TTPs to operate key escrow and key recovery systems.

Proposals for legal frameworks for TTPs raise a number of privacy policy questions:

- liberty to use encryption to keep messages and data confidential versus concerns of law enforcement agencies about the ability of criminals, terrorists, etc, to use cryptography to evade investigation and detection
- claims of the right to anonymity in transactions where it is not necessary to declare true identity versus concerns of regulators about the need to identity individuals and businesses for taxation and other law enforcement purposes
- concerns about the data protection regulation of TTPs and the difficulties of both uncertainty of jurisdiction and of extra-territorial application of laws: TTPs will probably seek to attract clients, perhaps to take deposit of escrowed keys and to offer certificates across frontiers; they will therefore need to operate in several jurisdictions, which may have very different data protection requirements, and it may be unclear in which jurisdiction they may be liable for any alleged violation of laws.
There are wider issues about TTPs which have secondary connections with the privacy questions. These include:

- whether there will be much demand for TTPs services
- what kinds of organisations will be willing and able to enter the market to become TTPs (banks and phone companies have sometimes expressed an interest: as Volume 2 shows, these agencies begin with very different profiles of public trust and scepticism, even before considering the effect of becoming a TTPs on the basis of that trust)
- whether individuals and business will in fact trust them
- to what extent TTPs will be liable to those who rely on their certificates in conducting business with their clients or persons who purport to be their clients, for any inaccuracies, in respect of any losses that those bodies may incur; whether the market will function properly, if people are uncertain of the real value of a certificate and the extent to which different TTPs check out their clients and their trustworthiness – can individuals be left subject to the rule of caveat emptor?
- problems of conflicts of laws between states; for example, there are states in the US with quite contradictory requirements upon certification agencies in the event that a certificate is challenged
- whether there will be competition between different countries regulatory regimes to attract investment in TTPs that will operate globally (just as the US state of Delaware competes with other states for the location of business by offering the most minimal regulation of company law and very low business taxes); and if so, will people wanting to create TTPs – perhaps as additional services offered by offshore Internet banks – flock to the least regulated country offering the lowest levels of liability, because that will prove cheaper? Or will they go to the most regulated countries offering the highest levels of liability because that will attract greater trust, just as Switzerland's confidentiality rules in
banking have – at least until recent scandals – worked to attract trust in Swiss banks?

If there is little demand, little trust and not much competition, then the privacy issues associated with the existence and service offerings of TTPs specifically will not be very important.

**Regulation and culture of private security measures**

It should be clear that even in the field of cryptography, which depends on mathematics so complex that only a tiny proportion of those who use it even today understand it and therefore is much more under the control of technologists, the technology itself has not led the way: in fact, cultural forces have. Conflicts between liberals and civic republicans over the question of whether to regulate – if so what to regulate and how to enforce it – and resistance by Internet communities and security forces alike to developments they fear, have shaped the ways in which the technology is developed and used.

Increasingly, the issue of regulatory capacity to keep strong cryptography out of private hands has been settled, as liberals have wanted, by market forces. There are too many legitimate reasons of business confidentiality and needs for security in large financial transactions for government to ignore. However, it does not follow that there are no choices about how societies will proceed in order to cope with the consequences of the growing private use of encryption in ordinary communications, in embedded systems and in many other contexts.

**Technologies of storage and transaction: smart cards**

The lubricant of the information age has been miniaturisation. One of the most convenient forms of miniature computing power is now occupying space in wallets across the world, embedded on plastic cards the size of credit cards. Some ‘smart cards’ contain little more than storage capacity (‘chip cards’), others contain processing capacity which, when activated by a card reader device, can carry out transactions on the card. They are now widely used across the developed
world for storing and processing value in the form of money or vouchers in ticketing systems for public transport or in telecommunications, as library cards, to store ‘loyalty card’ applications in the retail sector (while many schemes still use magnetic stripe technology, many of them are planning to shift to smart card systems), in the public sector to handle benefit payments and provide a check on identity, and in many buildings they store authorisation procedures for securing access. Most citizens in Britain will possess several of these in the next few years.

So far, most smart card systems have carried a single application. However, there are now commercially available multi-application cards, which store a number of applications each in a separate directory. The best known is Multos, developed jointly by the MAOSCO consortium of which the electronic cash group Mondex is a member.85

The key privacy risk from multi-application cards is that data held in one application may be accessed by the reader devices intended for another – this ‘peeking’ would be unauthorised data matching. The use of encryption and biometric based identification and authorisation systems may help here, but not entirely. The Multos system does contain firewalls between the directories in which distinct applications can be sited, but not all multiple application operating systems offer a significant degree of security. It may soon be possible to design a card reader system that will be able, without the knowledge or consent of the cardholder, to collect data from a card for later decryption attack. It has been shown that it is possible to tamper with most smart cards in commercial use today, in order to read and then to use massive parallel attack to decrypt data from them.86 Security is far from complete.

Perhaps more worrying is the possibility that a culture may grow up in which insurers, employers and other agencies who bear risks in their contracts with individuals may routinely insist on access to data from any smart cards held, when those data are not necessary for the purpose of the transaction and when in some cases they might be misleading and lead to unjust inference. At present, in theory, insurers and employers can demand many kinds of information but they do not in fact do so: the ready availability of large quantities of data from smart
cards may, it is feared, change the culture in these fields. When being offered a new card, it is quite probable that many consumers will not have sufficient information about the levels of security that it offers against rogue reader devices and so, without some kind of kitemarking scheme at least among the more reputable suppliers, it may be very difficult for market forces to ensure that people can choose the levels of security they want effectively.

Peeking is much more likely if suppliers and providers of applications own the cards and decide which other applications they are willing to have their application reside with, and if they continue to put great weight on the marketing value of the logo on the card. However, there is no particular reason why this should generally be the case. The market may yet offer consumers ‘blank’ smart cards, just as it offers blank floppy disks and other large capacity disk drives, so that consumers can decide for themselves which applications they will risk putting on the same card. So, for example, someone who is a health care researcher with private health insurance may put her library card application on a different card from the one on which her health insurance application sits, if she does not trust her health insurer not to look at her borrowing history, see that she has been reading about AIDS for her work, wrongly conclude that she is a higher risk than they had thought and thereby increase her premium.

Because many consumers will not have reader devices at home which will enable them to access data held about them on their smart cards, there is a risk that, unless arrangements for real time access are introduced commercially or, failing that, by regulation, a whole range of privacy violations could occur. For example, inaccuracies could creep in as data on cards and centrally held databases diverge or updating fails to take place as cards are read and written.

However, with a kitemarking system for levels of security, with consumer owned blank cards and with arrangements for real time subject access, there is no reason why smart cards could not prove to be a powerful technological force for greater individual control over personal information. Smart cards as such do not present privacy risks, but the ways in which we choose to use them do.
Technologies of insecurity: hacking and information warfare

All information and communications systems are open to unauthorised access and deliberate damage. The spectrum ranges from theft of free telephone line time (‘phone phreaking’) through to ‘I-war’.87

The minimal form of attack is mass e-mail attack, often weighed down with additional embedded garbage information, in order to bring a server to a halt as a result of simple overload. This is sometimes organised by social movements in protest against certain governmental and business activities and usually results only in temporary disruption.

Hacking in its original sense88 – the unauthorised access to computers by individuals, has become the lifestyle and habit of a community of people with a dissident political culture ranging from anarcho-egalitarian to anarcho-libertarian in its occasional public expressions, some being on the fringes of organised crime. The community holds both physical and virtual conferences, maintains web sites and produces and distributes hardware and software. Members are occasionally hired by security forces and commercial security teams to test systems to destruction or to carry out particular kinds of design work. The purposes for which unauthorised access is gained are various, but some are more interested in demonstrating their ability while others in acquiring commercially or militarily sensitive data that can be sold.

The writing of viruses or malicious software distributed unofficially over networks, on disks and by other means that may do little more than annoy or may do serious damage to data or processing capacity appears to be a relatively common affair. The motives of virus developers are not well understood, nor are their numbers known with any certainty. However, the Internet has become a major means by which their work is distributed.

‘Phone phreaking’ (the fraudulent theft of telephone line capacity) is growing, partly because many criminals prefer for reasons of their own security to clone someone else’s telephone identity and constantly to change the numbers from which they appear to make calls. Some of the hardware on sale and in use for this purpose is very sophisticated and new products are constantly being brought out.
Weaponry more likely to be used by sophisticated terrorist groups or military personnel engaged in special operations intent on causing greater damage includes High Energy Radio Frequency (HERF) guns, which can, used at short range, incapacitate computing equipment temporarily or permanently by damaging circuitry, and Electro-Magnetic Pulse Transformer (EMP/T) bombs, which is a more powerful version of the HERF technology.

Certainly, the risks of attack in these various forms are probably greater than some of the more complacent imagine, and the preparedness of the security arrangements in government agencies, in private firms in the financial services, utilities and other leading sectors to respond to them is less than might be hoped. There are probably many more unreported attacks than reported ones. Corporations fear for the impact of such reports on their share prices and, in the case of banks, for the impact on confidence in the financial system as a whole.

However, what is perhaps remarkable is the limited damage that has been done to date and the generally low technology approach of organised crime and terrorist groups in designing attacks on civilian systems in the developed world. Once again, technology does not determine history and privacy is not simply a residual left behind when technologies of insecurity have done their worst. Just because something can be done, it does not follow that someone will do it. While the cultural dynamics of the social world of hackers, phone phreaks and virus writers are not well understood, it is not obvious that, because these movements exist, privacy will decline any more than the existence of organised crime means the collapse of law and order. Indeed, there have been cases where companies’ hiring of hackers and phone phreaks has resulted in those individuals providing useful services and becoming rather less disaffected with the corporate world they affected to despise or loathe. Just as movements can spring up quickly, they can also fade away, not least when a better offer becomes available, as was the case with the 1970s Citizens Band radio cult.
Technologies of identification, authorisation and anonymity

In many contexts, people are required to prove that they are authorised to be somewhere, have access to something, are entitled to a particular service, or are entitled not to be treated in some way they would prefer to avoid. In some of these situations, it is considered necessary for the purpose of establishing authorisation to prove one's identity first.

In fact, the boundaries of where it is and where it is not necessary to show true identity shift over time as cultures among citizens, governments and businesses change. In many situations, true identity is revealed but the information is not used to add much to other authorisation procedures. For example, when drawing cash from one's bank account with a traditional magnetic stripe card in an automated teller machine, the personal identification number (PIN) is the principal means by which authority to withdraw is established. Some card reader systems also take the name of the cardholder from the card, revealing identity but this is little more than a routine check. If someone has the PIN and the card, then they have that identity and they have the means of establishing authority to withdraw, even if they have stolen the card.

In many administrative and commercial contexts, it is not necessary for the purposes of the transaction that the person processing it knows the true identity of the individual whom the transaction concerns and there may be good privacy grounds – based on dignity rather than liberty or justice – for wanting to prevent routine access by processing staff to true identities. For example, a public auditor in a National Health Service hospital may need to check data on operations performed in theatre, in order to determine whether the use of the theatre represented value for money or whether the finished consultant episode relating to an individual patient was fully accounted for from admission to discharge. However, to complete that task, there is no need for the auditor to learn that the hysterectomy performed on the 14 May 1998 was that of Mrs Joan Smith of 10 Acacia Avenue: after all, the auditor may live at 12 Acacia Avenue.
While law enforcement agencies prefer to work with true identities on all occasions, there are occasions even in that context when true identity is not necessary. A simple check on a driving licence conducted in order to test whether a person has the right to drive a car does not require that the police officer needs to know the person’s identity.

However, for situations in which true identity is considered necessary, a PIN is the most elementary and vulnerable form of authorisation procedure and at best a very primitive form of automatic identification (‘auto-ID’) procedure. Recent developments in biometric technology enable much more rigorous tests to be conducted in real time.

**Biometric and dynamic recognition technologies**

There are two categories of automatic identification technology. Encoding systems pre-label something – a card, a chip, a piece of data, an item in a store – in a form that can later be read when the item is passed through a transaction: essentially they add a feature to the item. These include optical technologies such as barcodes and their more sophisticated derivatives, optical mark reading and optical character recognition; magnetic technologies including magnetic stripes on cards; electronic technologies such as radio frequency identification used in contactless smart cards or touch memory systems used in contact smart cards; and charge injection systems which apply a charged area to a piece of plastic.

Feature extraction technologies examine something – for example, a person, some part of their anatomy, physiology or functioning – and identify it from some distinctive features against a database of their distinctive features. Examples include biometrics such as retina or iris scans; fingerprint and palm print recognition systems; hand geometry, vein pattern or pore pattern recognition; recognition of facial structure, patterns of heat on the face, facial vein pattern, and in future perhaps recognition of ear shape or even characteristic body odours; action-related techniques such as recognition of a signature, a ‘dynamic
signature’ in which the way in which characters are written is observed and recognised, recognition of speech or keystroke dynamics.

Even biometrics and dynamics are not wholly fraud-proof, although they are more expensive to defeat than simple systems using PINs or human comparison of signatures.

These systems can be used both to protect and undermine privacy. Clearly, their use to exclude unauthorised people from access to data would be a privacy enhancing use. But there are risks. For example, although in most biometric or dynamic systems currently in use the individual is aware of the scanning, there are contactless scanning systems available that can be applied without the person being aware that data is being collected about them and analysed. If they have given prior consent to such random scanning as part of their contract with the agency using the techniques there may be no great issue but, where no such consent has been given, there are privacy concerns on ground of dignity and potentially also of justice.

There are risks of unauthorised disclosure if data collected from individuals is not kept securely: imagine a conference to which admission was on the basis of retinal scans but where the data from the reader device was not kept secure or was disclosed casually. Many people would feel that they had given such data in confidence and would not want it being matched with other data about them by anyone capable of doing so.

Risks of unjust inference – typically unjustified refusal to accept true identity – can arise if the systems are designed to allow too few degrees of freedom from the original template stored in the database for comparison. For example, signatures and dynamic signatures change over time and facial structure changes with age. Moreover, biometric and dynamic recognition systems are not wholly error proof: few systems yield a 100 per cent recognition performance against a template: setting the error tolerance too low for the purpose can also bring risks of unjust inference. As smart objects begin to proliferate during the early years of twenty first century, it may be possible to introduce cars, computers, personal organisers or refrigerators that will only open or function for authorised people. If too few or too
many degrees of freedom or error are permitted in such systems, risks from inaccuracy arise that may allow people not supposedly authorised to use them. In turn, this creates risks of disclosures of personal information and also of unjust inference.

**Digital signatures**

If electronic commerce is to achieve its potential volume and economic importance, businesses and individuals need to feel that they can rely on contracts made across electronic networks. Even within the same organisation people need to be able to feel sure that a document purporting to reflect a decision made or a view taken comes from the source it claims to. These needs are generally known as non-repudiation and authentication. In traditional face-to-face or paper arrangements, a simple signature in pen at the appropriate place is accepted for most ordinary purposes as sufficient guarantee of both things – a symbolic behaviour underpinned in British law largely by custom and practice. Where this is no longer possible, some digital equivalent is required. But the means by which digital signatures are implemented are also means of securing privacy.

Technically, there are various options. Public key cryptography provides a straightforward form of digital signature because, if you receive a document from me that you can decrypt using my public key, then you know that it could only have come from me as only I possess my private key. In this way, a digital signature can therefore be used to enhance privacy. There are other systems such as the use of one-way hash functions on documents that can be examined for certain features that will be peculiar to the genuine author but not themselves decrypted.⁹⁰

However, in countries where strong or public key cryptography is not legally permitted to businesses other than specially licensed groups such as banking clearing house systems, digital signatures have at best doubtful legal status, depending on the exact framing and drafting of the law. The earliest digital signatures legislation, such as the Utah model, provided for the legality of such uses of public cryptography
but set in place a mandatory key escrow structure which, as we have seen, has problems of its own.

**Privacy enhancing technologies: pseudonymity and anonymity**

We have seen that in many situations, transactions can be processed effectively without as much personal information being made available by one party as is often routinely offered or required. The card authorising me to access a building need only declare that the bearer (perhaps verified as the authorised card bearer by means of a biometric) has the right to enter, but need not declare my name, address or driving licence endorsements. Similarly, when I pay for something using a debit card, the store need only be given an authorisation that there are sufficient funds in my account to cover the cost, but need not know my current balance or my credit rating.

Any system designed to reduce as far as possible the volume of personal information that is revealed in the course of a transaction on the ‘need to know’ basis may be regarded as privacy enhancing, although clearly some systems go further than others. The key development in privacy enhancing technologies (PETs) has been the development of secure and effective systems of identity protection or the use of pseudonyms wherever true identity need not be revealed to a particular user of the system or, in some cases, to any user. Privacy and security are not the same thing. While security may be an additional benefit of a PET, or a means of achieving the confidentiality afforded, not all secure systems are privacy enhancing: they may allow personal information to flow freely across transactions but simply exclude those who lack the means to decrypt or access the data.

A good example of this comes from the system used in some advanced electronic cash applications such as David Chaum’s Digicash™. This is an electronic cash system which offers a high degree of both security and privacy. To achieve this, it uses a ‘blind signature’ to encrypt the cash stored on the smart card, which is a digital signature to authorise a transaction. The true identity of the signer is
not revealed to the other party in the transaction, whose interlocutor remains anonymous. However, only in the event that someone tries to cheat the system and spend the same e-cash twice, does the system release details of the identity of the fraudster. Another simple example is the web site www.anonymiser.com which provides anonymous intermediary services to its clients.

In effect, well-designed privacy enhancing systems cordon off true identity and other types of personal information not strictly required for the purpose of the transaction. The willingness to design, purchase and implement PETs varies enormously among different cultures: a study in the Netherlands and Ontario found a much wider take up in Dutch business and government than in Canadian. This may simply reflect differences in the distribution of knowledge about PETs or it could reflect deeper cultural assumptions about the dynamics of expenditure on such systems upon the competitiveness of firms, or deeper cultural assumptions of liberal and civic republican traditions within the different national balances in the two countries.

There are now some models of fully privacy enhancing systems in operation in the Netherlands, which demonstrate the case that, if these are part of the original system design, the cost increment over a less privacy respecting system is negligible.

Technologies of transaction

Electronic money: accounted versus near-anonymous versus anonymous schemes

Most money is now electronic. Credit and debit instructions from cards and tills pass to banks and other institutions routinely: near-monies such as the more liquid traded stocks and other financial instruments are a growing proportion of the world's money.

Notes and coins are a declining technology, principally because they are so costly to use. Security for notes and coins in the form of banks vaults and armoured automatic teller machines to store and handle them, armoured vans and personnel to transport them, and ever more sophisticated watermarking, magnetic strip and other technologies to
prevent forgery represent a large proportion of the costs. Replacement
costs for worn out notes and coins are also significant. The costs of soap
and detergent to clean up the bodies and equipment of cash handlers
and their systems after a day’s takings should not be forgotten either.

Electronic purse applications are the next generation and are of part-
ticular interest in the field of retail sectors and in small transactions
work generally because they will replace cash, perhaps sooner than
anyone thinks. Already governments and businesses around the world
are asking their citizens and customers not to pay them in notes and
coins, even though they issue them, preferring the cheaper, cleaner and
less bulky digital alternatives.

There is a distinction between unaccounted, partially accounted and
fully accounted schemes. In a fully accounted scheme, as in a credit or
debit card account today, each transaction is recorded and an audit trail
assembled, which can be read at the appropriate time and used to build
up large profiles of individual account holders’ spending, to be analysed
for the issuing banks’ own commercial purposes. Visacash will be one
such fully accounted electronic purse scheme. Many regulators feel
strongly that accounted schemes are the only means by which it will be
possible to prevent the cyber-cash world becoming the principal haunt
of organised crime and money laundering.

Unaccounted schemes emulate pure cash in anonymity. In the pure
form, no audit trail of transactions is collected at all. They preserve
privacy in transactions as well as notes and coins do.

There is a variety of partially accounted schemes. Mondex offers,
for example, an audit trail that can in certain situations be recovered,
tracking the last ten transactions. DigiCash offers a system that is
completely private until someone tries to abuse its system to spend ‘the
same’ digital money twice, in which case the software can issue an
audit trail and transaction identification at the point of sale.

Another alternative is an unaccounted scheme, but with a ceiling on
the value that can be stored at any one time on a card or a limit on the
total value of transactions over time. These measures would make
such schemes much less attractive to organised crime as vehicles for
money laundering or forgery of value.
The great unknown about the future of electronic purse schemes is the extent to which consumers want privacy and what they are prepared to pay for it. Unaccounted schemes are more expensive to consumers and retailers because issuing banks are often less willing to finance reader machines for retailers. Some may be prepared to pay between 3 per cent and 10 per cent for anonymity but not more, it has been argued, not least because accounted schemes offer another kind of proof of purchase. A risk with traditional cash and with wholly unaccounted schemes is that lost money cannot be recovered. Many people may be prepared to pay a premium for an accounted scheme if they are offered some possibility of recovery of value on loss, as the present credit card schemes offer, by cancelling lost cards and issuing replacements. However, this shifts some of the risk for loss on to the card issuer and, as theft of electronic value becomes a more profitable activity, issuers may charge higher premia.

A second problem for unaccounted schemes is that because issuers do not collect data from each transaction, it is not financially worthwhile for them to finance the investment for the reader machines in the millions of retail outlets in which they would be used. Finance houses and other companies offering accounted schemes, however, need that data capture capacity and may be willing to provide financial help to the retail sector.

Should we accept demands from fraud police and financial regulators that only accounted schemes be offered to the public? Certainly, we should resist any temptation to panic about e-cash. Unaccounted notes and coins have been used for millennia during which fraud and money laundering have been contained. Certainly, the costs of investing in equipment, software and skills capable of forging significant amounts of stored value are quite large to the forger. Although the costs of today’s technology may fall, this is an arms race, just as the watermarking, metals, magnetic strips, inks and other counter-forgery strategies of traditional mints have been. No doubt cryptographic systems and other software foundations of electronic purse schemes will improve and there is every prospect that the rising cost curve for forgers of matching issuer’s technology can be maintained.
Thus, the future direction of privacy in the global market in electronic purse schemes is hard to predict. While conventional economists are confident that consumers will neither want nor, in large numbers, be offered private, unaccounted schemes, there are clearly segments of the population for whom transaction privacy is very important and who may be prepared to pay some premium for that facility. Moreover, conventional phone card schemes are entirely unaccounted and popular. What remains uncertain is just what kind of electronic purse scheme majorities of the developed world’s populations will want and what price they will set on privacy of transaction.

Private monies: trust and ‘forex’ agent software

The new retail loyalty schemes, air miles, and many other voucher-style schemes, and at the margin, Local Exchange and Trading Schemes (LETS) are creating new private monies that are not backed by any state central bank, but dependent on the profitability of the issuing corporation or group and its commitment not to issue too much near-money to create inflation in its quasi-currency.

It is becoming increasingly likely that these private monies will not remain under the control of the issuers and so it will no longer be possible to direct individual and named, accounted consumers to purchase only the goods and services of the issuing group or its strategic partners. They are already becoming fungible. ‘Forex’ systems, initially based informally on barter, are emerging, including on some Internet sites.

The implications of this new fungibility are potentially enormous. The first is the simple loss of issuer control of accounted money schemes. One simple consequence might be that issuers will decide that once they lose control of the uses to which their currencies are put, they will cease to find it so attractive to issue them at all and will withdraw them as, only one generation ago, large retailers withdrew from the Green Shield stamps scheme. Private monies could simply be a cyclical phenomenon of experimentation, short run competitive advantage eroded by rising costs from increasing competition of the
discounts and other carrots for a relatively small gain, followed by withdrawal.

But there is another scenario. Private monies may continue to grow, because there are network benefits for corporations to issuing them. Much as it benefits the largest software companies to give away some software free and recoup the costs through later subscriptions, support and other software sales, and through the dissemination of the brand image, so companies of all kinds may find that it is in their interest to have their currencies circulate globally. Indeed, it is possible that consumers may come to trust them at least as much and, in some cases, more than state currencies that are particularly vulnerable to inflation due to over-issue.95

In that case, people will gradually get used to the idea of thinking of their net worth measured in a 'basket' of currencies, only some of which are state backed. This will bring major new trust problems. The key issue will be that most people will not want to be constantly watching the forex markets between air miles and supermarket card points schemes and the pound sterling to work out which is the best currency to pay for a particular item with. They will want software agents that crawl the nets to find the best deal, trade on their behalf and make the decision for them. The key question for trust is whether that software will be unbiased or not. There have been protests about particular software systems used by travel agents to select flights and hotels in the holiday industry, claiming that they were systematically biased in favour of a certain US airline. Clearly, people will want to feel absolutely sure that the software agents managing their electronic money from their smart card in their digital television, personal computer or mobile phone, is honest, unbiased and acting only in their interests.

In this scenario, of course, control passes from the issuer, who began with an accounted scheme with benefits specially tied to purchase of the issuer's main services, first to the more sophisticated consumers and finally to the issuers of software agents that manage forex transactions.

The key issue for privacy here is that privacy enhancing technologies are not, as yet, being sufficiently designed into set-top box systems
and software to manage these currency transactions. The risk is that people will expect to be conducting transactions using these electronic monies over digital television based systems that are at least as private as conventional banking or payment, but in fact they will be much more readily observed by third parties.

**Technologies of data manipulation: matching, mining, profiling**
Data handling technologies are becoming more sophisticated at a rate that defies any attempt to analyse or summarise developments for the technically uninitiated. However, relational and now object oriented database software systems enable the analysis of data in ever more fine grained ways and the matching of data across different data systems, such as geodemographic databases, transaction data and questionnaire data where some means of identifying individuals or households is used or found. Software tools exist that can also crawl the World Wide Web to find additional data to match and then build profiles of particular individuals. Data warehousing systems now exist to handle very large volumes of transaction data or combined data types going back many years and handle it for analysis in times far shorter than those of which data management systems were capable even a year ago.

The levels of accuracy in crude matching by name using large databases is poor because of the significant numbers of people sharing common names and the quality of data in respect of accuracy, being up-to-date and so on. However, there is steady progress being made in the development of automatic procedures for weeding and sifting these ‘raw hits’ to reduce them to manageable numbers of putative matches before a final decision on a match is made.

**Technologies of distribution: push, capture, target**
Typing in the address of a web site and collecting information from it requires the active choice of the computer user to ‘pull’ down information from a site chosen specifically at that point. By contrast, conventional television, unsolicited mail from direct marketing companies
and subscribing to an e-mail listserve or usenet group involves little specific active choice on an item-by-item basis, because the media ‘push’ content at the user. In a push system, material can be updated from servers without a new connection being opened up every time a client chooses or remembers to update and the transaction traffic of requests and replies is reduced. Moreover, push systems achieve multicasting or narrowcasting, without the lack of discrimination between users involved in broadcasting.

We stand on the verge of a major transformation of media by new kinds of ‘push’ technologies, by which software will search, select and deliver content from a wide variety of media to the individual, using neural nets to model preferences. Individuals will ‘train’ their neural nets by expressing preferences on content offered to them, until such time as the systems collect and offer only the kinds of material that the user is interested in. The ambition of the direct marketing industry is that push technologies will deliver the ‘marketplace of one’ and that private contracts offering a guarantee of confidentiality of data collected will suffice to reassure any anxious consumer. The commercial possibilities of push systems give media and information companies new reasons for wanting access to the profiles of the interests, tastes, past behaviour and attitudes of individuals that will be assembled by the new generation of sophisticated push technologies.

Because many push systems will be international, it may be difficult to enforce existing data protection laws in the destination country on the disclosure of these kinds of material in the source country, particularly if – as seems likely – that will often be the United States. Moreover, it is not clear that all implementations of push technologies will offer the individuals who are the subject of these profiles the opportunities to correct their profiles and control what the software actually learns about them.

**Disciplining technologies for privacy**

New information and communications technologies generate impulses to create new professional and institutional practices for their use and
privacy has slowly become an important part of this wider process of the emergence of institutionalised information ethics. Here we consider briefly the professionalisation of the computer industry and a recent Internet kitemarking initiative for privacy.

**Professionalisation in computing**

New professions in information and communications systems are emerging. Often it will only be professional software writers and designers, protocol designers, cryptographers, systems analysts and the like, who will know whether violations of privacy are occurring or what the risks of violations are; in many cases, only professionals will know just how trustworthy the institutions that operate upon and regulate information networks are.

Yet many such professions have not typically developed sophisticated codes of ethics, systems of accountability other than to those who hire their services or systems of support for whistleblowers, nor have they achieved such closure of access to jobs that ‘rogue’ operators can be identified, excluded or disciplined effectively. In short, they are not yet self-regulating monopolies in the way that traditional professions such as medicine, dentistry or legal practice are.

There are vexed questions about the desirability of such developments. Critics of professional power and restrictive practice point to the self-serving character of most professional codes and the feebleness of their real disciplinary effect, while advocates regard the professional ethics as a valuable, if imperfect, contribution to building ethical frameworks for practice. Moreover, there are questions of feasibility. Professions are traditionally organised, regulated and licensed nationally, but the nature of modern information systems is that they transcend national frontiers. There are few, if any, effective, international systems of ethical discipline upon professionals that do not rely on effective national systems.

**Truste™**

One important recent development towards trust based competition has been the introduction of an Internet kitemark for sites and companies
to apply for, indicating that their information ethics and privacy compliance systems meet certain basic standards set by a private standard ‘franchising’ agency. The system is now known as Truste™. Run by an independent, nonprofit agency, it offers an accreditation system and the right to put the Truste™ logo on a web site’s home page, provided they have adopted a privacy policy and make a copy available to site visitors on clicking the Truste™ icon. The statement must provide the visitor with details of the type of information the site gathers, how it uses it, with whom it shares the information, whether the visitor can opt out of having the information collected, used or disclosed, whether they can change or update information once it has been disclosed and whether they can remove their entry from the site’s records. Members of the scheme agree that their sites will not monitor personal communications such as e-mail or instant messages except as required by law or insofar as it is necessary to maintain the site.

The kitemarking agency conducts seeding of members’ web sites with dummy information and commissions audits from leading accountancy and audit firms and inspections of its members’ compliance. It has not yet been adopted on a large scale, but there is growing interest in the kitemark. Third party audit plays an important part in such schemes in securing public trust.

The economics of surveillance and dataveillance

A key shaper of the future of privacy will surely be the real costs of surveillance and dataveillance to business and government agencies, the net profit yielded from this activity in the private sector and the net ‘public value’ yielded in the public sector by comparison with the costs of introducing and using privacy respecting or privacy enhancing technologies.

It is not possible to make a definite assessment of the balance of these costs and benefits across industries. There are several reasons for this. One is that the cost trajectories of technologies such as smart card and reader device systems are affected hugely by the level of take-up which in turn is affected by cultures of privacy and public trust in
issuers. Secondly, even if we could reliably estimate the rate at which costs fall on today’s data processing mechanisms, no one can know how quickly they will have to be replaced by new and cryptographically more powerful systems or algorithmically more complex systems. And that in turn depends on the future of regulation of encryption.

Certainly, we can say that the simple story told by some privacy fatalists that costs of dataveillance are uniformly falling cannot be squared with the information that we have heard from businesses and public agencies in the course of the research for this study. Even as the costs of data capture fall in some retail sectors, partly because of automatic assembly of databases without costs of manual high data entry having to be incurred, the costs of manipulation, analysis and targeting are not falling nearly so rapidly. True, off-the-peg software for database manipulation is becoming more readily available and cheaper, but the skilled personnel to use it and use it well are not. The computer press has been reporting a global skills shortage for some years now, despite the frequent stories of the cheapness with which programming and database work can be contracted to Bangalore and Guangdong.

The costs of short key cryptography software, affected as they are to some extent by national state regulation, US export controls and the like, may tell us rather little about the cost trajectory over time of longer key systems. Similarly, while rapid progress is being made in the embedding of cryptography in a variety of ‘smart objects’, the fundamental trust dynamics involved in transactions that require taking a public key, trusting the other party’s private key is not compromised, signing one key with another, and so on are very large and require skilled, trained and astute staff to operate them safely when large sums are at stake. The costs of hiring and training such staff are not likely to fall nearly as rapidly as the cost of the software.

In the press coverage of the introduction before Parliament of the Data Protection Bill 1998, there was extensive debate about the costs to industry of implementing the legislation. Estimates ranged from £0.8 billion to £2 billion. The true figure cannot now be known. It is certainly true that introducing systems of pseudonymity at least to certain categories of user into databases that have already been
designed to work with true identities at all times, are much greater than the costs of designing privacy enhancing measures into a database from the beginning. However, it is possible that research and development in this area may reduce these costs.

**Conclusion**

There is a vast array of new information and communications technologies that are transforming the collection, processing and use of personal information. Powerful as these techniques are, and much as they exacerbate some privacy risks, they do not alone determine the future of privacy. The costs of introducing and operating these systems vary widely and it does not necessarily make economic sense for businesses to invest vastly in technologies for collecting, processing and disclosing personal information unless they are confident of the value of the processes. Moreover, there are technological choices. Privacy enhancing technologies can now be designed into many kinds of systems and, if this is done from the earliest stages, the additional cost implications are minimal. Finally, technologists are beginning to recognise the importance of securing trust and have started developing new institutions for this, ranging from professional codes of practice through to kitemarking schemes. They have also started debating much more openly the risks for public trust in information and communications technologies if the systems of regulation on offer have ‘back door’ access to law enforcers but at the price of commercial and public trust in the privacy they provide. Some privacy activists feel that information and communications technologies are intrinsically hostile to privacy. This is a fatalistic view that is simply not supported by the evidence.
In this chapter we turn to the executive functions of government. First, we examine the role of the public sector as the assessor of risk. Then we turn to the implications of the emerging paradigm of public management in which integrative and preventive activity is the priority rather than the focused, functionally organised processing that dominated in the era of ‘reinventing government’ in the 1980s and early 1990s.100

Holistic and preventive government – a threat to privacy?
The emergence of new tension
Pressures for cross-departmental and cross-agency working are increasing. The agenda of the 1980s was that of fragmentation by function, and increased managerial focus on those functions, while in the late 1990s, the ground has begun to shift radically. For generations government has been organised around functions such as medicine, policing and criminal justice, social work, law, cash benefit administration, land use planning and so on. While some functions have been formally brought together in gigantic ministries, they remain separate within those ministries for many purposes. Budgets, auditing systems, systems of financial accountability and spending control, information systems, parliamentary supervision, recruitment, promotion, and
career development are all organised around functions. However, increasingly the ‘wicked’ crosscutting problems – ill health, unemployment, poor educational achievement, crime, environmental degradation – cannot be handled in this way. Recognising this, governments have begun to innovate by developing more holistic systems of budgeting, management and information management.

A debate is now opening up about how protection against privacy risks can be made compatible with the need for more holistic problem-solving government. One implication of this is that there will be a pressure for much greater sharing of personal information between agencies and departments of central and local government. For much of the post-war era, many people have fondly imagined that the most effective protection for their privacy vis-à-vis government is the poor coordination, inefficiency and weak data management of the public sector. If the promise of integrated information systems to support holistic governance bears fruit, then we shall have to look to other kinds of protection for privacy against government.

Demands for more matching and mining across departmental boundaries to detect fraud are also increasing. In this context, it was only to be expected that the government would examine the possibilities for removing some of the firewalls in the network of public sector data systems – as it announced in the 1996 green paper, Government.direct.101

The issue is important not only in fraud control, but in the management of risks presented by convicted persons, where joint coordinated arrangements between the probation service, relevant local authority departments, the police and others increasingly involve the sharing of ‘soft’ personal information.102 While confidentiality is supposed to be maintained within the group of agencies sharing information and subject access is granted,103 the kinds of information recorded and shared are very wide indeed compared with the restrictions in data protection law for conventional situations; for instance, official record-keeping on convicted persons is subject to a number of specific exemptions from data protection law.

Broadly, several options seem to be opening up. All firewalls within the public sector could be removed but in practice, no government is
likely to take such enormous risks with public trust and public fears. While the public – it became clear in our qualitative research – is not particularly confident about the present firewalls insofar as people are aware of them, public confidence would almost certainly plummet if they were explicitly removed. It is possible that specific firewalls can be removed, and some purposes for the collection of personal information by public agencies redefined. In addition, more detailed codes can be developed to control the situations and procedures under which matching and mining across governmental databases might be permitted.

Difficult conflicts are likely to emerge, not only with the public, but also between the very different information ethics of public sector professionals. Whereas general medical practitioners have a code of confidentiality of a strictness that makes the consulting surgery the equivalent of the priestly confessional, police officers, social workers, housing managers and teachers have more relaxed principles about the situations in which disclosure of personal information about clients may be acceptable.

However, there are other forces shaping how executive government handles personal data. As in business, the role of information technology professionals, and their codes of ethics, are important, but still poorly developed. Government is traditionally poor at providing frameworks in which whistleblowers can exercise their ethical responsibilities.

**Purchasing, private finance and contracting**

The fact that much personal data handling is now contracted to private businesses raises new issues of enforcement of data protection. In general, data protection is not a well-developed element in the output and outcome specifications of many contracts issued by public bodies, and there have been occasional scandals when contractors have made unauthorised disclosures. It is still not clear whether contracting out of public services will prove to be the means by which more holistic government is delivered. Contracting out contributed to fragmented government by the various ways in which many contracting systems have
identified who is responsible for what. Is privacy primarily the responsibility of the purchaser or the provider, or does it depend on a particular contract?

The advent of contracts for the provision of public services in which the private sector provides the capital raises new privacy issues. Traditionally, in such contracts the public sector either hypothecates all or some part of the revenue from the service to the private contractors or else pays them an income stream from general taxation revenues. However, there are a number of problems with this, which are becoming increasingly apparent to finance ministers and treasury policy makers. Such contracts tie up large revenues for many years in ways that diminish treasury flexibility and may prove exceptionally difficult to sustain at times of future financial stringency.

In some private sector circles, it is now being suggested that a better way in which to secure private capital might be to permit ‘information barter’. Briefly, in return for providing the system, the private sector would be permitted access to certain categories of individuals’ personal information held by public bodies. It is not yet clear just how attractive this would be to the private sector or which kinds of companies would be interested but here is interest in the idea among some contractors. Of course, unlimited access to personal information collected by the public sector would be incompatible with the basic principles of privacy and data protection law. Where individuals provide information on the understanding that it is collected for one purpose, it cannot be made available and used for another, and disclosure to third parties is in generally not permitted or acceptable to the public.

However, there may be categories of personal information where, provided some form of active rather than passive consent system were operated at the point of data collection, this might not prove to be an insuperable obstacle, because the purposes for which the information was collected would not be dissimilar from the purposes for which the private sector would be interested in the data. Consider the holistic package of services to be offered by the public and private sectors to the unemployed. An individual who uses such a holistic information system as part of his or her job search would be offered a choice of
services provided by both the public and private sectors. These would include search engines on jobs of particular types, information about education and training options, career counselling, temporary work agencies and so on. An individual could be offered the chance to provide some personal details that would, if the individual consented electronically, be shared between the public and private agencies offering their services there. A similar system might operate to meet the need for a home, or for care of a sick relative.

In addition, it might be possible to propose a change in the conditions under which certain existing personal data on them is collected and kept, in order to permit private organisations access to certain fields, subject to certain restrictions on use, disclosure and so on. While it would be improper for, say, police records ever to be made available in such financing transactions, it might be that certain data of the type collected in the census and in the electoral rolls, which is already collected by the public sector and made available to the private sector for the development of geodemographic profiling tools, could be offered more cheaply, in more up-to-date form, by such a system in return for capital and expertise.

If such an experiment were to be tried, a number of safeguards would have to be put in place before the Data Protection Commissioner could reasonably be expected to allow it to proceed, including:

- a clear and detailed code of practice on data shared
- a detailed description and delimiting of the data categories to be made available
- a system of active and revocable consent
- named individuals appointed within the information system’s structure responsible for compliance with data protection principle
- systems of real-time subject access.

The future of public purchasing raises important challenges for the public sector in coordinating its purchasing practice and its policy on privacy and data protection. Policies that seek to personalise the provision
of government services conflict with the desire for privacy as anonymity. Those who positively welcome government offering them packages of services on particular events – such as birth, bereavement, unemployment – will presumably accept the necessity for profiling and data sharing, while those more concerned with privacy will be more likely to content themselves with more passive, fragmented government.

**Freedom of information**

Policies of greater openness in government can come into conflict with those of privacy. Governments have been under pressure to make available data which, although anonymised, can without great difficulty be connected to identifiable households, individuals or families. Electoral register information and census data have long been the basis of many privately published and sold database tools for marketing purposes. In many countries, there have been conflicts between social movements and governments over the collection of census data and their publication in the form of geodemographic profiling tools for use by the private sector. For example, in the 1970s in the Netherlands, widespread refusal to provide census information led to the creation of national voluntary campaign body called Privacy Alert.105

The new legislation on freedom of information in the UK will have specific exemptions for information that would be protected on grounds of data protection. It will also provide a right of appeal for individuals who fear that their privacy will be affected by any application under the freedom of information laws for disclosures of information that would identify them or from which they might be identifiable by an applicant in possession of other information. Data protection and freedom of information regimes on time limits, charges, appeals and so on for applications for subject access and release will be aligned for matters of personal information. The Data Protection Commissioner and the Information Commissioner will be expected to work together on complex interlocking cases.106

However, there remain tensions between data protection and the freedom of information regime proposed by the Labour government.
In particular, under the freedom of information provisions people may apply for disclosure of information that would breach the duty of confidentiality that a government agency owes to another individual because personal information about that other individual would be released if the application were granted. An individual whose privacy would be breached could appeal against an impending disclosure but would have to show, over above a breach of the data protection law, that ‘serious harm’ would be done to their interests. While this clearly weakens the power of data protection law in public sector contexts, it is not yet clear just how burdensome the ‘serious harm’ test will be for people seeking to ensure that freedom of information for others does not harm their privacy.

**Government as risk assessor**

A growing role for the public sector in many countries, including Britain, is that of providing risk assessments to other agencies. Many of the activities of public agencies involve the collection of detailed information on individuals that is of great commercial value to private companies which must bear risks in relation to the same individuals.

The education system supplies references on its former pupils and students to employers, both in writing and verbally. In the near future, all school children in the country will be given computerised identification numbers to allow tracking of academic performance from age five onwards.107

The National Health Service, and general practitioners in particular, are under steady and constant pressure from employers to assist them in managing their risk through their supply of certification to authenticate the integrity of employees’ claims to good or poor health. During a 1997 strike among British Airways staff, for example, many employees chose not to strike but, unwilling to cross picket lines, took time off sick; the management response was to put pressure on GPs to provide sick notes on a daily rather than the usual weekly basis, which the British Medical Association (BMA) resisted. In such cases, the accountability of the public account holder to the client is sorely
strained. In other cases, public sector bodies help to manage risk for other agencies within the public sector, as we have seen in the context of fraud control.

The public health role of the medical system in preventing and controlling disease means that there is extensive reporting of the incidence of certain conditions and, while in many cases, this can be done anonymously, there are growing numbers of health risks where there is pressure for identified reporting. This disclosure raises a number of concerns for patients and medical practitioners. The proposal from the NHS Executive for the creation of NHS Net, a central information and communications network for the entire service, arouses the opposition of the BMA on the grounds that it would present risks of unacceptable violation of individual confidentiality of patient records and unacceptable centralisation of information through data matching and mining.108

Some insurance companies would like to collect medical information from doctors without patients being informed but the BMA strongly advises doctors to inform patients. While doctors do provide insurance companies with some information on request and with the consent of patients, there remains widespread concern about the large scale acquisition of patient records that could be sold for database marketing to insurance companies, pharmacies and other industries. There would be great commercial value to insurers, commercial pharmacy interests and similar businesses in NHS databases containing sensitive information on matters like sexual health, drug use, terminations, marital, emotional and psychiatric matters.

The public places great trust in doctors’ and the NHS’ handling of personal information but it is still not clear just what kinds of disclosures within the NHS would be generally acceptable. For example, NHS Net would enable hospitals and GPs to interrogate, search, match and copy each other’s records on shared patients. The original conception that all medical data would be open within the ‘NHS family’ but the BMA has resisted this. It argues that records should be open only to doctors, for specified purposes, and that there should be an audit trail of access gained to any medical record showing its purpose, destination
and use. Some people might be content that GPs should have access to their hospital records but not that hospital consultants have access to GP’s records, despite the obvious usefulness to hospital staff in many situations of having more information about a patient in order to assess the risks of side-effects and malign interactions between concurrent treatments.

A recent major study of the role of police officers in Canada, concluded that much police work is centred upon the management of risk for a wide variety of private agencies. Police reports on incidents are often routinely supplied to insurance companies and owners of land and other property. Collaboration with banks and other financial services institutions in the flow of personal information in connection with incidents of alleged fraud is mandatory and routine. Verbal and occasionally written reports are supplied to school staff and even parents in the context of disciplinary issues for minors. References are supplied to employers, information on missing young persons and alleged paedophiles shared with social services and information on people suspected of social security fraud shared with benefits authorities. Legal controls on the flow of personal data typically provide wide exemptions for any data of use in the detection of crime, which is interpreted widely by police officers, and they usually find that more specific rules are enabling and clarifying rather than restrictive.¹⁰⁹

In 1997, following a consultation paper,¹¹⁰ the last Conservative British government introduced a new scheme for the provision of criminal record checks to employers. The new Criminal Records Agency takes data from local and national police records in order to provide registered employers who have adopted codes of practice on confidentiality with either: a simple certificate of an individual’s unspent convictions; a full check including spent convictions and details of cautions for employers involved in sensitive areas such as those dealing with care for children, the elderly or disabled people; or an enhanced check (where local police data other than conviction information can be drawn upon) in the case of jobs involving regular supervised contact with children or in the gambling industries. In the
third category, therefore, soft information of various kinds may be disclosed to employers about potential employees.

**Government as risk manager of last resort**

The current concern with the use of data matching techniques in combating fraud – raised in the 1997 Social Security Administration (Fraud) Act – is one symptom of a rising wider concern with the perceived need to limit moral hazard in public services. It is being felt in connection not only with cash benefits but in health care services, where there are arguments about what levels of service to offer to smokers. Similarly, the public sector is moving toward more holistic forms of detection and risk assessment in coercive family services such as the Child Support Agency and the Child Protection Register database system, which contains data pooled from all local agencies including police, education, health, social services and housing.

If the general culture in public services is shifting to one more concerned about risks of abuse than about risks to individuals from their not receiving services, this will have serious long term consequences for privacy. As local authority social services departments increasingly experiment with matching and pooling data on children at risk, from sources across the authority and other public bodies such as health authorities and using geodemographic profiling methods, there is a real risk that draconian action in individual cases will be taken on the basis of misinterpretation, simple mismatching or excessive reliance on models that predict risk of abuse inaccurately on the basis of apparently correlated characteristics. While many authorities are currently confining the decision making based on such modelling exercises to matters of generic priorities in aggregate resource allocation, it is possible to see a natural line of development into decision making in individual cases. Today, data resources and data handling techniques are available to local authority social services departments which allow them to develop indicators showing the risk of individuals who are not yet parents turning into abusers of their own children. Decisions about keeping such persons under surveillance purely on the basis of such
modelling exercises would raise privacy concerns about unjust inference as well as unwarranted intrusion and reversal of the presumption of innocence.111

Much of the information held by the police, social services and housing authorities on individuals takes the form of allegations, hints, suspicions and other ‘soft’ data. Outside the police service which has specific exemptions, these soft data traditionally have been kept in manual systems precisely to escape the application of the Data Protection Act. The new legislation will extend coverage to manual records. Agencies at the local level have very different codes and principles for the treatment of such data – including over matters of recording, disclosures to third parties and subject access. The risk from more holistic strategies of government is that pooled data on individuals who present risks will become subject to the lowest standards of the least self-regulated.

Increasingly, therefore, a key role of executive government is the management of risk, both for its own purposes and for certain categories of business activity. In carrying out these functions, the volumes of personal information collected, matched, warehoused, manipulated and mined within the public sector and the pressures to disclose to third parties are growing. Perhaps this reflects a shift in the culture of governance away from the liberal toward the civic republican in which the control of risks in the name of safety, precaution and punishment is seen as catastrophic and even risks seen as simply damaging take precedence over traditionally liberal conceptions of individual rights.

Privacy represents a major challenge to trust for executive government as a data user. Where innovation in decision making about entitlement to service or treatment of individuals involves using ‘softer’ kinds of data, sharing data or constructing profiles using data sources assembled for different purposes, the state runs risks with public trust. Inevitably, when data sharing is involved damage to the reputation of the public sector as a trustworthy handler of personal information cannot always be limited to the offending agency.

One contrast between the public and private sectors that emerged from our programme of expert interviews is that the private sector has
taken up and developed codes of practice on information ethics, however inadequately and sometimes complacently, with much greater enthusiasm and sophistication than the public sector. In many reputable banks, insurance companies, direct marketing companies, tele-communications companies and the like, there are data protection compliance officers and agreed written codes of information conduct. There is often great interest and concern at board or senior management level about the privacy issues that can, if they are mismanaged, bring the company into disrepute. The public sector lacks even this level of institutionalised concern. Few local authorities have well-developed codes or compliance staff, although the Local Government Information Unit has developed a code on the use of closed circuit television. Here are some examples of innovation, mainly in the field of criminal justice: the Inner London Probation Service has developed guidance for officers on disclosures of information about their clients to other public agencies, the Association of Chief Police Officers in Scotland has a code on information handling and the Metropolitan Police and London Probation Services have developed protocols for sharing information concerning potentially dangerous offenders.

Nonetheless, in no area of public service has there been sufficient thought about the implications that the changing role and structure of the state – namely more holistic working and more preventive work on safety and collective risk management – will have on information ethics. It is therefore not entirely surprising that many parts of the public sector attract much less public trust than they deserve. For example, although much of the public supports limited data matching in order to identify benefit or tax fraud, qualitative research suggests it is concerned when information from outside the tax and benefit sphere is matched for these purposes. Even policies intended principally for the targeting of services rather than their denial can raise concerns, as in the recent case of data collection for the Department for Education and Employment on the outcomes achieved for trainees on the New Deal welfare-to-work schemes.

Moreover, any creeping distrust about government as data user may spill over into doubt about government as a regulator. For if executive
government is making *ad hoc*, inadequately informed and poorly integrated decisions about the conflicts between and within privacy concerns, it is even more difficult for the privacy regulator in government, with far fewer resources and far less information, to promote a concern for privacy and a learning process about these conflicts across the public sector.

**Serious criminals and holistic risk assessment: the debate about paedophiles and privacy**

A major case study in the conflict between on the one hand, holistic strategies and the role of the risk assessment in the public sector and, on the other, rehabilitation of offenders and the presumption of the innocence of those without convictions, is the recent furore over paedophilia and disclosures.

In 1997, a national register of persons convicted for sexual offences, including those against minors, has effectively been created by earmarking existing police records. Limited disclosure to the wider community is permitted, subject to assessments of the person’s risk of re-offending and using the existing exemptions in data protection law for the prevention, detection and apprehension of criminals or where the prevention of injury to life or health is at stake. However, the register does not include information about other individuals nor is it supposed to include allegations or circumstantial evidence about other possible offences.\(^\text{115}\)

Housing managers, social workers, police officers, probation officers, NHS general practitioners and psychiatrists – each with quite different legal exemptions, data systems and professional codes of confidentiality – may all find themselves in possession of information about alleged or convicted paedophiles. There is increasing pressure upon all of them from politicians, the public and Home Office officials to pool their records and information, however ‘soft’. Social services have specific duties to act on individual cases on relatively soft information in ways that other services would not normally do. For example, social services officers working in child protection cases have been
given legal advice that they are duty bound to disclose to third parties suspicions they may have about persons alleged to be paedophiles but who have not been convicted of any offence, when such people apply for work or volunteering posts in certain settings. For this purpose, some social services officers are beginning to demand some form of controlled access to the soft information held by other agencies. On the other hand, practice varies enormously around the country. There are social services departments that are reluctant to divulge soft information they hold about alleged child abusers to housing departments.

This raises some policy conflicts in the area of privacy that are quite specific to government. For example, should professionals be content to divulge soft information to each other across functional boundaries but not to the public? The parents in the West Midlands and west London who put pressure on housing managers expressly to assure them that they knew of nothing that would indicate that certain individuals presented any risk to their children posed this dilemma very sharply: should public officials be instructed, in the name of non-disclosure, to lie in response to such questions, especially when refusal to comment will be taken to mean that they do have information indicating risk? Courts and the rehabilitation of offenders lobby are generally ill-disposed to disclosure, while the probation service in many areas generally favours it. How does society balance the impulse for privacy and the fear of lynch law on the one hand against the impulse to do everything possible to protect children from abuse on the other?

The Chartered Institute of Housing has issued a policy document to guide its members. Although housing managers are often faced with demands by anxious parents for clear assurances that a neighbour presents no risk, they are not trained in risk assessment in such cases, and they are subject to rules against disclosure of any such information obtained from the police or probation authorities. The 1996 Housing Act and accompanying guidance grant local authorities the powers to prescribe whole categories of people not to be ‘qualifying persons’ for local authority housing – so called ‘blanket bans’. The Institute considers it legally unwise to use this power and counsels authorities to make sure that they make case-by-case decisions.
Certainly, refusing housing to all sex offenders, and indeed any blanket ban, could be open to legal challenge. However, the power is used sometimes to refuse housing to convicted paedophiles and could in principle be extended to persons against whom no crime was ever proven. Moreover, under the homeless persons provisions of housing legislation, a local authority might be able to defend in any judicial review a finding that reoffending by a convicted paedophile could constitute behaviour that made that person intentionally homeless if it were the ground for a possession order against them. Even in such cases, general rules risk falling foul of the Wednesbury principle in judicial review that public authorities may not fetter their discretion.

The Chartered Institute’s guidance to its members deals with some issues of disclosure of information about alleged and convicted sex offenders including paedophiles. It urges local arrangements for information sharing with probation, social services, police and area child protection committees on a strictly ‘need to know’ basis, while housing officers should leave risk assessment to others. The guidance urges that community disclosure decisions should be taken only in extreme situations and normally by the police, in consultation with others, rather than by housing officers, except where local media or others have ‘outed’ paedophiles.

The Association of Chief Police Officers, Association of Directors of Social Services and Association of Chief Officers of Probation have issued guidance on developing local protocols for information sharing, recommending that they should cover definitions of groups of offenders covered, forum for decision making (for example, area child protection committee), risk assessment structure, process of information sharing, level of seniority in each organisation for authorisation of sharing, action following information sharing and suspects’ rights.

The issue of privacy for certain categories of serious offender after release from imprisonment or during probation or other punishment in the community is complicated by the widespread popular press criticism of the professional faith in either the feasibility or the desirability of such rehabilitation. Professionals tend to stress the differences
between sex offenders who represent a significant threat and those who do not.

On several occasions, parents of victims or people who fear that their children will be victims have taken the law into their own hands and in some cases committed vigilante crimes against alleged paedophiles, ranging from illegal eviction through to assault and even attempted murder. There have also been cases of alleged unlawful evictions, threats and other efforts to drive them out. One professional remarked that in a climate of moral panic leading to lynch law which could not be contained or prevented, the choice for professionals was often between making disclosures to direct the vigilantes to those believed by public agencies to be guilty or leaving the vigilantes to choose their own victims on the basis of even worse evidence. Such cynicism may be shocking but it certainly represents one current of professional feeling in this area.

Even beyond the high profile issues around paedophilia, crime control issues – or rather, risk management – have become increasingly central to activities in the public sector that were traditionally largely independent from it. Housing management is no longer purely a matter of solving problems of lack of housing or allocating scarce housing resources; with the widespread demand from tenants for closed circuit television systems (considered in Chapter 8) to control crime, housing management has become ever more embroiled in community safety issues.

**Governance and criminal justice**

Privacy concerns about the state have long focused on the criminal justice system and the risks that its capacities for personal data compilation, profiling and risk assessment present and also the related risks of injustice accompanying privacy violations. This concern is perhaps the oldest in liberal thought.

While political liberals accept the need for an agency that will investigate crimes and detect and apprehend criminals, they fear that such agencies, if not tightly circumscribed by law, will abuse powers by
extending their operations into general surveillance in the name of crime prevention. There have been widely reported abuses by the security forces in the past. For there are civic republicans who consider that subjecting society to general surveillance is an acceptable price to pay for the prevention of risks of at least the more catastrophic types of crime, such as terrorism, murder and other serious offences.\footnote{119}

On the other hand, the liberal tradition does stress the importance of the rule of law as a paramount duty on individuals and organisations as much as upon the apparatus of the state. In order to secure the rule of law against a variety of threats, that tradition has long been willing to endorse or at least reluctantly tolerate a powerful role for policing in surveillance for the purposes of detection on the basis of reasonable suspicion. As we saw in Chapter 6, there has been in Britain in recent years a hardening of popular and partisan positions on the need for tougher systems of criminal justice\footnote{120} and some erosion of the liberal principle that it is worse to convict an innocent person through unjust inference than to sometimes fail to convict guilty persons for lack of evidence that puts guilt beyond reasonable doubt.

The principal privacy concerns raised by policing strategies as follows:

- **Routine surveillance undertaken without connection to a particular investigations.** The procedures and grounds for the routinised collection of personal information by, say, closed circuit television camera (see Chapter 8); for example, there has been a long-standing political liberal concern that the police will collect information on people of dissident political views, not in connection with any particular criminal investigation but with a view to the abuse of police powers to harass such people.

- **Routine data matching and mining of data on individuals on a precautionary or speculative basis.** The role of the National Criminal Intelligence Service, put on a statutory basis by the Police Act 1997, is to facilitate intelligence-led policing and to do so by means of holding and maintaining a large database
of various kinds of information about large numbers of individuals who have become known to the police in any kind of way, in order to analyse the database on request to identify potential troublemakers in advance, provide lists of suspects for particular crimes, enable frontline police officers to prevent crime, and so on.

- **Trigger conditions for investigation.** The evidential standard of ‘reasonable suspicion’ of crime that triggers the police duty to investigate, and which then justifies overriding some privacy considerations in order then to assemble profiles of individuals, build up dossiers, match information from a variety of sources, arrest persons in order to interview them for up to a certain maximum period, seek judicial warrants for entry to premises and the like.

- **Process conditions for data collections during investigations.** The evidential standards and other substantive and procedural conditions that have to be met before search warrants for premises, authorisation to arrest persons, authorisation to intercept telephone or other communications, conditions and authorisation procedures for gaining access to national insurance data systems and other databases held by banks and others.

- **Strategic scope.** The legality of entrapment and the *agent provocateur* role of informers and plain clothes police officers working undercover in incitement to commit a crime in order to enable an arrest and conviction to be made.

- **Inference rules,** both in the course of the investigation and during trial, and in particular, the extent to which the rule that someone is innocent until proven guilty is in practice compromised by the way in which inferences are drawn from data of various kinds (financial data, observational and behavioural data, witness reports, forensic data and so on) and the matching of those data.

- **Disclosure rules,** or the principles that govern the disclosure of data collected by the police and other law enforcement
agencies to each other (for example in information pooling through Europol and Interpol in the course of investigating international crime) and to third parties (insurance companies, credit reference agencies, social workers, housing managers and so on), where some of the information held by the police may be ‘soft’, that is, it may take the form of unsubstantiated allegations and suspicions (by members of the public or by police officers) that may turn out to be false, or purely circumstantial evidence that would be risky to rely on in making inferences of guilt, where the information may relate to offences that are legally deemed to be ‘spent’ under the rehabilitation of offenders laws, and so on.

In the context of the criminal justice system, then, it is not always easy to disentangle privacy concerns from wider ‘civil liberties’ concerns about the manner in which policing activities are conducted. While the routine surveillance and disclosure rule concerns are clearly conventional data protection issues, the issues of evidential standards, authorisation procedures for special kinds of data collections, strategic scope and inference rules are concerns about unjust inference in the criminal justice system that merge with wider concerns about the substantive and procedural justice of the crime detection, apprehension, prosecution and punishment businesses. Nevertheless, the development of intelligence-led policing has increased the concerns of many political liberals about these risks of abuse of power and violations of privacy. The subject of rules of evidence and inference from evidence in criminal cases is too large to be embarked upon here. Disclosure matters have been dealt with above in the discussion of holistic government and government as risk assessor and CCTV was considered in Chapter 8. I therefore concentrate the discussion here on process conditions and strategic scope, both of which raise clear and specifically privacy related concerns.

The Police Act 1997 introduced a new system of authorisation for the conduct of surveillance operations in the course of particular investigations on property and for the interception of telecommunications.
Without special authorisation, entry to property to install listening devices would be civil trespass and might also fall foul of Article 8 of the European Convention on Human Rights, although evidence obtained illegally can be admissible in the criminal courts (but judges have discretion to exclude evidence obtained by trickery after the time of the crime if the result compels someone to incriminate himself or herself unfairly and prejudicially)\(^\text{123}\)

The Act makes these kinds of entry and the use of such devices lawful, subject to (in some cases, prior to) authorisation by a chief police officer or in some cases by a commissioner of police. However, it does not set out a general scheme for their regulation or clear criteria for the admissibility of data collected from them as evidence. Authorisations last for three months but are renewable. There are few restrictions on the kinds of activities or targets. For example, it is not necessary that the property be one owned or rented by a suspect. The only requirements are that the investigation be one of ‘serious crime’ (violence, large financial gain, conspiracy or likely to gain a convicted adult at least three years in prison), other ‘normal’ means of investigation must have been tried and failed or be inherently unlikely to succeed, there must be a good reason to think the use of the equipment would lead to an arrest and conviction, the operation must be feasible and the chief officer must be satisfied that the intrusion into privacy is commensurate with the seriousness of the offence.

Interception of mail and telephone messages without consent is governed by the 1985 Interception of Communications Act. This activity is lawful only if authorised by the Secretary of State for the Home Department, who can issue a warrant for two months (which is renewable) in the interests of national security, to prevent or detect serious crime or to safeguard the economic well-being of the UK, provided the information sought cannot, in the Home Secretary’s view be obtained by other means and that the number of people to whom the information is disclosed is kept to a minimum, the information disclosed is kept to a minimum and so on. Copies must be destroyed as soon as they are no longer necessary. No right of appeal or judicial review is now available to a person aggrieved. Material gathered from

---

This page is covered by the Demos open access licence. Some rights reserved. Full details of licence conditions are available at www.demos.co.uk/openaccess
such interceptions is not normally admissible evidence, although the warrant procedure is intended to allow police officers to use the material gathered to lead them to other material that will be admissible evidence.\textsuperscript{124} Cordless, cell and satellite phone systems do not fall within the definition of transmission by means of a public telecommunications system and so no warrant is necessary for interception of the radio signals from them to be lawful; therefore, such material can legally be collected and is admissible evidence.

The European Court of Human Rights recently held that the workplace carries ‘a reasonable expectation of privacy’ and that phone taps at work, even in a private telecommunications system, fall foul of Article 8.\textsuperscript{125} The European Court of Human Rights has also held\textsuperscript{126} that any legislation that empowers signatory states to take measures to counter terrorism, espionage and serious crime, overriding Article 8 of the Convention, must not be undertaken haphazardly without due and proper care. Surveillance must be reviewed and accompanied by procedures guaranteeing individual rights and, while in principle a judge’s authorisation is preferred, with adequate safeguards other agencies exercising effective and continuous control will serve; the French police have fallen foul of these rules.

For centuries, police methods such as entrapment and the use of \textit{agents provocateurs} have caused the liberal tradition anxiety. However, English law does not rule out as admissible evidence, material gathered by trickery or even illegally or by \textit{agents provocateurs}; the only test applied is that of relevance.\textsuperscript{127} Entrapment is not a defense to a charge of any crime, although the \textit{agent provocateur’s} act of incitement to commit an offence that would not otherwise have been committed is itself a crime and in theory a police officer acting in this way could be charged with such an offence. In practice, undercover police officers have been allowed by the courts to do things short of verbally asking someone to commit a specific crime, without prosecution, especially where the activities are necessary to maintain cover.\textsuperscript{128}

In short, the principal privacy risks that many people fear in connection with the use or abuse of police powers are those of physical intrusion, disclosure without consent, function creep, excessive surveillance
(that is, disproportionate to the purpose of detecting crime and apprehending criminals), unjust inference from matched data that may not be rectified without great difficulty and loss of the presumption of innocence.

The question of how personal information concerning a convicted person should be handled is another special question, similar to that of convicted and alleged paedophiles. At heart the problem is that of balancing the presumption of innocence (in the case of those never convicted) or the importance of rehabilitation (in the case of those with criminal records) with the importance of reducing the risk of crimes being committed.

There is not space here to explore and evaluate all the changes in police powers in Britain in recent years and to identify all their implications for these privacy risks. It must suffice to note that the assembly of a large nationally available database that can be checked by any police officer from any force in the country by phone from almost anywhere, and the fact that the database contains records with soft information including allegations and suspicions on individuals who have not (yet) been convicted of any offence is perhaps the most important development in police capacity in handling personal information.

**Conclusion**

The new phase of reform and change in executive government poses both new challenges and new opportunities for privacy. Holistic government involves much greater sharing of personal data across the conventional functions, professions and activities of service provision and governance. There is an urgent need to consider both the conditions under which this will be acceptable and how best to control this. In Chapter 19, I offer some specific recommendations on how this might best be tackled.

A shift toward more preventive government, while welcome on other grounds, does call for safeguards lest it become the occasion for draconian action and the abuse of personal information. There are often very effective ways to engage in preventive action relying on
aggregates, which will not run the same risks of injustice as using individualised data.

Government services are increasingly called upon to provide risk assessments for private bodies and for the community at large. In the process, they disclose personal information about individuals, sometimes without their consent, and handle information of varying degrees of reliability. Again, it is important that we make explicit and transparent the trade-offs that are being made between the reduction of unacceptable risks and the impulse for privacy in this process, and that we use quite well-established principles to ensure that soft information is not abused or unjust inferences drawn in the effort to manage risks.

Police powers have grown in recent years partly in response to the public’s own concerns about crime and law and order. National databases have been introduced. The collection of information in more intrusive ways is permitted with only executive authorisation. While the best police forces have made great strides in the improvement of their practices in the management of personal information, there remain risks and concerns.

Nevertheless, the steadily rising public concern about some privacy matters and the publicity given to legal changes means that in Britain today there is probably a more informed debate than there has been for many years about privacy issues in government. There are legislative opportunities ahead for a review of these issues, and a number of executive initiatives are under way to review the implications of the imperative for more holistic and preventive government. The issue is whether the policy communities at the centre will be sufficiently attuned to the wider public balance of cultures to address these issues.
In previous chapters, we have seen the pressures and problems that the dynamics of business, technology and the changing character of executive government place upon the protection of privacy. In this chapter, we analyse the regulatory function of government which is expected to provide some collective response to these pressures. The aim of the chapter to identify the key trends and dilemmas in government capacity to regulate the flows of personal information and to trace some of their likely impacts on the future of privacy.

The chapter begins with a discussion of some of the specific emerging new regulatory challenges in connection with the business of personal information and describes the current state of data protection law before turning to the larger issues of regulatory capacity.

It is now conventional wisdom that regulation of personal information is growing more difficult. The usual reasons given are that:

- the integrity of the national space for information flows is being eroded by the growth of transnational business and even transnational government
- business avoidance strategies are becoming more effective
- regulators can never possess sufficient information to regulate effectively, by comparison with the information advantages of the industries regulated
the damage that regulation does to business competitiveness only erodes the tax base and the levels of employment that can sustain effective and legitimate government

regulation is always captured by the regulated industries

regulators cannot afford the rising cost of skilled and knowledgeable labour as the regulated industries can.

The conclusion often drawn from these arguments is that data protection regulation will suffer from acute regulatory failure and therefore in the medium term it is doomed. Of course, these are wholly general arguments, specific neither to the era of informational capitalism nor to the regulation of personal information. In principle, they could apply as much to regulation of the money supply, regulation of utility pricing or any other kind of regulation and, indeed, exactly the same arguments are often put.

There is not sufficient space here for a comprehensive and comparative cross-industry assessment of the general deregulationist case, or of the argument that the arrival of informational capitalism is the natural habitat of that policy in a way that the post-war era of industrial capitalism was not. However, in the second half of the chapter and in Part 4, some comments will be offered on the merits of the case in the specific field of privacy and data protection. This chapter argues that indeed, new challenges are presented to privacy regulation and that, as yet, regulatory strategies to meet them have not been fully developed. Nevertheless, there are reasons to believe that effective strategies can be developed, based on more innovation in the syndication of regulation, efforts to diffuse cultures of self-regulation, a commitment to learning in the design of the regulatory process and attention to the cultural conditions in which informational capitalism is operating.

Probably, in some areas of privacy control there will be an element of deregulation: for example, as we shall see, the EU Directive requires restrictions on the movement of data to third countries that offer inadequate protection and this is likely either to become unenforceable or to lead to counter-productive trade wars. However, deregulation in one area is often attended by reregulation in others: for example, in the
1980s there was extensive deregulation of market structure in many fields, but reregulation of market behaviour. There remain powerful forces – of which trust and legitimacy of informational capitalism with consumers is a major one – that will ensure that a demand for some forms of regulation, however light and differently implemented, will always emerge.

The chapter considers data protection regulation in some detail before assessing the implications of the case for the efficacy of regulation in this field. Encryption regulation was dealt with in Chapter 8 and some of the implications of that argument are also brought into play in this chapter. It concludes with a discussion of the two principal stories about the relationship between data protection regulation and the general dynamic of business competition.

**Data protection law**

Data protection law has evolved significantly in much of the developed world since the 1970s. The Organisation for Economic Cooperation and Development published its first guidelines for member states in 1980 and the Council of Europe published its Convention in 1981. These have formed the basis on which the European Union has developed its initiatives of which the 1995 Data Protection Directive is the most recent. In Britain, following a number of private members bills and reports of commissions, the Data Protection Act of 1984 was passed, and the 1998 Data Protection Act will become law shortly, implementing the 1995 EU Directive. There is not space here for a detailed description of the Acts and the Directive and the subsequent principal cases and the evolution of the principles. However, it may be helpful to outline some basic elements of the legislation as it will look once the 1998 legislation is passed.

The legislation sets out a series of key principles that must govern the use of personal data by those who use it in the public and private sectors alike (‘data controllers’, formerly ‘data users’) and creates the Data Protection Commissioner with powers to enforce the application of the principles upon receipt of a complaint from a person with
a proper interest in a case. The costs of compliance with data protection are to be borne by those who use it, not by the taxpayers or by the individuals who are the subject of the data (‘data subjects’).

**Scope**
The 1998 legislation covers all personal data, defined as information relating to living and identifiable individuals – that is, where the individual may not be named with their true identity but where someone would be capable of attaching it to a true identity, if they have reasonable likelihood of securing access to other information with which to match the data. It includes matters of fact and opinion. Although it does now include information that indicates the intention of the controller toward an individual (for instance, of an employer’s intention to offer work or sack or of an insurer’s reserve sum for settlement of a claim), there are exemptions for this kind of information from the rights of data subjects to have access to their personal data. The legislation applies to all data processing, from collection through use and manipulation to destruction, including organisation, adaptation and alteration, retrieval, consultation, use, disclosure, alignment, combination, blocking or erasure. ‘Data’ now covers manual records such as card indices or microfiches where these form a structured set of personal data readily accessible by specific criteria (but not those which only incidentally contain personal data), as well as those capable of being processed automatically. However, mere text preparation, such as word processing is not subject to the duty to notify the Commissioner.

**Legitimacy test for data processing**
The 1995 Directive and 1998 Act introduce a new duty on controllers to process personal data only when at least one of six conditions is met:

a. the data subject has given consent to processing
b. processing is necessary to carry out a contract to which the data subject is a party or taking steps to enter such a contract
The future of privacy

c. processing is necessary to carry out a legal duty on the controller
d. processing is necessary to protect the data subject’s vital interests
e. processing is necessary to carry out a task in the public interest or the exercise of authority vested in the controller or a third party to whom the data are disclosed
f. processing is necessary for the administration of justice
g. processing is necessary for the purposes of the legitimate interests pursued by the controller or parties to whom the data are disclosed, except where those interests are overridden by the interests, fundamental rights or freedoms of the data subject in respect of privacy.

Where processing is justified under (e) the public interest or (g) the controller’s legitimate interest, the citizen will have the right to object, where they have some legitimate ground, free of charge to further processing and even to a first disclosure, in particular for the use of personal data for direct marketing. However, this may be overridden in certain circumstances.

Clearly, the ‘legitimate interests’ clause is sufficiently broadly framed that it is unlikely to make wholly illegal industries of personal information processing where active consent of users is not obtained and not likely to be obtained in advance. For example, it is hard to imagine that any court would hold the basic activities of database marketing industries or credit rating agencies either not to be legitimate interests or else to be overridden in their entirety. Naturally, rogues in those industries may be caught but they are more likely to be caught under the main data protection principles described below than by their failure to comply with any of the six limbs of the legitimacy clause. However, where consent for continued collection is unambiguously refused by a data subject, the weight of the legitimate interest will have to be significant in order to override this.

Presumably, the legitimate interest of companies producing and selling geodemographic profiling and targeting databases and software
tools includes there being a sufficiently complete description of the population that they are, in the Sale of Goods Act terms, fit for the purpose for which they are intended. If large numbers of subjects were to refuse consent for data on them to be held in such tools, and if the companies’ legitimate interest did not override their refusal, then the industry could be put out of business. It is hard to imagine the courts comprehensively disabling a whole industry in this way and, presumably, while some specific breaches of the principles could be cracked down upon, the legitimacy clause will be interpreted in a way that does not do large-scale damage to business interests.

**Basic principles for processing personal data and data quality**

The principles by which controllers, whether or not they have complied with the duties of registration or notification, must conduct all data processing are as follows.

*Fair obtaining and processing*

Personal data must be obtained and processed lawfully and fairly; in particular, obtaining by deception or misleading people about the purposes is unlawful and unfair, but where someone has statutory authority or duty to provide the data, it is always lawful and fair. Where the controller seeks information from the subject himself or herself, he or she must inform the subject, where necessary, of:

- the identity of the controller and any representatives
- the purposes for which data are intended
- the recipients or categories of recipients
- where replies to questions are mandatory or voluntary, and the possible consequences of failure to reply
- the existence of rights of access and correction.

Where the data are not obtained from the subject, at the time of recording or no later than first disclosure, the controller must inform the subject of the same things.
Use only for purpose
Personal data must be collected, processed and held only for specified, explicit lawful purposes; the purposes must be notified to the Data Protection Commissioner.

Accuracy
Personal data must be accurate and not misleading as to matters of fact and kept up to date; but data controllers will not fall foul of this if they have taken every effort to erase or correct data that are inaccurate or incomplete for the purposes.

Restricted disclosure
Personal data must be used or disclosed to third parties only in a manner compatible with those purposes; the categories of people for whom disclosure is intended by consequence of the purpose must also be registered; employees, agents and contractors of the data controller do not count as third parties provided they work under the controller’s direct authority as set out in the contract. There are, however, the exemptions from the restrictions upon disclosure, where disclosure is:

- necessary for national security
- necessary for the prevention or detection of crime; the apprehension or prosecution of offenders; the assessment or collection of taxes or duties
- required by law
- obtaining legal advice in the course of legal proceedings
- made to the data subject or a person acting or her or his behalf, at the request of the data subject or with her or his consent
- made to a servant or agent of the data user
- urgently required to prevent injury.

Adequacy
Personal data must be adequate, relevant and not excessive in relation to the purposes.
Duration

Personal data must be kept in a form permitting identification of subjects for no longer than necessary for the purposes (except in the case of data kept for historical, statistical or research purposes).

Subject access

If they apply to data controllers in writing making clear their identity and exactly what information is sought, citizens are entitled at reasonable intervals (construed with regard to the purposes, the nature of the data and the frequency of updating) and without excessive or undue delay or expense (a maximum charge of £10 and a maximum period of 40 days from payment and complete request being received are currently set), and in an intelligible form, to be informed by controllers that data is held about them; what the purposes are; whom the intended recipients of disclosures are; and the data subject will have a right of access to those data and where appropriate in order to ensure compliance with the other principles to have them corrected or erased and details of any recipients to whom the data have been disclosed. Where data are used for automatic processing, subjects may have access to the logic by which any automatic decisions are taken, although this information need not be so detailed that trade secrets or intellectual property in algorithms are given away. In addition, where disclosure has taken place, subjects can insist on any corrections or erasures required being provided to recipients, unless this proves disproportionately costly or difficult. ‘Enforced subject access’ or the practice used by some employers and others of requiring a subject to exercise this right in order to insist that the information then be disclosed to them, will be made illegal. The main exemptions from subject access are the following:

- for the purpose of identifying third parties
- where subject access might endanger national security or undermine the effectiveness of the armed forces
- important economic and financial interests of member states or the European Union, including monetary, budgetary and taxation matters
for the purpose prevention and detection of crime, apprehension and prosecution of offenders; assessment or collection of taxes or duties

for the purpose of investigation and enforcement work of regulatory authorities, even though the suspect activity is not a criminal offence

judicial appointments

legal professional privilege

research or statistical purposes

back-up data

where subject access would expose the controller to criminal proceedings

examination results

certain categories of data protected by human embryology law

medical records, social services records, and financial services data which are subject to special procedures

data revealing the intentions of the controller in respect of the data subject

employment and academic references provided in confidence

data concerning honours and public appointments

examination scripts

records about individuals gathered and held by news media organisations, if, in the light of the special importance of freedom of expression, that eventual publication will be in public interest, construed according to and subject to agreed codes of conduct (this exemption applies to most data protection principles other than organisational and technical security).

Exemptions

National security

Data are not subject to any of the principles including subject access if national security is at stake, and a minister’s certificate is conclusive proof of a national security concern. However, a subject can appeal to
the Tribunal against a certificate on the same procedural grounds as for a judicial review.

**Crime and taxation**
Data processed for the prevention or detection of crime, apprehension and prosecution of offenders, assessment or collection of taxes is not subject to the principle of fair and lawful obtaining and processing, nor to subject access nor nondisclosure, if that would prejudice these purposes.

**Health and social work**
The Secretary of State has powers, which were exercised under the 1984 Act, to exempt medical and social work records from subject access.

**Regulatory activity**
Subject access and other principles do not apply to data processed for financial service protection regulation, charity supervision, or regulation of health and safety at work.

**Journalism, literature and art**
Data collected for these purposes are exempt from the data protection principles, provided that the controller believes, having regard to the special importance of freedom of expression and having regard to codes of broadcasting and press practice, publication would be in the public interest. The courts cannot hear any proceedings until such time as the self-regulatory bodies have disposed of any dispute in this regard.

**Research, history and statistics**
Provided data for these purposes are not used to support decision about individuals, their research use does not fall foul of the purpose restriction, and they may be kept indefinitely.

**Right to prevent processing likely to cause damage or distress**
If a subject notifies a controller in writing within a reasonable time to cease or not to begin processing any of the subject’s personal data for a specified purpose on the ground that processing might cause damage
or distress, then the subject has the right that the controller comply, unless it is necessary to carry out a contract with the subject, to comply with a legal obligation or it is in the subject’s vital interests.

**Right to prevent processing for the purpose of direct marketing**
Subjects also have the right in writing to require controllers not to process data about them for direct marketing purposes, defined as the communication by any means of advertising or marketing material directed to particular individuals.

**Right of rectification, blocking, erasure and destruction**
A court, if satisfied by a subject that data are inaccurate, can order a controller to rectify, block, erase or destroy those data, or, if the data accurately record information provided by the subject, the court may order supplementary data to rectify matters.

**Security**
Data controllers or their agents must take appropriate technical and organisational security measures against unauthorised access, alteration, disclosure, or destruction, and accidental loss or destruction, in particular where processing involves moving data over a network; agents must work to contracts that are tightly specified in written or equivalent form that permit no processing other than that specifically instructed by the controller. Controllers must take reasonable steps to ensure that their staff are reliable. Contractors must be selected on sufficient guarantees of their organisational and technical security measures.

**Sensitive data**
The 1995 Directive and the 1998 Act also recast the treatment of certain categories of personal data that are held to be particularly sensitive, namely those revealing:

- racial or ethnic origin
- political, or religious opinions or other beliefs
- membership of trades unions
physical or mental health, including disability
sexual life
commission or alleged commission of any offence or any proceedings in such a connection.

Such data may be processed only in the following specific circumstances:

- where the data subject has explicitly consented (except in countries, the national laws of which would prohibit it even then)
- processing is necessary for the controller to perform obligations in employment law, including employment contracts, health and safety and anti-discrimination law
- processing is necessary to protect the vital interests of the data subject or another person if the subject is physically or legally unable to give consent or has unreasonably withheld it on the subject’s behalf
- processing is part of the legitimate activities of a non-profit body with a political, philosophical, religious or trade union aim, where the data relate only to members or regular contacts and no disclosures are made to third parties without the subject’s consent
- where the data subject has taken a deliberate step toward making the data public, or processing is necessary for the seeking legal advice, asserting legal rights and involvement in proceedings for the establishment, exercise or defence of legal claims
- where the data are required for preventive medicine, medical diagnosis, care, treatment, management of health services, and where processing is done by a health professional or equivalent person who acts under professional codes and national laws of secrecy and confidentiality
- where the processing is for the purposes of medical research; personal social services; political canvassing; monitoring
ethnic origin, disabilities or, in Northern Ireland, religion; government statistics, social security and other government functions

- for the purpose of identifying third parties
- where subject access might endanger national security or undermine the effectiveness of the armed forces
- important economic and financial interests of member states or the European Union, including monetary, budgetary and taxation matters
- for the purpose of prevention and detection of crime, apprehension and prosecution of offenders; assessment or collection of taxes or duties
- for the purpose of investigation and enforcement work of regulatory authorities, even though the suspect activity is not a criminal offence
- judicial appointments
- legal professional privilege
- processing under official authority of data about offences, criminal convictions or security measures, civil trails or administrative sanctions.

Transferring personal data outside the European Union

The new law provides restrictions on the rights of data controllers to transfer data that are being or to be processed to countries outside the European Union. The only conditions under which such transfer is permitted is when the destination country in question has been deemed by the Commission of the European Communities to have an adequate level of data protection. Adequacy is to be assessed not in blanket terms but with reference to the nature of the particular data, the purpose and duration of the particular processing, the countries of origin and of destination, the legal rules in national law and international commitments on data protection in the destination country and the extent of their practical enforcement and application and security measures.

Where the Commission finds that a country lacks adequate protection, it has powers to take measures to prevent transfer, and to enter
negotiations with a view to remedying the situation. While in British law, it is for the controller in the first instance to decide on adequacy, the Commissioner has powers to use the enforcement notice system to require transfers to cease, or to permit transfer in situations where the controller will contract or administer to ensure that safeguards agreed with the Commissioner will be adhered to in processing, and to notify the European Commission when she or he believes that a third country has inadequate levels of protection.

This may be set aside where the subject has consented, understanding fully that the country to which data are to be transferred has inadequate protection; where transfer is necessary to fulfil a contract with the subject or to make a proposed contract possible; there is a substantial public interest and an order by the Secretary of State on this; the transfer is necessary for legal proceedings, to obtain legal advice, or establishing, exercising or defending legal rights; the transfer is necessary to protect the vital interests of the subject; the data are already part of a public register, or else the Data Protection Commissioner has approved it.

This has rapidly led to confrontation with the USA, which has much lower levels of privacy protection, especially in the private sector, than the EU permits. The US Presidency, preferring voluntary codes of practice, kitemarks and contractual solutions, has taken the view that the EU law constitutes a trade barrier that may be taken up with the World Trade Organisation.132 (Conversely, the EU, with the partial exception of the UK, takes the view that businesses and individuals should be allowed the unrestricted use of encryption, which the US opposes.)133

**Automatic decision making**

Where data controllers use automated processing methods to make decisions that have significant legal effects on the subject, or any significant effect based on evaluative data concerned with, for example, the individual’s work performance, creditworthiness, reliability or conduct, the data subject shall have the right to insist that the decision shall not apply, unless that decision is taken in the course of entering
into a contract where there are safeguards that, for example, allow the subject to have a chance to put their point of view, or where national law provides other safeguards.

**Notification**

A simpler notification scheme will replace the 1984 registration scheme, to be introduced by statutory instrument. All data controllers must, before processing any data, notify the Data Protection Commissioner of:

- the name and address of the data controller and any representative
- the purposes for which personal data are collected and processed
- the categories of personal data, including categories of subject
- the persons or categories of persons to whom disclosure is envisaged and why that is necessary to achieve the purposes
- any proposed transfers of data to countries outside the European Union
- the security measures
- whether any exemptions from subject access or restricted disclosure are claimed.

Some categories of processing that are deemed to present particular risks to rights and freedoms including privacy may be subject to prior checking, following the notification application, and no processing can begin until that is complete. The Commissioner must give notice within fifteen working days of receipt of the application that she or he intends to carry out prior checking. These could include some data matching exercises, use of certain genetic data and some private investigation activities.

The register of notifications must be publicly available for anyone to inspect. Controllers pay an annual fee for notification, which can be paid by direct debit. On-line access will be introduced, as will on-line
notification. Full renotification will no longer be required every three years but material changes must be notified.

Exemption from notification can be granted where the purpose of processing is confined to:

- payroll, personnel and work planning administration
- purchase and sales administration
- advertising, marketing (other than marketing to identifiable individuals: that is, untargeted marketing only) and public relations
- general administration
- processing for the purpose of holding registers and other data required by law to be made public
- processing in connection with mailing and membership lists
- processing by non-profit bodies with a political, philosophical, religious or trade union aim, where the data relate only to members or regular contacts, and no disclosures are made to third parties without the subject’s consent
- processing of bibliographic data
- word processing, where not covered by other exemptions.

**Enforcement**

It is an offence for:

- data controllers to fail to apply for notification
- data controllers to provide inaccurate information in a notification application
- agents or processors knowingly or recklessly to process information otherwise than in accordance with the controllers legally valid instructions
- anyone unlawfully to procure or sell personal data
- anyone to fail to comply with an enforcement notice.
The Commissioner may issue an enforcement notice to a data controller or agent, where she or he considers that there has been a breach of the data protection legislation, including:

- processing data in a manner inconsistent with the notified information
- failure to inform the Commissioner of material changes to the notification
- where the Commissioner requires information to pursue a complaint made by a data subject and the information has been refused.

Such notices must set out the remedial action, the right to make representations and any right of appeal to the Data Protection Tribunal.

Individuals can apply to the Commissioner by way of making a complaint, and also to the courts, who alone can award damages for distress arising from any breach of the law.

**The Data Protection Commissioner**

Newly renamed in this way, the Commissioner has power to carry out quality assessments on controllers systems but without power to compel their involvement, to propose voluntary codes of practice and has a duty to consider draft codes put to her or him and, if she sees fit, to seek data subjects views on them.

**Is regulation getting easier, harder – or both?**

**Globalisation and jurisdiction problems**

It is impossible for anyone to know through which countries a package of digital information will pass, when a transaction is conducted over the Internet. Packages are switched between servers relatively seamlessly across frontiers. Moreover, in principle, any unencrypted, unrestricted material posted for access on the World Wide Web can be viewed anywhere in the world.
Therefore, it is very difficult for any single country acting alone comprehensively to enforce clear principles of legal jurisdiction for transactions either using a source, route or destination principle. While particularly egregious examples of violations can sometimes be prosecuted, at least where extradition laws permit the apprehension of individuals who can be held responsible, it is much more difficult to enforce national law on the destination principle against all violators. Enforcing one’s rights in another country under its laws is very expensive and difficult, particularly in the US, where the 1974 Privacy Act is the only federal provision, and it is one of the weakest privacy laws in the developed world. This makes it very difficult, without resorting to extraordinary extra-territorial application of national laws, to apply laws for data protection, or for that matter, censorship of pornographic materials, or the taxation of financial transactions.

Recent cases in the USA, Germany and elsewhere have appeared to move in the direction of just such an unprecedented extra-territorial application. However, there are serious questions about how far this trend can be extended when the means of enforcement of national laws in other countries are lacking.

Competition between national laws might be an effective way in which to further the cause of privacy, if individuals and businesses were ‘footloose’ in their location decisions and if the fundamental economic dynamic of informational capitalism were one in which competition would bid up consumer and citizen protection – an uncertainty explored further below.

Restricting transactions with countries with ‘inadequate’ data protection

The 1995 European Union Directive on data protection and the British 1998 implementing Act seek to restrict the undertaking of information transactions with countries deemed to provide ‘inadequate’ protection of personal data. There remain serious difficulties in seeing how, particularly over the Internet, such a restriction can be enforced. Interpreted strictly, every time anyone sends an e-mail
message (which typically contains in the headers quite a lot of personal information of some value to third parties in some contexts) they risk violation, because they cannot know through which countries it might pass, and might, at least in theory, be intercepted. Unless it were deemed by the courts that the very act of using e-mail at all amounts to consent to third country transfer with understanding of the risks involved implied (which seems a rather forced interpretation) there are problems ahead here. On the other hand, if member states, when they pass national law to implement the Directive, interpret this restriction as requiring prior authorisation for certain types of transaction – as some seem to be doing – this could impose heavy burdens on businesses that make extensive use of electronic transfer of information.\textsuperscript{136}

**International trade negotiations and standards authorities**

Some privacy activists have argued that because information can no longer feasibly be kept within national borders privacy regulation must become a global affair. Lacking any other institution for such global regulation, many have begun to fasten their hopes on the World Trade Organisation, and aspire to a data protection dimension in future rounds of world trade negotiations on services, much as environmentalists and labour relations pressure groups are pressing for their favoured standards to become conditions of market access in such negotiations.

It is far from clear that this will be accepted quickly. One reason for pessimism might be that those passionately concerned about privacy are, at least at present, too small a percentage of the population in most countries to give the issue the political salience that, say, pollution control or rainforest logging or child or convict labour have had. Even these high profile issues have not become established parts of the world trade agenda. However, it is not clear that the alternative multi-lateral negotiation systems – for example, the International Telecommunications Union or the International Standards Organisation – could deliver the sort of treaty that will be required. While the International Standards
Organisation will continue to have an important role in establishing technical protocols for cryptography and privacy enhancing technologies, little more than this would be appropriate.

National regulation of the private ownership of cryptography is unconvincing, because Internet trade is now so straightforward that the US export ban seems decreasingly credible. Meanwhile, the conflict in regulatory impulses between the duty in data protection law to implement security measures and the security forces concern to prohibit the use of cryptography is particularly stark.

**Regulatory role and capacity**

There are intrinsic limits to the capacity of any regulatory body which is attempting to regulate the complex behaviour of vast numbers of people and organisations, if it is expected to employ comprehensive enforcement based strategies. The investigation, discovery and enforcement tasks before a conventional regulator of the price of the homogeneous output of a monopoly utility company seem relatively straightforward, in contrast with the job of the Data Protection Commissioner, and yet it is well-known that regulators in those industries suffer from severe difficulties in securing information from the regulated, in second guessing even the short-run economic impact of their regulatory decisions on the market. Moreover, at least some of the utility regulators have behind them the practical efforts and political support of active consumer organisations, whereas in the field of privacy and data protection, the organisation of data subjects is very weak.

One recent regulatory strategy in fields such as environmental regulation is to use the coercive power of law-making to redefine property rights, particularly where the behaviour of the regulated imposes external costs on others, in order to internalise those costs upon the budgets of the regulated in some way. Tradable pollution rights are an example of this kind of mechanism and have been tried with some success in California and elsewhere. However, efforts to apply this analogy in the field of personal information have not met with great
success, despite some privacy activists using the vocabulary of ‘informational self-ownership’.$^{138}$ A true owner of a piece of information would have the right to destroy it, to neglect it, to dispose of it at will and perhaps even falsify it. There are, unfortunately, too many situations when citizens cannot be permitted to exercise these ownership rights. These do not only occur in the context of duties to provide true and accurate information to public authorities for taxation and licensing purposes (where falsification and destruction of personal information is a criminal offence), but also in the private setting where obligations arise to employers, insurers and others who bear risks arising from our conduct and contract, and to others in tort and duties of care. If it were possible to describe completely all the abridgements of informational self-ownership that would have to be applied in anything less than a law library of many volumes, the resulting claim would hardly look much like ownership at all.

There are few alternatives in the field of privacy to focusing principally on the behaviour of data controllers. Of course, there are many more ways in which we can experiment with more market based mechanisms that will enable people as consumers and customers in private markets to choose the suppliers they trust and who offer them the level of privacy protection they desire. Chapter 8 examined a recent Internet kitemarking scheme of this kind. However, it would be wrong to imagine that such schemes, valuable and important as they are, will provide the range of protections against the whole range of privacy risks that modern informational capitalism and government present.

Conventional organisational theory of regulatory strategy distinguishes between two basic styles – a ‘deterrence’ model, where the style is adversarial and legalistic, and the emphasis is on punishing wrongdoing; and a ‘compliance model’ in which the style is advisory and negotiating and the emphasis on preventing problems and building up a relationship of sufficient trust and confidence between the regulator and regulated that problems can be detected early and ironed out.$^{139}$ The expectation in the legislation – particularly when it concerns itself with such issues as the encouragement of codes of practice and envisages
some contact with controllers at the point of application for notification – seems to be that the Data Protection Commissioner will exhibit the latter style. However, the compliance model still makes demands of the limited resources of the Data Protection Commissioner that no regulatory agency could possibly fulfil, if it has to deal with almost every organisation in a national economy in an age in which personal information is the basic raw material of the economy. No such agency could develop that kind of relationship with every one of its potential clients.

The only sensible strategy for privacy regulators in such a context is to develop tactics for changing cultures voluntarily, beyond the conventional repertoire of enforcement and bargaining, and to find the grain in the mainstream culture of the organisations and populations with which they deal, along which they can cut most effectively. One example of regulatory bodies that have worked along these lines, albeit with more powerful social movements behind them than privacy commissioners can hope for, might be anti-discrimination regulators. It was not principally by their enforcement activity that the Commission for Racial Equality and the Equal Opportunities Commission made their contribution to the relative success Britain has had over the past 30 years in removing racist exclusion from lettings adverts, clubs and restaurants and more generally in challenging cultures of racism and sexism, although enforcement remains an important part of their repertoire. It has been their careful orchestration of elite and public opinion around key issues on which overt racists and male chauvinists have been culturally vulnerable that has won them important bridgeheads in the wider culture. The building of alliances, the development of a small cadre of professionals in the public and private sector committed to their cause and the backing and encouragement of high profile media debates on relevant issues have been a key part of the anti-discrimination strategy of these regulators, and one that the classical organisational theory of the compliance model does not capture particularly well. In short, the effective strategy in such situations is to pursue cultural change using the apparently ‘weak’ tools of government, such as information, persuasion, networking, alliance building, example
and product innovation, rather than simply relying on the ‘strong’ tools of coercion, incentive and public expenditure.\textsuperscript{140}

Privacy regulators in the UK and in many European countries have tended naturally to look to civil liberties groups and movements as their natural allies. In Europe, privacy concerns are generally seen as a part of human rights law, with its peculiar cultural niche. However, because civil liberties movements are relatively small – for reasons of the relationship between ideology and organisational culture and collective action problems identified in part one – their power and cultural influence is weak. Therefore, as informational capitalism increasingly depends upon the use of personal information, it will become necessary to draw consumer movements and private sector professions into the debate.

The international network of privacy commissioners and their immediate cultural allies is relatively strong, by the standards of statutory regulators, and is reinforced by the requirements in EU law for some collaboration and the interest of the OECD in the field. This network can provide the basis for the gradual emergence of more transnational strategies both in enforcement and in cultural work in areas where that is likely to be the most effective.

In the context of a strategy focused as much on voluntary cultural change as on casework using enforcement or bargaining methods and working increasingly transnationally, it is necessary to think through the actual goals of regulation. Enforcement and even compliance based regulators can expect to achieve relatively high levels of total conformity with the letter and spirit of the code of behaviour they are charged with promoting. But in the case of simple price capping of a single price or a small number of prices upon a single monopolist, it is possible to secure complete conformity. This cannot be the aim of a regulator with the resources, numbers of targeted organisations and limited strategic choices that face a privacy or data protection commissioner. Rather, the goal shifts to influencing the overall climate of business and governmental culture, international business ethics and citizens’ awareness. While deterrence and compliance models of activity continue to have a place in repertoire for dealing with individual
cases, the value of the casework is as much in its visibility, in the signals it sends and in the learning it stimulates, as in its practical enforcement effect.\textsuperscript{141}

Seen in this way, some of the traditional deregulationist arguments seem to miss the point. The standard deregulationist claims about transnationalisation rendering the tools of regulation blunt are dealt with by shifting the goal and the strategy to the multilateral plane. True, business capacity to evade regulation is great, but when the aim is as much to change hearts and minds over time as to enforce the details of a code today, the fact that hearts and minds have yet to be won over has rather less force. The deregulationist point that the regulator cannot have sufficient information on which to enforce comprehensively is well taken, but the strategy is designed around that acceptance without being resigned to impotence. The costs of hiring sufficient expertise from industry and government into the regulatory office may not be so formidable when persuasion skills are as important as technical understanding of the means of evasion.

The test of whether a ‘hearts and minds’ strategy of ‘regulating by cultures’ is feasible is whether it can be made culturally sustainable, given the balance of the four cultural traditions about privacy and private life identified in part one. In Part 3, I shall offer a richer account of what the test of cultural sustainability is, and in Part 4, offer more detailed and specific policy suggestions about how it might be met.

Two deregulationist arguments remain and must be taken seriously. The first is that regulators are always ‘captured’. It is certainly possible to imagine this process in privacy regulation in the context of the revised strategy. Indeed, there may be an even greater danger of capture when the regulator is engaged in constant dialogue rather than mechanically enforcing rules whenever putative breaches are observed. However, there are ways to reduce the risk, through turnover of staff, improved public accountability and scrutiny of the regulatory office in the legislature. The latter point in particular will be addressed in part four.

This deals with the last of the deregulationist arguments about the limited capacity of privacy regulators to achieve anything worthwhile.
The final and perhaps crucial deregulationist argument that is the most difficult to answer is the one that privacy regulation imposes such costs on business that it will render individual businesses and indeed national economies that subject themselves to data protection uncompetitive with those that will not. It is to this concern that the next section is devoted.

**Regulation of personal information and the dynamics of competition**

These economics of personal information therefore raise questions about the economic impact of privacy regulation upon informational capitalism. The point of this argument is not that British business and government agencies are necessarily engaged in large scale flouting of the principles of the Data Protection Act, or that no form of regulation of the ethics of the use of personal information can ever work. Rather, there continue to be enormous pressures within the dynamics of modern business and government for the use of personal information in ways that will continue to present privacy risks.

In this context, business competition and regulation may have one of two possible effects. There may be a kind of Gresham’s law in privacy. In this scenario, privacy and data protection laws are seen as brakes upon competitiveness. Seeking to diversify their activities to follow the customer interests they detect from their databases, businesses find themselves restricted by the purposes for which they originally began to collect information and find it more costly to undertake that diversification that it might otherwise have been. Advantage lies with the firm that evades the costs of having to respect privacy or data protection principles or the country that sets itself up as a ‘data haven’ from such data protection regulation. Indeed, in the course of this research, some corporate lawyers and other business counsellors said that they frequently counselled their clients to try to operate in the European market from bases outside the EU because of the costs of compliance with EU data protection law. Indeed, some US commentators look upon the EU Directive as a shackle upon the competitiveness
of European businesses when in rivalry with the less regulated US private sector. Over time, therefore, in this scenario competition forces down standards of business commitment and regulatory protection.

An alternative dynamic is conceivable. In this scenario, privacy is a key element in securing consumer trust. When businesses collect or use personal data in ways that their customers distrust or regard as violations of privacy, they can face high costs of re-establishing trust. Lotus, Microsoft and Netscape have all recently faced consumer revolts because they created and distributed software to collect or display information about customers’ activity or assets in ways that their customers regarded as lacking in transparency and legitimacy. None has suffered long term damage but it was quite possible that they could have done. Advantage, in this scenario, goes to businesses that invest in meeting high standards of privacy and to countries that offer high standards of regulatory protection.

What is the relationship between these two scenarios? One organisation that is perhaps charged with thinking through this question and its implications for the regime under which transnational trade is governed is the World Trade Organisation. In the course of the current round of negotiations on trade in financial services, paragraph eight in the agreed Memorandum of Understanding states that while member states may not take measures that restrict trade in information or processing, but ‘Nothing in this paragraph restricts the right of a member to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of the Agreement.’

Similarly, the current WTO ‘most favoured nation’ trading rules allow ‘the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts’ as one of the general exceptions from openness of trade under the general agreements, ‘subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services.’ While this amounts to
acceptance that data protection and privacy laws are reasonable concerns that should not be overridden *en gros* by free trade law, this hardly amounts to a clear view about the economic impact of each on the other. Whether these provisions will amount to a carte blanche for any kind of data protection measure or law of breach of confidence is not yet clear. Moreover, it is far from clear that the current EU law in the 1995 Directive on transfers of personal data to third countries would be read by the WTO as wholly compatible with these solemn commitments.

It is quite possible that both of these dynamics may operate at the same time but in different market segments. For example, small and medium sized enterprises might find it burdensome to install firewalls, software protocols and systems for obtaining consent that will ensure that privacy is respected, while established large or multinational corporations with highly visible and well-known brands may find it more affordable and advantageous. Alternatively, it may be that industry rather than size in the crucial factor. For example, it may be intrinsically more difficult and a bigger obstacle to effectiveness and profitability for geodemographic profiling, credit rating, direct marketing and other such services, to handle the costs to the value of their product from individuals’ exercising their rights to opt out of their data collection systems. Therefore, they will wish to locate in countries that make no such requirement.

Potentially, large multinational corporations may find it easier and least costly to work with different standards of privacy in their operations in different parts of the world. The case for this strategy is simply that observing local laws, cultures and *mores* about privacy – for example, being meticulous in Germany but much more relaxed about data sharing in Japan – is the natural way to achieve trust in each country. However, such businesses run the risk that they will be accused of hypocrisy by pressure groups working in high privacy protection countries, just as environmental and health campaigners in Europe and North America have levelled charges of hypocrisy against multinationals they believe to operate different standards in different parts of the globe.
Another issue for business may be the ethics of the costs of providing data subjects with access to the information held about them. Very often, the transactions costs involved in charging each individual that chooses to exercise their right are greater than the charge itself. Businesses therefore treat such costs as part of their general overheads which they cover in their product pricing decisions. In effect, some of the costs of respecting privacy are passed on to customers who may be quite unconcerned about privacy. On the other hand, is it ethical that only those with intense preferences about data protection should bear the costs of ensuring that companies comply with the disciplines it imposes? This is an issue not only for transaction costs but for the costs of putting in place any kind of privacy enhancing technology or system.\textsuperscript{145}

**Conclusion**

The economics of informational capitalism have made personal information the fuel of both business and government. Personal information now performs a role not wholly dissimilar from that played by land in the mediaeval economy: it is the primary resource, in which business and government must invest first before attempting any other kind of activity.

In this context, the key implication for the future or privacy is whether it is more likely that business and government will thrive on the basis of trust in ethical handling of personal information that will secure public confidence in new innovations and directions such as electronic shopping, smart card systems and or on the basis of simple cost and price reduction to consumers in all transaction processing. That both will be important in some measure is not in doubt. What is at stake in the future of privacy is which will be more important, when they come into conflict.

However, the most important conclusion of the argument in this chapter is that the kind of regulatory capacity that matters most, is the capacity to diffuse the values of privacy, to influence the ways in which cultures change, to stir up stigma among consumers and businesses.
alike for practices that do not respect privacy, and to win hearts and minds for a conception of privacy that is itself changing as cultures of private life change. Clearly, regulators of the size, expertise, budget and legal status of a typical privacy or data protection commission cannot achieve this alone. We return to this issue in Chapter 21 on privacy education.
This chapter reviews developments in the media that affect privacy. The first section provides a general overview of how and why privacy has come into greater conflict recently with news values, and identifies the main risks to privacy that modern journalistic practices can present. The second section provides a review of the state of media law on privacy, including the main civil and criminal law remedies available to those whose privacy may have been violated, and considers the impact on privacy law of the incorporation of the European Convention on Human Rights into British law. The section then goes on to describe the main features of the self-regulatory practices of the press and broadcasting industries in Britain. The chapter concludes with an assessment of the balance of forces between media imperatives that put privacy at risk and legal protections, and considers where the debate is now moving.

Like all categories of risk, privacy is essentially the creature of conflicts of power. The elective affinity of claims of privacy rights with liberal thought and culture has been founded upon the conflict between individuals and large organisations with powers effectively of coercion, de jure in the case of the state, de facto in the case of other institutions. There have emerged many powerful business interests with the capacity to affect the lives of individuals who have not even chosen to be their customers, or who may have little choice but to become customers of at least one of a small number of suppliers, because their
services have become effectively essential to the achievement of what is now considered a decent standard of living. In the first category, we need to consider the power of the press, broadcast and other media, while in the latter category, earlier chapters considered the power of the financial services industries, and behind them as providers of fuel for their operations, direct marketing, geodemographic profiling and the data mining, matching and warehousing methods that make possible a sophisticated informational capitalism.

In this chapter, we consider the changing strategies of the mainstream media and their relationship with personal and private life, both in its construction and maintenance and its surveillance. The chapter examines the present legal and ethical framework within which they conduct their business. The argument is that like information and communications technologies, the media are a resource for private life and privacy as much as a threat to it. There are real choices to be made about the framework which can guide the relationship of the media with the personal and private. However the dilemmas that structure those choices are becoming more acute, more urgently felt, and more complicated in their relationships with other kinds of legal and ethical questions. The section argues that this has happened as a result of a variety of distinctively late modern social pressures and forces, which, when correctly and comprehensively understood, cast important new light on the cultural dynamics on which the futures of privacy will turn.

**Media of record, media of opinion, media of prurience: the construction of private life**

No media are wholly transparent and objective or restrained, for all the obvious reasons about the impossibility of a wholly unbiased perception, understanding, selection and presentation of any kind of information. However, there are clear differences in any kind of news and current affairs, documentary, comment or essayistic reportage between the accurate and inaccurate, the subtly and the blatantly biased, the biased that still offers readers, listeners and viewers enough
material on which to come to an alternative opinion, the sycophantic or the paranoid-dissenting and the constructively critical, the prurient and the high-minded, and so on. Contrary to the received wisdom that ‘the newspapers are getting worse’, and that bias and privacy violations are a peculiarly recent aberration, most of these genres are very old.

Nevertheless, there have been changes in the importance and the strategies of the principal media in recent decades that have profoundly reshaped the context in which private life is conceived in the public sphere. The effect of the growth in numbers of broadcast stations, their international reach and their capacity to deliver news quickly have had a great effect on the printed media. They have diversified their content away from news reportage into comment and opinion (broadsheets) and greater personalisation of news and current affairs on the ‘celebrity’ figures (broadloids). The tabloids have moved in the same direction as the broadloids but have also diversified into a variety of types of entertainment that are less closely connected with conventional broadsheet or mainstream broadcast news and current affairs. In the glossy magazine market, there is increasing competition in the sector offering personal profiles (ranging from the sycophantic to the aggressively intrusive or malicious) of assorted ‘celebrities’ from the worlds of sport, broadcast drama, film, music and politics, and, to a lesser extent, arts, entertainment and other fields. Although there is nothing new about newspaper prurience, the scale of detailed profiling of the lives of stars has grown, in one generation, to become central in media strategy.

There has been a steady stream of controversies about privacy violations by the media, and especially by the tabloid and broadloid press in recent years. Many, and perhaps most, have concerned the powerful and the famous, but some have concerned people of no prior public reputation whatsoever. It is a commonplace argument in media circles that by becoming famous or powerful, people forfeit their right to privacy, at least partially, although this view has not achieved any clear legal status. Many people have celebrity thrust unwillingly upon them, for example by virtue of winning the National Lottery, being a victim of a crime, being related to a famous or powerful person or through a
local dispute that attracts media interest. This had led to allegations of cases of information collection behaviour by some unscrupulous journalists and photographers that, were they conducted by private individuals, would be viewed as:

- **harassment**: such as continuous telephoning or doorstepping, accosting in the street, refusing to accept refusals to comment or particular answers
- **trespass**: camping outside people’s front doors, even in their gardens
- **bribery**: payments corruptly made to people to disclose national insurance records, medical records, CCTV footage, tax details, without proper authorisation and in violation of data protection laws; (in practice, juries typically acquit journalists of making payments ‘corruptly’ if the effect is to uncover a major public scandal: there have been cases where the person accepting a newspaper payment was convicted of accepting bribes, but the newspaper itself acquitted of bribery, on the grounds that the journalists were able to satisfy the court that they were wrongly illinformed about the contractual status of the bribee)
- **theft**: seizure of documents or even mail
- **interception of communications**: use of bugging devices
- **surveillance**: use of telephoto lens photography and high sensitivity distance sound recording equipment
- **deception**: misleading neighbours, friends, shopkeepers into divulging information
- **impersonation**: pretending to be the subject of the investigation in order to obtain information from others, or impersonation of others in order to gain access to home or work or even hospital beds
- **entrapment or incitement to commit offences or other misdemeanours**: usually in combination with impersonation and deception, this involves obtaining a story by persuading the subject to do something illegal or embarrassing.
While in the broadsheet sector, such practices are used sparingly, there are sections of the media where they are regarded as more widely acceptable, and where editors and journalists take the view that the rule of freedom of the media should be interpreted as allowing them the rights to collect information in ways that would be illegal for others. This claim for special status is discussed in greater depth in Chapter 17. However, for the present, it is important to make clear the scale of the legal and policy questions that it raises about the triangular relationship between media power, media freedom and privacy. For if privacy is the provisional unaccountability of individuals, then the claim to special status of privilege from the restrictions on the methods of data collection that a consistent application of the ‘fair obtaining’ principle in data protection law (let alone the ordinary criminal and tort laws) would extend amounts to a much greater unaccountability of the media.

Whether this can be justified on the basis of the public interest must depend on distinguishing sharply between the public interest and the public’s prurient curiosity and the private interest of the media in meeting that demand.

The continuing popularity of the published products of this formula with large segments of the population in Britain and other developed countries suggests that newspaper editors must be right, at least in part and even if the response is self-serving, when they answer charges of prurience and low taste with the point that while the public condemns their excesses it still wants to read the products of those excesses. Moreover, there is a steady supply of individuals and families willing to make themselves available to the press, talk and game show media and to expose to the public gaze facts about their lives that are considered private, in the hope of exposure and perhaps also financial gain or enhancement of social status and, in rare cases, access to the first step on the ladder to celebrityhood. A confessional style of stylised self-revelation is now expected practice for politicians, film actors and actresses, musicians and sports players, and even broadcast presenters. Where they fail to offer the required confessions, they can expect details to be obtained without their consent and that they will
be criticised for ‘secretiveness’ and a ‘recluse’ lifestyle, with the implication that only someone with something shameful to hide would choose not to play the confessional game.

What is remarkable, for the present purposes, about this culture of confessionalism and celebrity-seeking is not that demand has called forth supply, or even that this has become a multi-billion pound section of the media industries. More germane and perhaps more surprising is that, contrary to the common wisdom, confessionalism is not at all the enemy, but the rather tempestuous and destructive lover of privacy or the principle of confidentiality and non-disclosure.

For the weight of a taboo can be reinforced precisely by being broken in a way that constantly emphasises the frisson of breaking it. Personal information about the famous is only of interest to the prurient precisely because it is private. If confessionalism were wholly routine to the point that the culture of privacy were dying, then it would not be confessionalism at all but something much more mundane, less interesting to millions of people and much less profitable for media businesses. The value of privacy is paradoxically affirmed by the very manner in which its violation is conducted. In being able to confess or in having one’s confidences breached or privacy violated, the otherness and fascination of the rich is illustrated and constructed. The rest of us are reminded that our privacy is a blessing that the famous cannot share with us and a burden that marks out our lives as more humdrum and less interesting than theirs. Privacy is constructed in the popular press, the talk show, the celebrity magazine as at once a mark of underachievement and a delicious but fragile risk of success. In this way, the media are engaged in the continuous construction of privacy and private life, albeit with a peculiar spin, at once salacious and socially divided and yet demotic and cynical.

Therefore it is not surprising that from time to time, both confessionalism and the enforced confession of a violation of privacy itself becomes a scandal. The pursuit of Diana, Princess of Wales by paparazzi photographers in Paris during the last hours of her life and the strategems used by a tabloid journalist on a Cabinet minister’s son to expose the willingness of the protagonist to sell small amounts of
cannabis are but the most recent disputed cases in Britain from a long line stretching back some years. Many have prompted official commissions of enquiry, proposals for legislation, court proceedings for breach of confidence, debate about the implications of European and international law, developments in collective self-regulation by the media, complaints to self-regulatory bodies, and so on. The controversy of these methods is of course entirely understandable and perhaps even predictable in the context of a strategy that serves to underline the importance and value of privacy even as it infringes it.

Moreover, as we have seen, there are other pressures in our society that are also reinforcing the importance of privacy and therefore serve to undermine even such efforts as are made by some media leaders and commentators from time to time to downplay or criticise the claim of value. Growing individualisation in culture and the claim of right to seek personal satisfactions with some provisional unaccountability to others, the continuing importance of personal space in the home, conflicts over the need for personal space in the workplace and the employer’s claim for flexibility and the continuing concern about the risks of unjust inference in the fields of consuming and being governed, combine to sustain and even enhance the importance of privacy, albeit with many conflicts and without claims to any absolute status for privacy rights. Despite some alarmist talk of the media usually referred to in this context as the ‘fourth estate’, as the greatest power in modern society, there are key social values in contemporary culture over which the media have in fact rather limited capacity to influence the extent to which people attach importance to them.

No more than information and communications technologies, then, are the media a force simply for the decay and erosion of privacy. Indeed, in some measure, the opposite is true: they make money only because there remains, and they must sustain, a frisson of taboo-breaking attached to the violation of privacy.

Moreover, this should serve to remind those who are sceptical of the essential unity of concern that underlies the range of privacy risks. There is nothing intrinsically different about the issues of media
privacy from the questions raised by the use of personal information in government or other kinds of business.

**Privacy and the media**

Despite the frequency with which it is claimed that Britain lacks a privacy law, there is a body of law in the criminal law of theft, statutory offences of unlawful interceptions of communications, the civil law of trespass, in contract, in the quasi-tort of breach of confidence, and now in the European Convention on Human Rights, that governs the privacy of individuals who become the subject of any public attention, not least in connection with the media. In the media context, of course, these legal rules could, at least in principle, and may yet in practice following the incorporation into British law of the European Convention, come into conflict with the principles and legal commitment to freedom of the media. It is worth briefly rehearsing the principles of that body of law.¹⁴⁶

**Collection of information**

**Theft**

The ordinary law of theft in section 4 of the 1968 Theft Act defines property that may be subject to prosecution for theft as including ‘money, and all other property, real or personal, including things in action and other intangible property.’ This surely applies to many of the kinds of personal information that unscrupulous journalists might be inclined to try to seize, although there is a grey area in the field of theft of ‘intangible property’, where the courts have been strangely reluctant to develop the law consistently with the general principles of the law of theft.

**Trespass**

At present, the law of trespass makes it a tort or civil wrong physically and bodily to enter the property of another without permission or warrant, but this does not make it wrong to use telephoto lenses from outside the property or to use sophisticated sound recording equipment from outside to gather information on conversations conducted.
inside the boundaries of the property. Nor does it deal with electronic data capture without consent, which is still left to the narrow and confined law on the interception of communications. Moreover, a landowners’ consent to entry, once given for one purpose, cannot be limited to that purpose, even if the journalist or photographer has actually come with another purpose, although consent can subsequently be revoked. The courts often do not apply to the media the principle that no one should profit from their wrong, and injunctions against the publication of material gained by trespass are rare: if any remedy lies for such privacy concerns, the courts usually consider that damages are sufficient. The Calcutt report of 1990 recommended a new law on media trespass that would cover many new forms of surveillance, albeit with a public interest defence, but neither the Conservative nor Labour governments have been willing to legislate these ideas.

Interception of communications

Most of the law on interception of communications is out of date because it has been framed in ways that were specific to the technology of the day when the laws were drafted. For example, the 1949 Wireless Telegraphy Act prohibits devices uses wires to intercept messages that might interfere with radio transmissions but leaves modern bugging and other covert data capture equipment untouched. The 1985 Interception of Communications Act introduced an offence of intercepting public telecommunications without a warrant, and also for a telecommunications company to disclose intercepted messages except for the prevention or detection of crime, in the interest of national security and so on. However, because it is difficult to work out when such interceptions have taken place, prosecutions are rare. It might have been more effective to attack the information gained from such activities rather than the activity or procedures themselves.

Computer misuse

In the same technologically specific and therefore vulnerable way, the 1990 act introduced the offence of knowingly and without authorisation
causing a computer to perform any function with intent to gain access to any program or data, or to make any unauthorised modification to the contents or data, or impair access for others. Targeted against hackers, it could be applied to adventurous and unscrupulous journalists seeking a story.

Journalists’ privileges
In general, journalists and media organisations have been held to be subject to the same kinds of laws as any member of the public or any other business organisation in respect of the collection and disclosure of information. However, it has become a consequence of the legal principle of open justice that court reporters are deemed to be representatives of the public and good reasons (such as national security) have to be given for their exclusion from proceedings, even if temporary reporting restrictions are in place, and most importantly, even if the rest of the public is excluded. Other special privileges in connection with putative violations of privacy have grown up ad hoc.

In general, then, the law makes few distinctions between the position of the media and other individuals and businesses, in respect of rights to collect information or restrictions upon collection, whether on privacy grounds or otherwise. Yet, as we have seen, journalists often do collect information using methods that would be unlawful if used by private individuals, and, as we shall see in the next section, the courts do not always conclude from this, that the product should not be published.

Publication, disclosure and freedom of the media
Article 10 (1) of the European Convention provides that

Everyone has the right to freedom of expression. The right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.
The convention permits restrictions on the right of free speech provided that they meet certain conditions:

- They must be ‘prescribed according to law’: that is, clear, certain, predictable, and with sufficient precision to enable people to determine in advance whether a proposed course of action will be lawful.
- They must be ‘necessary in a democratic society’, that is, justified by a pressing social need.
- They must take the form of specific exceptions for national security, territorial integrity, public safety, prevention of crime or disorder, protection of health or morals, protection of reputation or rights of others, preventing disclosures received in confidence or maintaining the authority and impartiality of the judiciary: these must be specific exceptions and not balanced against the general freedom.
- They must be no greater than reasonably proportionate to the pressing social need.
- Expression may not put private interests in suppression above the right, nor does something that ‘pre-judges’ a matter that may at some later date become a matter of litigation amount, by that fact alone, to compromising the impartiality of the judiciary.

Of much longer standing in English law is the general presumption against prior restraint. However, prior restraint is sometimes granted by way of an interim injunction in certain types of case. The presumption is one in common law, rather than one with an unambiguous modern statutory basis, and the courts have made exceptions, such as in the case of injunctions having been sought and granted restraining publication or other disclosures in advance in the contexts of certain breaches of confidence. The Lord Chancellor, Lord Irvine of Lairg, in an interview in February 1998 suggested rather surprisingly that prior restraint might be exercised by the Press Complaints Commission, on news concerning ministerial private lives.
There are particular difficulties in making such restraints stick where publication has already taken place elsewhere in the world, but not in the domestic jurisdiction: in such cases, as the *Spycatcher* trials showed, it can be impossible to show that they will be effective. However, private individuals such as Hollywood stars, have managed to use breach of confidence to secure prior restraint against the publication of photographs in newspapers and magazines, even though they have appeared on the Internet, provided they can also demonstrate effective means of suppressing the Internet publication.\textsuperscript{147}

In those cases, there emerged a new principle that all those who ought to know of an injunction are bound by it and its spirit or else they are at hazard of contempt of court, even if their own case is quite different from that of the media body against whom the injunction was granted. The Attorney-General, who has wide discretion in ‘the public interest’ in decisions to prosecute or seek injunctions on behalf of government, has thereby acquired a role as a kind of occasional censor in cases where prior restraint is in question.

In the case of broadcast media, government retains statutory powers of censorship, which have been used in connection with Sinn Fein in 1988, and in time of war, but the powers are not restricted to conditions of emergency. In addition to national security justifications, obscenity and impartiality rules in connection with broadcasting have been used to justify prior restraint. However, there are no specific broadcasting rules permitting prior restraint by administrative action on the part of ministers or the regulatory bodies on grounds of breach of confidence or privacy.

**Confidentiality and breach of confidence**

Actions of several kinds in breach of confidence therefore provide the principal legal means in England whereby privacy concerns of individuals, rather than companies or government, may come into conflict with media freedom, whether through prior restraint or subsequent award of damages.
Article 8 of the European Convention states that:

(1) Everyone has the right to respect for his private and family life, his home and correspondence.

The exceptions permitted to this right are broadly the same as those permitted to the right to free speech, described above.

The convention is to be incorporated into British law, and thereafter, it will be for the courts to work out how to reconcile Articles 8 and 10.

Prior to the incorporation into British law the Convention, breach of confidence has been the usual civil action by which aggrieved people who feel their privacy has been violated through a disclosure – such as publication in the press – of something told in confidence.

Contract law

A confidentiality clause in a contract is in general likely to be regarded by the courts as enforceable. Even where such a term is absent, the courts may imply it. In particular, the courts have implied such terms in contracts of employment upon employees not to disclose lists of the employer’s clients, other commercially sensitive data, intellectual property, trade secrets, and so on. In this context, the trickiest area is that of ‘whistleblowing’, where an employee claims that the public interest overrides any implied term because of the rule that ‘there is no confidence as to the disclosure of iniquity’. That may protect individuals in some cases, but this will depend on whether the disclosure was made to the appropriate outlet. Going to the press may be less appropriate than going to a regulator, the police, or other public authority, depending on the nature of the misdemeanour on which the whistle is blown.

The quasi-tort of ‘breach of confidence’

Most violations of privacy occur where there is no formal contract between the parties. In the quasi-tort, which is an independent principle of equity, prior restraint by way of an interim injunction is granted more readily than in libel and defamation cases, on the grounds that
damages can compensate for loss of reputation, while a secret cannot be made confidential again by damages. In its most recent statement, the quasi-tort empowers the courts to restrain disclosure in cases where the information in question is:

- **Confidential in nature.** Declaring something to be confidential does not make it so, but confidentiality should be clear and natural in the circumstances, and the information must not be trivial.
- **Not in the public domain.** The information may remain protected even if there are a few people who know about it; however, confiders are expected to be well-informed about the nature of the risks in the environment of disclosure:

  Those who exchange confidences on a bus or rain run the risk of a nearby passenger with acute hearing or a more distant passenger who is adept at lip reading … When this is applied to telephone conversations, it appears to me that the speaker is taking such risks of being overheard as are inherent in the system.¹⁴⁸

This dictum was confined to legally authorised telephone tapping, and does not permit violations of the interception of communications laws, but it does raise questions about what degree of public domain will be implied into unencrypted e-mail sent across the Internet.

- **Entrusted to another in circumstances imposing an obligation not to disclose without consent.** Examples include relationships between spouses, close friends and members of the Cabinet. The nature of the relationship is not crucial, but rather the particular transaction of giving the information in confidence and acceptance on that basis, even if the
information was not expressly stated to be confidential but was clear from the surrounding circumstances that it was intended to be kept so.

○ *It is in the public interest to protect the confidentiality.* The right of confidentiality is a public, not a private right, and so there is no confidentiality if there is no public interest. It is not a question of balancing confidentiality and public interest, but of determining where the public interest lies. There is none in protecting ‘iniquity’, although it remains unclear whether this applies to suspicion of iniquity or only to proof. There is no public interest where the confidences are old and stale, and no longer worth protecting. A purely private individual or company can expect from the courts at least a general presumption that confidentiality in general is a valuable behaviour in the preservation of which there is a *prima facie* public interest, as can people abiding by professional codes of ethics on confidentiality. However, the public interest can condone underhand and deceitful means by which confidence is obtained and disclosed:

‘Some newspapers had many functions and practices, some more attractive than others, but one function was to provide a means whereby corruption might be exposed. That could rarely be done without informers and often breaches of confidence’

○ *Unauthorised disclosure must be to the detriment of the confider.* The information gained cannot be used as ‘springboard’ for actions detrimental to the plaintiff, of which there is a *prima facie* presumption that disclosure is one.

*Breach of confidence takes no account of wrongful collection*

What may seem surprising is the fact that the courts will not necessarily rule something to be a breach of confidence and therefore prevent disclosure on the grounds that illegal or reprehensible means were employed to
obtain the information. Information from stolen letters, from warranted telephone tapping, secret filming, photographing someone in a secluded place or where they believed they were alone, and covert unauthorised copying of information have all been found by courts not to be breaches of confidence. The principle is that there has to be some transaction between the parties before breach of confidence is available.

Photography in public places

‘No person possesses a right of preventing another person photographing him any more than he has the right of preventing another person giving a description of him.’ No one can prevent aerial photography over their land, although constant surveillance might amount – at least in theory – to nuisance, which would have a different remedy in tort, one that would have no connection with any right to prevent disclosure. However, stolen photographs can sometimes be protected, if there is a public interest and they are not in the public domain.

Private photographs

The Copyright, Designs and Patents Act 1988 provides that copyright belongs to the photographer, unless commissioned for private and domestic use, in which case it belongs to the commissioner. Use without consent – a species of privacy risk – is thereby a breach of the subject’s copyright only if the subject of the photograph owns the photograph by virtue of taking it themselves, or else has patented or copyrighted her or his own image generally. The litigation expected over the efforts by the trustees of the estate of Diana, Princess of Wales to achieve this for their late client will presumably determine the limits to which this can lawfully be done.

Data Protection Act 1998

The 1998 legislation on data protection grants the media wide exemptions from duties, where the personal information is undertaken with a view to the publication of any journalistic, literary or artistic material, the data controller believes publication to be in the public interest, and compliance with subject access would be incompatible with these purposes.
In particular, the exemption applies to the fair and lawful obtaining rule, in effect putting many information collection activities of the media beyond the reach of data protection law. In addition, the exemption covers rights of subject access, the right to prevent processing leading to damage or distress, correction or erasure and automated decision making.

Privacy and media self-regulation
The state of the law on the relationship between media freedom and privacy seems hardly to satisfy anyone. Certainly, the corpus of law is untidy, lacking in consistency and inadequate because of the range of privacy risks over which it affords little or no protection.

There have been a series of official enquiries in Britain into issues of privacy and the press since the end of the second world war, including Ross (1949), Shawcross (1962), Younger (1972), McGregor (1977), Calcutt (1990 and 1993), of which the last was preceded by several private members' bills proposing a statutory right to privacy, and followed by a Select Committee enquiry and a formal government response.151

Calcutt concluded that the Press Complaints Commission had been ineffective and that the press would not change its ways. He called for a wholly independent statutory regulator with powers of prior restraint of publication of any material obtained in ways that violated the code, and also of imposing fines and awarding costs. He also proposed new criminal offences on physical intrusion, specifically on physical entry into private property for the purpose of obtaining information for publication, placing bugging devices on private property, photographing or sound recording individuals on private property without consent, and civil remedies on privacy. The government's response was that it proved intractable to design the drafting of offences that would catch all and only those abuses without also preventing journalism in the public interest, and for which evidence could practically be obtained in any prosecution. In the consultation in Scotland on a new statutory privacy tort, there was widespread support for such a reform, but the government concluded that there was not sufficient support for the introduction of legislation.
It has been difficult to tackle the problems head-on by way of legislation because of the difficulties of avoiding draconian measures and also because of the political difficulties facing any government that seeks to legislate to curb media power, and the capacity of the media to target its investigative powers upon any ministers contemplating introducing such curbs. Therefore, successive governments have tried instead to encourage self-regulation, the adoption of collective complaints systems by the media, and the development of codes of practice.

The Press Complaints Commission code of practice recently revised following the public dismay at the actions of the paparazzi photographers in pursuit of Diana, Princess of Wales in the car chase that led to her death, was described by the Commission as tougher on breaches of privacy than its predecessor. It sets its face against deliberate inaccuracy, and calls for corrections with due prominence. Some key clauses are the following:

### 3. Privacy

1. Everyone is entitled to respect for his or her private and family life, home, health and correspondence. A publication will be expected to justify intrusions into any individual’s private life without consent.
2. The use of long lens photography to take pictures of people in private places without their consent is unacceptable. Note – Private places are public or private property where there is a reasonable expectation of privacy.

### 4. Harassment

1. Journalists and photographers must neither obtain nor seek to obtain information or pictures through intimidation, harassment or persistent pursuit.
2. They must not photograph individuals in private places (as defined in the note to Clause 3) without their consent; must not persist in telephoning, questioning, pursuing or
photographing individuals after having been asked to desist; must not remain on their property after having been asked to leave, and must not follow them.

3. Editors must ensure that those working for them comply with these requirements and must not publish material from other sources which does not meet these requirements.

6. Children
   1. Young people should be free to complete their time at school without unnecessary intrusion.
   3. Pupils must not be approached or photographed while at school without the permission of the school authorities.

8. Listening devices
Journalists must not obtain or publish material obtained by clandestine listening devices or by intercepting private telephone conversations.

9. Hospitals
   1. The restrictions on intruding into privacy are particularly relevant to enquiries about individuals in hospitals or similar institutions.

11. Misrepresentation
   1. Journalists must not generally obtain or seek to obtain information or pictures through misrepresentation or subterfuge.
   2. Documents or photographers should be removed only with the consent of the owner.
   3. Subterfuge can be justified only in the public interest and only when material cannot be obtained by any other means.
The future of privacy

**Public interest**

There may be exceptions to these clauses [all quoted above] where they can be demonstrated to be in the public interest

1. The public interest includes:
   (i) detecting or exposing crime or a serious misdemeanour
   (ii) preventing the public from being misled by some statement or action and individual or organisation.

2. In any case where the public interest is invoked, the Press Complaints Commission will require a full explanation by the editor demonstrating how the public interest was served.

3. In cases involving children, editors must demonstrate an exceptional public interest to over-ride the normal paramount interest of the child.

The Code does indeed include new statements on privacy and a clause on persistent harassment. The definition of private places is new and an important improvement: the old one was ‘a private residence, together with its garden and outbuildings … but excluding the surrounding parts of the property with the unaided view of passers-by; hotel bedrooms (but not other areas of a hotel); those parts of a hospital or nursing home where patients are treated or accommodated.’

However, there are many aspects of concern about media ethics in information gathering and collection that are not dealt with. Payments to witnesses and people with criminal convictions are ruled out but payments to people to release personal information are not mentioned (no doubt the PCC would say that it is unnecessary to remind journalists of the data protection laws, but some certainly do need a reminder).

Finally, the public interest exception seems to run widely and is not well defined: indeed, it is largely left to the self-regulation of the editors in the PCC to determine whether the public interest was served. That a public interest exception is permitted in the case of subterfuge is perhaps less than reassuring. The subterfuge clause is silent on the specific issue of entrapment or incitement to commit misdemeanours, although
the PCC might suggest that such a prohibition, save when in the public interest, is implied.

The key issue is whether the public can trust the PCC to enforce the code, and whether the sanctions it has at its disposal are sufficiently tough that they will outweigh the profits to be gained from increased sales arising from a ‘scoop’ achieved using violations. The track record of the PCC and its predecessor bodies is not wholly encouraging in this regard.

The Broadcasting Standards Commission has also recently revised its own Code on Fairness and Privacy, which took effect from the beginning of 1998. Some important clauses follow.153

**Deception**

13. Factual programme makers should not normally obtain or seek information or pictures through misrepresentation, except where disclosure is reasonably believed to serve an overriding public interest and the material cannot reasonably be obtained by any other means. Where the use of deception is judged permissible, it should always be proportionate to the alleged wrong-doing and should wherever possible avoid the encouragement of conduct which might not have occurred at all but for the intervention of the programme-maker. Prior editorial approval at the most senior editorial levels within the broadcasting organisation should be obtained for such methods. The programme should also make clear to the audience the means used to obtain access to the information, unless this places sources at risk.

**Privacy**

14. An infringement of privacy has to be justified by an overriding public interest in disclosure of the information. This would include revealing or detecting crime or disreputable behaviour, protecting public health or safety, exposing misleading claims made by individuals or organisations, or disclosing significant incompetence in public office. Moreover, the means of
obtaining the information must be proportionate to the matter under investigation.

16. When broadcasters are covering events in public places, they should ensure that the words spoken or images shown are sufficiently in the public domain to justify their broadcast without the consent of the individuals concerned. When filming or recording in institutions, organisations or agencies where permission has been given by the relevant authority or management, broadcasters are under no obligation to seek the individual consent or employees or others whose appearance is incidental or where they are essentially anonymous members of the general public. However, in clearly sensitive situations in places such as hospitals or prisons or police stations, individual consent should normally be obtained unless their identity has been concealed. Broadcasters should take similar care with material recorded by CCTV cameras to ensure identifiable individuals are treated fairly. Any exceptions to the requirement of individual consent would have to be justified by an overriding public interest.

17. People in the public eye, either through the position they hold or the publicity they attract, are in a special position. However, not all matters which interest the public are in the public interest. Even when personal matters become the proper subject of enquiry, people in the public eye or their immediate family or friends do not forfeit the right to privacy, though there may be occasions where private behaviour raises broader public issues either through the nature of the behaviour itself or by the consequences of its becoming widely known. But any information broadcast should be significant as well as true.

18. The use of secret recording should only be considered where it is necessary to the credibility and authenticity of the story … Where recording does take place secretly in public
places, the words or images recorded should serve an overriding public interest to justify the decision to gather the material, the actual recording and the broadcast.

The BSC Code is in general a longer, more detailed and more reflective document than that of that produced by the PCC. In a number of respects, its code is the stricter, particularly in respect of subterfuge, the principle of proportionality in any justified breaches of privacy, and in a number of detailed provisions on door-stepping. However, a key weakness of the BSC code is that it deals more with the period when recording or shooting, and says less about the ethics of background research for programmes, where privacy violations of various kinds are also possible.

**Conclusion: the balance of forces for privacy in the media**

It is clear that in many respects, the debate has moved on and developed in sophistication since Calcutt and even since the 1995 White Paper which responded to debate initiated then. The focus on defining protected geographical space around individuals in property terms is slowly beginning to fade, as the new definition of ‘private place’ in the PCC code shows. Calcutt’s preference for innovation in criminal rather than civil remedies has rather lost its attraction in the years since his report, and indeed, internationally, both in the US\(^\text{154}\) and Germany,\(^\text{155}\) it has long been civil remedies that have been the more effective, notwithstanding the difficulties in designing effective and acceptable statutory torts.\(^\text{156}\)

The quality of the codes produced by the self-regulatory bodies has improved much faster than their real efficacy in disciplining the media on privacy. Entrapment – or something not very far from it – is still practised, as was shown in the case of the journalist who appears to have induced the son of a cabinet minister to sell a small portion of cannabis;\(^\text{157}\) doorstepping is relatively common place among some tabloid newspapers; and some sharp practices are in regular use when
gathering background information on a subject. The case for a new statutory tort will not go away, and in many ways, the improved drafting of codes has provided Parliamentary Counsel with better raw materials with which to work than were available when Calcutt was preparing his report.

The incorporation of the European Convention on Human Rights will not force any British government to introduce a statutory tort, and the view of the present government is that they will leave it to the courts to implement the law and to find a way of reconciling Articles 8 and 10 with each other and with the inheritance of English law of breach of confidence, interception of communications, data protection, law of tort on nuisance, harassment, trespass and criminal law on theft and deception.

This policy may yet prove to be a bed of nails for government and media alike, and still may do little to enhance privacy. While the exemptions for the press from data protection law have staved off privacy controls on the press from that quarter the European Convention may open the way for more activist and innovative development of the law by the courts of appeal. While it may be possible, if the ‘right’ kinds of cases present themselves, for the higher courts to develop a reconciliation of these interests, there are limits to the extent to which the courts alone can close gaps, reconcile competing principles and integrate bodies of law that Parliament has left in a degraded state.

The commercial imperatives that drive the press toward intrusion, which are created in part by the steady extension of the star system from its original home in the film industry, throughout many other areas of life, are not weakening. The view that celebrities are ‘fair game’ may be widely held, but the view is perhaps less widely or consistently held, that the violation of the privacy of involuntary celebrities or ordinary people thrust into the limelight is an acceptable price to pay in order to prevent the rich, famous and powerful from escaping with wrong-doing. Popular views of the extent to which those who chose to become, or even those who have reluctantly become, public figures forfeit privacy rights are in turn influenced by the self-serving arguments of the popular press. However, the usual concomitant of that
view, namely that the only people who want privacy are people with something shameful to hide that ought to be exposed, is one that does not, in other privacy contexts, commend itself to the public. As we have seen in contexts where privacy is usually conceived by lawyers in data protection terms, the public may be willing to consent to data collections, but under clear and strict conditions, and the presumption of innocence even in privacy is deeply valued.

But the media system of stardom that sustains a concept of the celebrity as fair game is only part of the story. Much of the future of press privacy ethics turns not so much on ideas about privacy as about private life itself. By this, I mean that it turns on the issue which inferences we think unjust or fair because they amount to a basically unsound or basically sound intuition about what people are like.

When a politician’s adultery is exposed, the conventional justification for publicising what is usually a rather sad, even pathetic, business is that it is reliable inference that someone who can cheats on his or her spouse will be of such a deficient moral character that she or he is unfit for public office or any form of trust or responsibility. (Clearly, this is not applied to the form of high public office and trust that media editors feel themselves to occupy.)

One could imagine – without necessarily wholly admiring – a society in which whenever that kind of claim was put forward, its truth or otherwise was debated on the facts of the particular case. In some cases, the ability and willingness to deceive might be the sign of a generalised character flaw, while in others, it might be confined to the behavioural compartment of a person’s sexual conduct. The prospect of putting public figures through some kind of moral investigation of character in which they seek to demonstrate the latter and their critics the former is one that most of us would find tawdry. But it is at least possible that a society could think in that way about such claims.

However, the conventional debate about the relationship of private life with public role – not only in political or administrative office but also in business, acting, music and elsewhere – in our society is not conducted in this way. Rather, the claim is not taken to be an empirical one at all. It is often taken by editors and pundits to be a kind of
dogma, which, once uttered, can only be countered with the equivalent and contrary dogma that the private sin is – save in the case of the really criminal – sequestered from the public role.

That we have arrived at these coarse and simple-minded conceptions of private life was not inevitable, nor is it inevitable that we should cleave to them indefinitely. However, they are sustained by powerful cultures of confessionalism and the ambivalent culture in Britain that any one who is successful deserves either idolatry or else bringing down, and that by virtue of their success, the successful hold their private lives publicly accountable to these competing dogmas. In terms of the four traditions about private life identified in Part 1, this shows a continuing and perhaps surprising egalitarian streak in an otherwise liberal culture.

Indeed, the debate about privacy regulation and the media exhibits once again one of the key fractures in the liberal culture with which this book is concerned: namely, between the economic liberalism of the media proprietors, for whom the issues of dignity take second place to the issue of freedom to dispose of one’s property, and political liberalism, itself fractured between considerations of freedom of speech and privacy, each of which yield competing forms of restraint upon the media whether though cross-media ownership and rights of reply or else through the controls on collection of personal information.
1. A serviceable definition of personal information is that offered by Wacks P, 1989, *Personal information: privacy and the law*, Oxford University Press, Oxford, 26: 'those facts, communications, or opinions which relate to the individual and which it would be reasonable to expect him or her to regard as intimate or sensitive and therefore to want to withhold or at least to restrict their collection, use or circulation.' This would be narrower than the definition of personal data in the 1984 Data Protection Act: 'Information that can be processed automatically and which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user)', but for the specific exemption of indications of the intention of the data user in respect of that individual. The impact of the implementing legislation for the 1995 EU Data Protection Directive in the UK will be to extend the definition of personal data covered by the Act from those that can be processed automatically to all records, including those recorded and held manually, and will remove the exemption for indications of intention. For the purposes of this volume, the term is understood in the broader sense that the 1998 Data Protection Act will bring into effect, rather than Wacks' narrower one.


8. This is, of course, the mid-twentieth century concern with the powers of the totalitarian state that inspired Orwell's grim vision in 1984. Of course, it remains an important element in privacy discourse: see for example Margalit A, 1996, The decent society, Harvard University Press, Cambridge, Massachusetts, ch. 12.


11. The time squeeze, Demos Quarterly, issue 4.


The future of privacy


27. Unpublished research by the Office of the Data Protection Registrar.


34. It is too early yet to tell whether there is a case of market failure or other social problem here that would call for government intervention. If the numbers of people denied insurance or only offered non-standard terms with very high premia are large, then there may be a case, if life insurance becomes a necessary passport to other essential activities or services, for some kind of government intervention, although probably on a targeted rather than universalistic basis.


39. This is the interpretation of a version of now canonical distinction between privacy pragmatism, fundamentalism and unconcern offered by Hine C, Eve J and Woolgar S, 1996, Privacy in the electronic marketplace, Centre for Research into Innovation, Culture and Technology, Brunel University, Uxbridge. In cultural theoretic terms, it corresponds to the ‘mobility hypothesis’ that cultural biases form a repertoire on which individuals may draw in particular contexts, subject to local institutional pressures and perhaps some underlying impulses capable of being overridden: Rayner S, 1992, ‘Cultural theory and risk analysis’ in Krimsky S and Golding D, Social theories of risk, Praeger Press, Westport, Connecticut, 109–110.


49. Castells M, 1989, The informational city: information technology, economic restructuring, and


55. Although many of those who use the word 'capitalism' are its opponents, I have no wish to associate myself with them. While many friends of the market tend to eschew the word, there are good reasons for retaining it. It can be read as stressing not just a certain means of exchange but a system of private property rights and a presumption in favour of reconciling the goals of regulation in civil liberties, human dignity and social cohesion with as much liberty of business activity as possible, and a belief that such a reconciliation is possible, although its terms must constantly shift as markets, cultures and technologies do. For an example of a pro-capitalist thinker who is not ashamed of the word, see Seldon A, 1990, *Capitalism*, Blackwell, Oxford.


57. See Volume 2, ch. 2.

58. Evans M, O'Malley L and Patterson M, 1997, 'UK consumer attitudes toward direct mail: an empirical investigation', paper presented at the American Marketing Association Conference, Dublin, June, found in their small survey that inaccuracy-related risks were statistically significant as a factor in explaining negative attitudes towards direct mail generally.


67. Unpublished MORI data.

68. Facial recognition technology is sometimes used in connection with control room monitored CCTV by private security firms. This matches facial images on camera to a local database of ‘known’ or ‘potential’ offenders. The system operator is automatically alerted to a ‘threatening’ presence and informal intervention becomes an option.’ Coleman R and Sim J, 1996, ‘From dockyards to Disney store: surveillance, risk and security in Liverpool city centre’, paper presented at the Law and Society Association conference, University of Strathclyde, July 1996.


74. For details of a current British scheme in Leicester, see ‘City launches first pay-to-drive trial’, Guardian, 23 July 1997.

75. For details of a similar scheme in California, see Agre PE, 1997, ‘Beyond the mirror world: privacy and the representational practices of computing’ in Agre PE and Rotenberg M, eds, Technology and privacy: the new landscape,


87. For a comprehensive overview of the risks, albeit from an occasionally rather alarmist view point, see the monumental work of Schwartau W, 1996, Information warfare – cyberterrorism: protecting your personal security in the electronic age, Thunder’s Mouth Press, New York. I have relied heavily on this text as well as on more journalistic material for the following paragraphs. See, for example, Valeri L, 1998, ‘On the dark side’, Information Strategy, 3,3, 22–23.

88. It has, since the ironic extension of the meaning of the word by some science fiction writers such as Neal Stephenson and William Gibson to cover any kind of computer expertise in the dystopian worlds where the distinction between the lawful and unlawful has collapsed, become more widely used to mean anyone with programming or similar ability.

90. For an application of these technologies to document signatures to provide trust in the authenticity and source of a document in a distributed electronic library, see Anderson RJ, Matyas V Jr, Petitcolas FA, Buchan IE and Hanka R, 1997, ‘Secure books: protecting the distribution of knowledge’, unpublished paper, Computer Laboratory, University of Cambridge.

91. The key source on PETs is Registratiekamer Netherlands and Information and Privacy Commissioner Ontario, 1995, *Privacy enhancing technologies: the path to anonymity Vols I-II*, Registratiekamer Netherlands, Rijswijk and Information and Privacy Commissioner Ontario, Toronto.


93. Personal communication, Office of the Data Protection Registrar.


102. For guidance to probation officers on such joint coordinated arrangements, see Home Office,


111. It is a powerful measure of how moral panics and media scares can change the priorities that a book on privacy in the social services as recently as 1995 could make the issue of disclosures and paedophiles a relatively minor theme: Thomas T, 1995, *Privacy and social services*, Arena, Aldershot.


offenders list next month,' The Times, 12 August 1997; and leader article Ford R, 'A balance of rights: the register should be a tripwire, not a branding iron,' The Times, 12 August 1997.


118. 'Paedophiles in secrecy test,' Guardian, 1 July 1997.

119. For example, Betts RK, 1997, 'The new threats of mass destruction,' Foreign Affairs, Jan/Feb, 77, 1, 26–41, says that, in the face of the possibility – which has, as yet, not occurred – that terrorists will secure access to biological, chemical and nuclear weapons, and considering the arbitrary luck with which such terrorists as Timothy McVeigh were caught and the problems of internment without trial large numbers of foreign nationals, 'Those who fear compromising civil liberties with permissive standards for government snooping should consider what is likely to happen once such luck runs out and it proves impossible to identify perpetrators … Stretching limits on domestic surveillance to reduce the chances of facing such choices could be the lesser evil.'


125. ‘Phone tap laws to be reviewed,’ Financial Times, 16 July 1997.


127. Kuruma v R, 1955, AC 197, PC.


131. Sources include: Data Protection Bill 1998 (as published 16 January 1998); Secretary of State for the Home Department, 1997, Data protection: the government's proposals, CM 2725, The Stationery Office, London; Directive 95/46/EC On the protection of individuals with regard to the processing of personal data and on the free movement of such data

132. ‘US, EU at odds over Internet data protection,' Financial Times, 10 July 1997.

The future of privacy


138. The German courts sometimes talk in data protection of information self-determination, 'Selbstbestimmung,' but it is not clear whether this is intended to imply some kind of property right in any personal information pertaining to one in the hands of others.


141. This is a slightly different statement of the issue from that offered by Raab (Raab CD, 1993, 'Information technology and the production of privacy' in Gornostaev J and Thomas R, eds, Proceedings of the international conference on information technology and people, International Centre for Scientific and Technical Information (ICSTI), 5–12; Raab CD, 1993, 'The governance of data protection' in Kooiman J, ed, Modern governance: new government-society interactions, Sage, London, 89–104; Raab CD, 1997, 'Co-producing data protection', International Review of Law, Computers and Technology, 1,1, 11–24) that a large and complex network of actors is engaged in the co-production of privacy, and that voluntary codes, whistleblowers, professional ethics, individual consumers’ own strategies are play as important a role as direct ‘top down’ regulatory enforcement. The point is certainly true, but the argument here is that it is necessary to take the argument further to explore the style of regulation that will enable this, and that will in turn be supported by this.


145. For a comprehensive overview of privacy enhancing technologies, see Information and Privacy Commissioner, Ontario, Canada and Registratiekamer, The Netherlands, 1995, Privacy
enhancing technologies: the path to anonymity, vols I and II, Information and Privacy Commissioner, Ontario, Canada and Registratiekamer, The Netherlands, Toronto and Fijswijk.


147. A recent case of his type involved the actor Brad Pitt and his partner, who were photographed having sex, lost control of the photographs but successfully prevented newspapers and magazines from using them, on the basis that they were able to identify the owners of the Internet sites displaying them and serve effective injunctions upon them also. Had they been unable to do so, they might have faced the same problems that the British government did in the Spycatcher cases.

148. Per Sir Robert Megarry VC in Malone v Metropolitan Police Commissioner (No 2), 1979 2 WLR 700.

149. Per Mr Justice Scott, in Cork v McVicar, 31 October 1985.


Part 3
Futures of privacy and private life
12 Toward futures for privacy

This part is devoted to developing the forces for change into a short series of preliminary scenarios for the future of privacy.\(^1\) It is important to think about the future of privacy for several reasons. In devising frameworks to think about policy choice, it is vital to think about the future habitat in which policies must make their way, and to recognise that those habitats may be different – perhaps very different – from those in which they are devised.\(^2\)

On the other hand, forecasting has proven to be a deeply disappointing business. Short range meteorological forecasting has fared tolerably well, as has short range pattern seeking forecasting for small numbers of share prices. However, economic forecasting, epidemiological forecasting and technology forecasting exercises, although undertaken frequently enough, have all proven regularly misleading. Few major companies or governments now make major investment decisions solely on the basis of forecasts, so grave have the errors been. Even when forecasting techniques have used nonlinear methods, data problems and sensitivity to initial conditions, sheer complexity and the perversity (by the standards of our available models) of human choices have left us with forecasting tools of limited usefulness.

The are several merits of the scenario approach, which devises possible futures and uses them to identify risks and opportunities and to challenge assumptions, rather than to assess probabilities or make predictions. In such exercises, the multiplicity of scenarios developed is an
important analytical tool in strategy, for it disciplines actors to think
through contingencies and to devise strategic responses that are
*robust*, that is, that are at least tolerably sensible in more than one
interesting scenario. We all carry with us implicit and inadequately
reflected-upon future scenarios about any subject with which we deal,
and the process of building explicit scenarios can be an important way
of dislodging some unexamined assumptions and mental maps we
have taken for granted.

Moreover, possible future scenarios are important ways of identify-
ing and assessing both risks and opportunities. In this connection,
therefore, in the 1990s the approach has migrated from the setting of
corporate strategic planning into public policy, where it has drawn on
a wide variety of related and compatible approaches from systems
thinking, organisational analysis and policy development.³

It is important not to claim too much for scenario building. Good
scenario building work turns away from problems that it is not well
equipped to solve. Where a problem cannot be structured in a way that
enables the scenario builder to do more than ‘join up the dots’ arbitrar-
ily between variables, the technique is probably not the most suitable.
This chapter argues that, in this field, conventional scenario building
techniques produce uninteresting results. Therefore, we shall need to
change the question and to augment these techniques.

A common reaction to any set of scenarios is a dismissive ‘but
they’re all aspects of what is happening now’. While it is certainly a
damaging criticism to say that a set of scenarios fails to be challenging,
on the other hand, a set of scenarios that are so surprising and unlikely
as to be of minor interest to policy makers and others in a field is per-
haps a sin at least as serious. In some measure, all modelling exercises
are caricatures: they take something familiar and stretch it until sud-
denly we see in the caricature some aspect of our lives that we would
not see in a photograph, map or history textbook. Scenarios are no dif-
ferent. As caricatures of possible futures, they are also caricatures of
partial presents. By highlighting forces, trends, mechanisms, dynamics,
balances and imbalances, they serve to help us to identify and assess
risks and opportunities and to challenge assumptions.
None of the scenarios offered for 2010 in this book is unrecognisable. Nor should any scenario for twelve years hence be wholly unrecognisable, in the way that, say, a scenario for 2030 probably ought to be. While history moves quickly and a week, to misquote the late Harold Wilson, is a long time in cultural change, twelve years is not a long period in a field like privacy and private life, where technologies can take more than a decade to mature, where the differing expectations of privacy are durable, where cultures of large organisations take years to change, and where cycles in social movements are relatively long. On the other hand, the risks of irrelevance and thinness in trying to paint scenarios for privacy and private life in 2020 or beyond are so great that it is better not to try.

The structure of the chapters in this part is as follows. In Chapter 13, the conventional off-the-peg scenarios on the future of privacy that provide the mental maps for many people are described and criticised for excessive simple mindedness, poor understanding of causal dynamics and weak structure. Chapter 14 contains the apparatus with which a more sophisticated approach is developed. The material from Part 2 on the key drivers of change is synthesised using a certainty-importance grid and cross-impact analysis. Chapter 15 develops insights from the recent use of cultural theory and, in particular, cultural dynamics, to introduce a new and more powerful approach to building scenarios.

In particular, scenarios are required that are culturally viable, in two senses. First, good scenarios for the future of privacy must recognise the mutual dependence and mutual tensions of all the four cultural traditions through which our conceptions and practices of privacy are refracted. Secondly, the goal for the strategic or policy discussions in Part 4 must be to devise strategies that make intelligent use of the dynamics of the relationship between the four cultures of privacy, work with a variety of possible temporary and shifting coalitions between them, and are sufficiently robust to make some sense in as wide as possible a group of scenarios in which different cultures play leading roles. Taking these scenarios seriously requires governments, businesses and individuals to entertain the making of certain types of decision in the next few years, and it is the intention of Chapters 14 and 15 to identify these.
The conventional wisdom about privacy’s future can best be summed up in two simple scenarios about the future. These narratives have changed little since the post-war era, although the technological details have been updated.

**The dataveillance society**

The contemporary form of the Orwellian surveillance society scenario is the ‘dataveillance society’, in which privacy is routinely overridden by ever more powerful systems of data collection, storage, exchange, matching and mining operating across private global networks without the capacity for most individuals to discover what is held about them or how it is used to make decisions about their fate. This scenario is frequently set out in the writings of civil liberty pressure group activists. Their argument is that digital technologies have made it more likely than the analogue technologies familiar in the post-war era could ever have, and that the information economy has given business and government ever more reason to pursue the creation of such a society. ‘What is happening is nothing short of an orchestrated effort to bring the public to heel … privacy has been all but engineered to destruction, so the odds are stacked in favour of the superhighway supremos.’ In one version of this scenario, privacy concerns simply dwindle away, as people cease to hanker for that which is no longer
feasible: this version of the scenario is sometimes set out by gung-ho technologists. The social experiment with privacy as a model of sovereign individualism comes to an end in a morass of informational networks.

**Crypto-anarchy**

The opposite scenario starts from the premise that strong cryptography will be universally and cheaply available in the hands of private individuals. In this scenario, technologies of decryption have been outstripped by the advent of public key cryptography using very long strings of bits for keys. In this situation, digital crime becomes virtually undetectable, companies find it almost impossible to secure their data against their own employees, and electronic sabotage becomes commonplace. ‘Encryption always wins’ (emphasis in original text).

Privacy is delivered, almost universally, but with anarchic consequences, because everyone works with so many digital identities and communicates with such secrecy that government and business agencies find it almost impossible to build up workable profiles of individuals. The golden age of privacy is delivered by privacy enhancing technologies, but it turns out to be a crisis for law and order, and for business. Economic growth suffers, and governability is threatened.

**Appraising the two standard scenarios**

These conventional scenarios share some common themes. The first scenario is the dystopia of the extreme civil libertarian, while the second is the law enforcement agency’s nightmare. Each group is willing to use its nightmares in order to alarm people into supporting their peculiar claims for protections or resources.

Both are technologically deterministic in the sense that both assume that technology does not run into any effective cultural or political resistance. Problems of trust do not derail dataveillance any more than popular fear of crime and disorder or the commonplace desire to establish the trustworthiness of others undermine crypto-anarchy. In neither scenario is the future negotiated between interests,
but enforced by the overall victor in a technological arms race between encrypter and decrypter. More fundamentally, even if strong cryptography and the capacity to generate and use multiple identities is universally available, it seems unlikely that the majority of the population would have any reason to actually conduct themselves in that way.

There is a second fundamental error in these two conventional scenarios. Both assume rather simple-mindedly that the future of privacy will be shaped by a single kind of causal mechanism – namely, that of positive feedback. Positive feedback occurs whenever a process is reinforced, a trend of growth or decline continues, when institutionalisation and lock-in or path dependency occurs, and when no countervailing force to dampen the effect or conflict with it can be effective.

In fact, any social system of the complexity that characterises cultural dynamics on questions of central values will exhibit many kinds of causal mechanism, of which positive feedback will be but one. Negative feedback – or the counterbalancing of a trend by conflict, reaction, resistance, the working out of internal tensions within a trend, a trend overreaching itself and exhausting its resources for continuation, or simple regression to the mean – is a category of some of the most important mechanisms by which systems are governed.9

Any technological dynamic such as those proposed in the dataveil- lance society or crypto-anarchy would surely set off some negative feedback from one or other of the cultural biases and traditions of sensibility offended by these processes. In the dataveillance society, it is quite plausible to imagine that a temporary liberal-egalitarian alliance could be formed that would seek and perhaps secure at least some enforceable constitutional restrictions on the use of dataveillance technologies and methods, leaving civic republicans with few allies (fatalists are weak allies for any culture). After all, the radical movements of the late eighteenth century in the United States, France and Britain all displayed this cultural character in reaction to a less technologically sophisticated system which they perceived as despotic. Equally, in crypto-anarchy, civic republicans and liberals would be able to make common cause against the egalitarians and extreme liberal-libertarians, around the theme of the security of property rights and the need for
economic order, and, because they form the more powerful diagonal, it is likely that they would be successful in at least some of their demands.

This kind of thinking is too simple. Power over information is partly in the hands of individuals, and could be more so, but is not likely to lead to crypto-anarchy simply because too few people have any interest in such a grim outcome. Neither government nor business is as sinister as the extreme civil libertarians paint them. Both need to secure their legitimacy with the public. Pressure groups will continue to put pressure on both public and private sectors. Some institutional forces are in place that can provide some security against the new risks to privacy. Privacy will always be a contested business, but there are choices to be made, which the determinism of the conventional wisdom fails to recognise. Insofar as these conventional wisdoms have contributed to fatalism about privacy, they have done great damage.

This kind of fatalism is misguided. For we have the power for the first time to make privacy concerns central to the design of business and governmental information systems. There are now practical measures that governments, businesses and individuals can take that can bring real enhancements of privacy. Scenario methods that rely on a single driver of change and tell too simple a story about even that force – be it information and communications technology or the economics of informational capitalism – simply reinforce fatalism. It is time therefore to try more sophisticated approaches to thinking about the future.

**Markets in privacy**

A third kind of future scenario for privacy is sometimes offered. The key shaping idea in this scenario is that a combination of the enormous global economic forces that have liberalised regulation, created climates of free trade, opened up markets and competition (where once there were monopolies either guaranteed by state mandate or effectively supported by regulation), and the new technologies that enable the breaking down of mass market services to the ‘market place of one’, will enable the establishment of markets in privacy itself.10
That is to say, we will be able to design services so that individuals will be able to specify the confidentiality and nondisclosure rules, the encryption protection for transactions, and the limits on the purposes for which their personal information will be used, but will have to expect to pay the going rate for the level of privacy that they want. In this scenario, information and communications technology will upload to any retailer or government agency from the consumer’s own software in their digital television, mobile phone, personal computer or smart card, a set of conventions that the consumer has chosen for the use of their personal information in transactions of the kind in question. In return, and in real time, a price will be quoted to the consumer from the supplier’s software that reflects the price the supplier charges for transactions at the level of privacy protection the consumer wants.11

In this scenario, not only does the consumer take more responsibility than many are prepared to do today, for specifying the information ethics with which they make decisions about what and how to purchase, but perhaps the consumer would also bear more of the liability for the information outcomes if a level of privacy or a transaction was chosen that was lower, in retrospect, than would have been liked. In this variant of the scenario, the consumer effectively opts out of statutory data protection law in return for protection solely in contract law.

The conceptual basis of this scenario is that certain kinds of personal information become the personal property of the individual, to trade as they see fit for goods and services, at whatever price they can afford to pay for retaining control over the use of their property. The aim is the deregulation of the market in personal information and the reintroduction of diversity, choice and preference through the power of the individual to contract – and the capacity of new information and communication technologies to manage – many different prices for goods and services bought and sold with different levels of privacy attaching to the data capture at the point of sale.

The human rights perspective on privacy that has informed European privacy law is quite misguided, at least in respect of the commercial sector: the human interest in privacy is not of the same
order as that in, say, not being tortured. As one advocate of making this scenario a strategic goal puts it, ‘You might argue that somebody’s privacy could justifiably be sacrificed in the public interest, but you could never argue that somebody should be tortured on such grounds.’

While many businesses use personal information to target the rich, many other down-market businesses emerge to target the less well off, and both need data with which to carry out the segmentation: the question for each market segment is what it will take to elicit personal information from customers and potential customers. In the neo-liberal view, there is no particular unfairness if the poor choose to sustain standards of living above a level that they would be able to afford if they demanded more privacy and paid for it, and the rich could afford both high standards of living and all the privacy they desired. Reasonably enough, people tend to adjust their preferences for privacy, as for any other service, to their income level. It is not appropriate or defensible, liberals argue, for data protection regulation to be used as an instrument of redistribution of privacy services to the poor. Indeed, they argue, it is not necessarily the case that higher levels of privacy will be more costly. After all, in some markets, the trade in personal information may work the other way around. Suppliers will have to pay individuals to elicit personal information from them in areas where people are reluctant to trust or where the information sought is particularly sensitive, just as today companies must offer personalisation of services, discounts, or other incentives to people to seduce them into joining loyalty schemes.

To the extent that government is engaged in the provision of coercive services or the provision of services without prices, or where there are other compelling reasons of equity for government to charge the same fee to everyone who wants a service, this scenario assumes that some other mechanism will have to be put in place to deal with privacy issues in the public sector. This looks very similar to an idealised version of the US model, where the Privacy Act 1974 governs federal activities, and state laws perform a similar function, but there as yet is no overarching, detailed and comprehensive privacy regulation in the private sector (although this could emerge).
In Part 4, I shall consider the attractiveness of this scenario as a putative goal of public policy. For the present purpose, however, we need to examine only its coherence, the credibility of the narrative that leads from here to its destination, and the extent to which it is sustainable.

One question that will occur naturally to commercial strategists in consumer relations about this scenario is this. Even assuming that a manageably small number of standard privacy packages can be devised that would be acceptable to a variety of consumers and suppliers and software can be written to handle such pricing complexity at the point of sale without creating even longer queues at the checkout till, it is not yet shown that more than a minority of consumers are sufficiently sophisticated to be able to set a realistic price on the value to commercial organisations of their personal information, and then to bargain effectively. That some consumers are is not in doubt. These are relatively highly educated, relatively affluent, high value customers for whom there will be much commercial competition in any case. But the less affluent and less well educated consumers tend to be less confident about putting such a price on their information. In this situation, the market in privacy could become a suppliers’ market, and very far from the consumer driven responsive world described by conventional neoliberal views.

The second question about the coherence of the scenario concerns the idea of the price for personal information. Executives in many of the largest and technologically most advanced corporations will admit privately that they make much less use of their vast banks of data than in principle they could, for reasons of time, cost, urgency of other priorities, the costs of using more finely disaggregated data in highly targeted marketing, and the dangers of making mistakes from trying to be too clever about getting close to the customer. Nevertheless, they remain committed to the view that when costs fall and they find better ways to avoid alienating consumers by making inferences about individuals that prove to be wrong, they will continue to get closer to the customers. The logical conclusion from these admissions is that probably many businesses do not know the exact value of the personal information they hold. Particularly when one factors in the dynamics
of innovation in fast moving consumer markets, which can change overnight the value of personal information held.

If businesses are in this position, then it is almost impossible for me, as a consumer, to know exactly what the value is to high street retailers of apparently simple but actually highly suggestive pieces of information about me: my preferred newspaper, say, or the regularity with which I buy socks or red wine. How, then, can I set a price on it and bargain accordingly? I quickly become the captive of the price that the suppliers are prepared to offer, which may well be a poor one over the medium term from my point of view, given the competitive advantage they may gain from that knowledge.

The first key problem this raises with the scenario is the traditional economic problem of market failure due to imperfect information. Consumers are, in the jargon of the economists, ‘information impacted’ – that is, they know much less than the suppliers about the value of the privacy service they are offered. Therefore, the likelihood of an outcome in which consumer surplus and producer profit are balanced utilities and all gain from the trade, is substantially reduced.

In such a situation, will consumers be as content to take back responsibility and even liability for the privacy outcomes they face in ordinary commercial settings as the scenario requires to be sustainable? It seems unlikely.

Indeed, the findings of the survey that we conducted, on which details are presented in Volume 2 suggest strongly that people will not be prepared for this. About three quarters of the sample said that their principal reason for trust in organisations, in both the public and private sectors, was the existence of data protection law. While people may be concerned about the costs, difficulty and hassle factor of enforcement, they have much less faith in other aspects of the situation that might enhance their bargaining power, such as reputation, reliability of staff or commitment to a local or national identity.

Related to this are questions about pricing. First, it is not clear how consumers would tell in advance whether, in a given market, they could expect to be paid in discounts or other benefits for surrendering information: whether they would have to pay for the levels of privacy
that they want in such areas as nondisclosure or whether the effect of the two forces would cancel one another out, leaving the consumer without any real price change if they are willing to provide information but want confidentiality.

Secondly, it is not clear how far in Britain it would be considered acceptable to the majority of the public to have a scale of price differentiation for goods and services according to the level of privacy that consumers and suppliers agree upon.

Finally, the markets in the privacy scenario depends for their sustainability on the extent to which people are willing to draw a sharp distinction between dataveillance in government and in the commercial sector. While neo-liberals believe that they ought to draw this distinction, our findings (see Volume 2) suggest that they do not. Sector is not the most important predictor of either risk perception, acceptability of risk or reason or task for trust.

Therefore, the sustainability of the markets in privacy scenario turns on the extent to which consumers are really privacy fatalists, prepared to accept and tolerate whatever they are offered in the absence of regulation as the best privacy they are likely to get. Certainly, some people do reach for fatalistic attitudes, but this does not crowd out all other views. In a situation in which the markets in privacy scenario had begun to degenerate, it seems likely that some negative feedback effects would emerge that would throw it off course. Consumer movements around privacy, demanding the restoration of baseline regulation with liability on suppliers, would be a distinct possibility.

The markets in privacy scenario has potential for application in certain specialist niches, but it has too many problems to be generally sustainable. This suggests strongly that a new approach is required to both building scenarios for the future of privacy and to the nature of the questions that are intended to be addressed.
This chapter seeks to bring together in summarised form the key themes from Parts 1 and 2 of this book into a set of possible futures for privacy, using conventional futures techniques to explore their scope and limits.

Drivers of change
Identifying the drivers
The first stage in building scenarios is to assemble a classification of the key drivers of change. Part two enables us to identify the key ones. Using the Demos Serious Futures approach, we would expect to find significant forces in each of the following categories. Indeed, the significant forces identified in Part 2 can indeed be grouped in this way. Figure 10 overleaf presents the forces according to a crude and general distinction of likely impact on the scope for privacy in order to set the context for the more interesting question about what privacy might come to mean or be worth.

Ranking the drivers
The next stage in any scenario building exercise is to rank and group these drivers of change. A useful tool for this purpose is known in the scenario building trade as a ‘certainty/importance’ grid. The horizontal dimension groups variables according to the importance they are
<table>
<thead>
<tr>
<th>Category of driver of change:</th>
<th>Value tendency</th>
<th>Potentially more often friendly to enforceability of privacy than not</th>
<th>Potentially at least as often hostile to enforceability of privacy as friendly, at least as currently organised</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demography</td>
<td>rising education; rising awareness of IT and associated risks</td>
<td>mobility</td>
<td></td>
</tr>
<tr>
<td>Technology</td>
<td>privacy-enhancing technologies; cryptography; biometrics; ‘blind’ digital signatures; secure payment environments</td>
<td>CCTV; smart transport; covert data capture; I-war; geodemographic profiling; neural nets for profiling in push systems</td>
<td></td>
</tr>
<tr>
<td>Innovative paradigms and capacity</td>
<td>‘environments of trust’</td>
<td>‘market of one’</td>
<td></td>
</tr>
<tr>
<td>Finance and productive capacity</td>
<td>falling costs of cryptography, etc</td>
<td>loyalty partnerships; information barter in capital financing</td>
<td></td>
</tr>
<tr>
<td>Organisational capacity</td>
<td>development of capacity in data protection regulation; convergence in developed world on regulatory style; business concern about public trust; probable ineffectiveness of encryption regulation; trust kitemarking</td>
<td>business desire to influence consumer attitudes and behaviour; trends towards holistic government; autonomy of law enforcement agencies</td>
<td></td>
</tr>
<tr>
<td>Culture, values and ethics</td>
<td>post-materialism; triumph of liberalism; widespread privacy pragmatism; rising risk perception about personal information rights and distribution of other risks in society</td>
<td>rising concern about crime leading to support for surveillance and dataveillance; privacy fatalism; prunence about the private lives of the rich and famous; the informed home space; desire for personalised services</td>
<td></td>
</tr>
<tr>
<td>Politics</td>
<td>continuing European cultural commitment to privacy; cyclical upswings in privacy social movements</td>
<td>mandatory key escrow; growth in transnational data flows; weakness of civil liberties lobby and weak coordination with business interests (fracture between political and economic liberalism)</td>
<td></td>
</tr>
</tbody>
</table>
likely to have for the future of privacy, while the vertical dimension groups them according to the degree of confidence that we can have in our understanding of the value the variable is likely to take. This yields a four quadrant matrix (Figure 11 on page 254).

The allocation of variables in Figure 11 is based on the expert interviews, qualitative research, literature reviews, reflection and discussion and the argument of Parts 1 and 2 that comprised the research for this book.

**Background scenario**

We attend first to the variable in the two ‘relatively certain’ quadrants. By definition, because they are relatively certain, these variables define what can be expected not to vary across the main scenarios and therefore form a partial description of the likely future context for privacy.

As with most futures studies, the more certain things are matters of demographics, general economic development and foreseeable technological development, few are concerned with cultural formations, except at the most general level. Therefore, we can pick out rising education and mobility, the continued development of the technologies of surveillance and dataveillance, the continued arms race in cryptography between the security designers and the hackers, and we can expect the continued transnationalisation of the flows of personal data wherever possible.

In this case, there are also certain general features of the formation of informational capitalism that seem set fair to continue for the foreseeable future. The basic paradigm of the information organised business, where personal information is the fuel for operations and transactional flows in the firm, is one of its most important assets because the basis of marketing will continue to be ever tighter targeting and segmenting on smaller groups.

At the most general cultural level, it seems reasonable to expect that large majorities will remain pragmatic about privacy, willing in principle to trade personal information for other benefits, even if they are not always clear about the price at which they will trade in a given context.
The future of privacy

Figure 11 Certainty and importance of key drivers of change

This page is covered by the Demos open access licence. Some rights reserved. Full details of licence conditions are available at www.demos.co.uk/openaccess
Key quadrant scenarios
Naturally, these things in the background quadrant do not take us very far. Therefore, we now turn to the key quadrant, of the factors that are very important but rather uncertain.

At the heart of the argument in Part 2 was the central importance of cultures and cultural viability, based on the fact that economics, technology, and organisational issues leave much about the future direction of privacy undetermined. Therefore, the construction of future scenarios will proceed in two stages. First, the factors other than the balance of cultures will be subjected to cross-cluster and cross-impact analysis and then the results will be put through a cultural theoretic scenario analysis.

Cross-clustering factors
In this preliminary stage of analysis, we identify those variables that, if they take a particular value, are likely to be found in conjunction with a particular value for another variable. Figure 12 back presents the results of the cross-clustering of these noncultural key quadrant variables.

From these key uncertain but important factors and their cross-clusters, some important considerations emerge.

The first is that the connections between the variables are not particularly tight, by the standards of scenario building exercises. Many of the drivers of change operate independently of each other.16

Secondly, the connections between privacy dynamics in the private sector and executive and regulatory parts of the public sector are relatively weak, being confined to areas such as:

- cross-sectoral organisational arrangements such as public procurement and the possibilities for information barter
- culturally influenced effects such as the possibility that if there is high public acceptance of surveillance based policing, then the business dataveillance involved in market place of one strategies will be more likely also to be acceptable, and correlative, the following two hypotheses
**Figure 12** Cross-impacts between key drivers of change

<table>
<thead>
<tr>
<th>Prurience</th>
<th>Public accept surveillance policing</th>
<th>Autonomy of law enforcers</th>
<th>Holistic government</th>
<th>Information barter financing</th>
<th>Trust or costs based competition</th>
<th>Business accept DP regulation</th>
<th>DP regulatory capacity</th>
<th>Strategic alliances</th>
<th>Market of one</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prurience</td>
<td>/</td>
<td>high prurience, more likely public acceptance, more likely high autonomy</td>
<td>high holism, likely high info barter</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>Public accept surveillance policing</td>
<td>/</td>
<td>high public acceptance, more likely low enforcement autonomy</td>
<td>high holism, likely high info barter</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>Autonomy of law enforcers</td>
<td>/</td>
<td>high public acceptance, more likely low enforcement autonomy</td>
<td>high holism, likely high info barter</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>Holistic government</td>
<td>/</td>
<td>high holism, likely high info barter</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>Information barter financing</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>Trust or costs based competition</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>Business accept DP regulation</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>DP regulatory capacity</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>Strategic alliances</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>Market of one</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
</tbody>
</table>
the more holistic, alliance based and personalised are business services to the individual (if this is publicly acceptable), the more those people who accept it in business will expect this in government

the more the public accepts cost based competition, holistic government, media prurience, the harder it is likely to be to justify augmentation of the regulatory capacity of data protection authorities

The relative independence that this analysis suggests will continue to 2010 between press privacy issues and prurience on the one hand, and business database marketing issues on the other, and is an important hypothesis to consider carefully.

Thirdly, the determinants of the outcome between trust and cost based competition are shown to be highly complex. It proves very difficult to develop any single hypothesis about the links between business strategic alliances and the market of one strategy in database marketing and the basis of competition, but certainly, the cultural relationships between prurience and acceptance of policing by surveillance and holistic government, and the place of trust based competition in the business sector are complex and important, if not wholly understood.

Fourthly, as expected, this analysis takes us no further in understanding the changing meaning of privacy, than enabling us to develop relatively independent scenarios in each sector for 2010 for the:

- preservation and protection of privacy (low prurience, low autonomy of law enforcement agencies, low or information ethically managed holistic government, limited or tightly information ethically managed purchasing by information barter, trust based competition, business acceptance of data protection regulation, moderate to high regulatory capacity, limited or information ethically managed strategic alliance based competition, and tight controls on the market place of one)
erosion of privacy (high prurience, high autonomy of law enforcement agencies, deepening but information ethically loosely managed holistic government, extensive or loosely information ethically managed purchasing by information barter, cost based competition, business resistance to data protection regulation, limited data protection regulatory capacity, commonplace and information ethically loosely managed strategic alliance based competition, and loose controls on the marketplace of one).

On the other hand, the cross-cluster analysis does at least identify some of the key choices and decisions facing politicians, business leaders, information professions, public sector professions and privacy regulators.

Fifthly, following from the argument of Part 2, there is an important point to make about the likely directions of the lines of causation. It becomes clear from a consideration of these highly important and highly uncertain factors and their cross-clustering, that they do not singly or collectively determine the cultural meaning of privacy. The balance between the four traditions of private life and privacy is unlikely to be set simply by the dynamics of competition, the design of executive government, or business attitudes to regulation. Rather, although these forces influence each other and there are important positive and negative feedback loops establishing and changing cultures, cultures are likely to be the more powerful long run causal forces in the system. Finally, the analysis so far has helped us to identify one potentially important wildcard, namely, that

the public starts making connections: Linkages between issues of prurience and press privacy, business database marketing and entitlement decisions to key passport services (that determine entitlement to other services) such as insurance, crime detection and prevention issues, and issues around personal information handling in executive government, might prove stronger than the assumptions underlying
figures ten, eleven and twelve suggest. In general, the more explicit making of these connections in the public mind is likely to raise concern about privacy, rather than to lower it, even if crime prevention surveillance and anti-fraud data matching are largely acceptable to the public when considered in their separate spheres.

This is as far as conventional scenario building techniques can take us in this field. While they can offer us ways to understand futures in terms of more and less privacy, they tell us too little about why these trends might develop or what they might mean to people. In the next chapter, we enrich the approach by using cultural theory and cultural dynamics to construct more useful scenarios.
Privacy and the scenario question

In conducting scenario building exercises, it matters very much for the interest and usefulness of the scenarios developed, just what question is asked. Most of the futures work, including that in the previous chapter, that has been done in the area of privacy, which has been concerned with the question that seems to have preoccupied most commentators has been about the scope left for privacy, or something like this:

In the future at some specified date, will be there be no privacy at all making society intolerable, too much privacy for society to be orderly and tolerable, or just as much privacy as we are prepared individually to afford?

One problem with this kind of question is that it assumes that privacy is the sort of thing that comes in relatively determinable quantities, of which there can be none; more or less; enough, too much or too little – as though privacy were a continuously differentiable variable for which individuals have a relatively fixed appetite. It is clear from the considerations in Part 1 that, in fact, privacy does not have to be conceived in this way at all. It may be more appropriate to ask questions about how different groups in society might come to conceive of
different kinds of privacy problem and solution, than to ask about whether there may be more or less of it.

The other problem with this kind of question is that it assumes that privacy will achieve some state of rest, at which forces of positive and negative feedback are in equilibrium. The analysis offered in Part 1 of this volume suggests very strongly otherwise. Cultures are not the sorts of thing that reach equilibrium, and the concept of cultural viability is precisely designed to capture the idea that sustainability must be a matter of picking a careful course, tacking against several cultural cross-winds, rather than seeking and achieving an equilibrium.

The way in which, I argue, it makes most sense to read the findings of Part 2 of this volume is to accept that privacy will be an area of continuing conflict. The solution to which will neither be a convincing victory either of the forces of dataveillance nor of the forces of privacy and data protection. Part 2 has been at pains to argue in each chapter that the future is indeed open and conflict ridden. There are technological and economic forces for greater dataveillance, but there are technological and economic forces for trust and privacy as well. We can take it that for the foreseeable future both will continue to matter. There are choices to be made according to the balance of cultural as well as economic, technological, governmental and other forces. Rather, the character of the struggle and conflict will change in ways that are more or less culturally viable, given different configurations of cultures within the population of citizens and consumers, in business, governmental and technology design circles, and so on. A better scenario question, then, is perhaps to ask something like the following:

What alternative configurations might the changing balance of privacy cultures in Britain and the rest of the developed world yield over the next ten to fifteen years, given that both privacy-friendly and privacy-hostile developments in technology would shape the meaning and intensity of privacy conflicts?
Cultural dynamics

Since it is of limited interest simply to develop scenarios of more and less privacy, in order to make progress on understanding the changing meaning of privacy – which may in turn influence the likelihood of each of the ‘quantity of privacy’ scenarios – it is necessary therefore to turn to the cultural variables, which, this study has consistently argued, are the crucial forces for change.

In Part 1, a classification of the key cultural traditions concerned with privacy and private life was presented, which identified four principal formations: fatalism, liberalism, civic republicanism and egalitarianism. It was also noted that liberalism has largely, but not completely, triumphed and that it has fractured into a political and an economic impulse or bias, with the impulse of political liberalism moving closer to the civic republican conception of a protected sphere of private life and also toward the egalitarian idea of enforceable rights for those informationally disadvantaged by government and business.

The fundamental conception of private life underlying each of these traditions was summarised as follows:

- **civic republicanism**: a sphere protected only for the preparation of civic virtue; loyalty in friendship
- **liberalism**: a set of asset-like economic rights to be traded for services; or, a set of discrete legitimate political rights; loyalty in contract
- **egalitarianism**: a suspect sphere designed to protect unacceptable behaviour; loyalty in community
- **fatalism**: a residue of discrete experiences not (yet) held socially accountable, loyalty not expected.

While individuals may reach for attitudes from across this repertoire, it is not unreasonable to think that most of us have some more basic views that, over the long term, colour our thinking, and that these will tend to centre on one or two of these cultural formations.

The starting point described in the first two parts of this volume, then, is one in which a dominant liberalism has become fractured;
there is some evidence of a growing commitment to some civic republican values especially in the fields of crime control. Many egalitarian social movements generally (including those that ally with political liberal privacy concerns) are currently in a trough in the cycle of their rise and fall; fatalism is to be found, but diffuse and not consistently held by many. There are institutional, economic and technological forces that make an alliance between civic republican commitment to public sector surveillance and economic liberal commitments to business dataveillance. However, there are contrary forces in technology, popular concerns and values that might make for a political liberal tendency around privacy, if such a tendency can find appropriate and powerful patrons, allies and connections. While certainly, any viable individual life involves the surrender of some control over personal information, there remains a variety of cultural issues and conflicts over the use, management, and disclosure that are not settled by existing institutional, technological or economic factors.

Using this conceptual toolkit, I now present a richer and more complex approach to the task of scenario building in general and apply it to the problems of privacy and private life in particular. All scenario building methods make some substantive assumptions about the causal nature of social change and stasis. The problem is that few of the conventional approaches make these theoretical foundations explicit. This section is therefore devoted to making explicit some of the basic social science assumptions about cultural dynamics – or theoretical account of how cultural change, both intended and unintended, works – on which the present scenario building exercise for the future meaning of privacy will turn.

While the relative dominance of the liberal conception of private life has been the assumed persistence of widespread privacy pragmatism, it is now time to drop this assumption. For empirical findings in cultural theory suggest strongly that one of the greatest weaknesses in any scenario building exercise is to ignore the egalitarian and the fatalist impulses, especially when they seem relatively weak. It was this mistake, in ignoring egalitarian biases, that cost the oil company, Shell, so dear when its famed scenario building programmes failed to alert its
executives to the possibility of a Brent Spar or an Ogoniland protest that would strike at the credibility of its global business strategy.

Some principles for the use of cultural theoretic analysis in scenario building can now be introduced or rehearsed from their brief mention in Part 1.

Cultural viability in general

1. Any modern society that is minimally socially viable at all will contain some mix of all these cultural formations and biases.
2. These cultural biases reflect ways of life into and out of which individuals move, not necessarily stable sociodemographic or even necessarily distinct attitudinal groups across the entire range of values and attitudes.
3. As ways of life, they sustain and are sustained by institutions, economic practices and social network configurations.
4. The cultures exist only in relations to one another, in mutual conflict but also in mutual dependence. Because of his (and theorem one), it is inappropriate to develop scenarios in which only one cultural bias or way of life is represented: even if one achieves dominance in a scenario, it must negotiate with and learn from its encounter with others.

Dynamics of stasis and change

5. Change within cultures comes about through:
   ○ positive feedback mechanisms from selection of social contacts in networks, institutional commitments and reinforcing persuasion
   ○ cyclical effects: in particular, treaties and settlements between biases suffer cycles, and the biases themselves do: the cultural biases on the negative diagonal and in particular, that of egalitarianism are the most subject to cyclical trends, because of the costs of collective action in dissident, enclave groups and the tendencies to fission.
6. Change between cultures takes place with difficulty because it involves challenging fundamental assumptions and only through a limited number of mechanisms, principally:
   - individual or group surprise, in which fundamental cultural assumptions are challenged in ways that no amount of positive feedback and cognitive dissonance reduction or avoidance can override, causing learning, but not necessarily leading from any given cultural starting point in predictable or linear ways to any stable resting point in some particular other bias (cases of all twelve conceivable bilateral shifts have been observed)
   - reaction, or the revolt of ways of life that have been suppressed or have lost ground or decayed, while others have become dominant, causing some individuals to (re)attach themselves to the resurgent cultural bias
   - collective decay, self-destruction, fracture or erosion through excessive isolation and ‘purity’ arising from lack of conflictual and adaptive contact with other cultural biases
   - formation of treaties, settlements, coalitions, or hybrids: these are usually temporary arrangements, which are peculiarly subject to decay and surprise, but can serve to solve the problems that particular individuals, groups or societies face at particular points in their cultural history

Viability

7. The concept of cultural viability is a useful test for any formation that relates each of the biases or ways of life. It is a not test of indefinite sustainability: nothing in cultural dynamics would meet such a test. Disequilibrium and complex nonlinearity is the norm in culture as in much of biology. Rather, it is essentially a short term test, related to the concept in conventional soft systems methodology of robustness, or the test that seeks the strategy that makes the
most short term sense, given the problem faced by a defined group or a society as a whole, for the foreseeable period ahead.²⁶

8. The robustness test of cultural viability does not take cultural formations to be fixed, background constraints. Rather, strategies increase their cultural viability by seeking deliberately to influence the rate, direction and balance of cultures in cultural change. Strategy can change culture as much as culture can change strategy. Tools for influencing cultural change include the amplification and attenuation of surprise, persuasion, example and experiment, and the development and use of deliberative institutions.

9. There are several strategic options by which a cultural formation or change might be culturally viable, in this sense:

- **lowest common denominator strategies**: these strategies stress those features or initiatives to which no culture has strenuous objections;²⁷ clearly, people with different biases can agree on means when they do not agree on reasons or ends, as political science has long known,²⁸ but such arrangements can be vulnerable to surprise and decay

- **partial and time limited separation** of cultural biases into different realms, where conflict has ceased to be viable because cultural conflict has become gridlocked;²⁹ protracted for any period, such arrangements tend to be vulnerable to decay

- **‘strong compromises’** between cultural biases, but which rely on identifying common short term conceptions or interests sufficiently close to the core of the cultural biases that they can collaborate or form a hybrid or treaty for a period³⁰

- **deliberative institutions** or initiatives – usually costly and precariously financed – that concede something to each bias or way of life, by way of procedures that cultivate and sustain consent through negotiation and renegotiation, avoid surprise where possible and create institutionalised
forms of learning through all the cultural forms (see Chapter 21).³¹

Settlements

10. Treaties, settlements or coalitions, between civic republicanism and liberalism are far more likely to prove sustainable for the period of the particular problems they are designed to address, than are treaties along the negative diagonal, between egalitarianism and fatalism. Egalitarian and fatalist ways of life are essentially reactive, in the former case as dissidence and in the latter as sceptical and stoic acceptance. Fatalism is a poor coalition partner for any cultural form, because it lacks creative capacity or sustained institution building commitment.³²

11. On the other hand, however, strategies that ignore egalitarianism and fatalism will lack cultural viability, because they will be vulnerable to surprise, reaction and decay.

12. Treaties and hybrids along the horizontal or vertical axes are much less likely to be culturally viable for significantly long periods (for example, a generation) than diagonal settlements. Thus, for instance, liberal-egalitarian treaties may serve to overcome particular problems that these ways of life face at certain times, but are liable to break up thereafter.³³

13. In periods of high political romanticism, cultural biases and their associated ways of life move apart, and harden their positions, making treaties and settlements more difficult to achieve. Romanticism is a cultural style in which values are perceived in polarities of utopian and dystopian forms. An assurance against risk is sought by drawing mainly on the historic and organic resources of one's own culture and tradition, when integration at the levels of the personal and the movement through cultural consistency is highly valued at the expense of wider social impact, and when messianic cultural forms tend to emerge.³⁴ In this context, it is treated as
in opposition to the cultural style of pragmatism, which, when dominant, makes treaties and settlements much easier to achieve. Romanticism and pragmatism are subject to cyclical trends, \(^{35}\) not least because of the elective affinity between romanticism and the more sectarian forms of egalitarian culture, although there are romantic styles in all modern cultures.

**Social capital**

14. Within each culture or way of life are certain conceptions of when, under what conditions, to whom and whether solidarity between people is appropriate. Solidarity is a social form, of which the different conceptions of loyalty embedded in the four principal cultural forms provide the microsocial foundations. For liberals, solidarity is appropriate in the enforcement of property rights, basic law and order, and philanthropy. For egalitarians, warm solidarity is to be offered between equals often within a particular enclave or movement or sect. For civic republicans, the central institutions of the community are there to manage the flows of solidarity to prevent excessive concentrations in factions, and to ensure that sufficient solidarity is created between groups for the social order to be perpetuated. The social basis of this solidarity defined by cultural formation we may call *infra-cultural social capital*. This is the commonest variety of social capital.

15. In encounters between cultures where some settlement or treaty can be brokered, there can grow up intercultural social capital, whereby, at least for the period of the settlement, a measure of trust develops on the basis of institutional commitments, reputation, and experience between individuals with different cultures (see Volume 2 for the general account of trust that underpins this conception).
16. Only in less common circumstances in which large scale settlements are possible, does *macrosocial capital* emerge, in which the whole society exhibits certain characteristics of high trust.

17. The most effective instruments yet discovered for the development of intercultural social capital are deliberative institutions (see Chapter 21 for more details).

**Applying cultural dynamics to the future of privacy**

The first principle rules out as uninteresting, any scenario that posits the prolonged and sole dominance of, for example, liberal or civic republican conceptions. Rather, we need scenarios that will combine ways of life in more fruitful ways, such as the potentially cultural viable strategies that are set out in the eighth principle of cultural dynamics.

The following seem to be scenarios potentially worth exploring. All work on the assumption that we shall probably not enter another age of high political romanticism before 2010, although there will perhaps be some resurgence at least within egalitarian circles.

**Minimal consensus between cultures of privacy**

A *lowest common denominator* (LCD) scenario might begin (like the markets in privacy scenario) with the acceptance by most cultural biases concerned with privacy that if there are ways to enhance the capacity of individuals to contract with businesses and government agencies for the level of privacy protection they would like, and which those agencies are prepared to offer, this could be done without prejudice to the level of personal liability and without any effective opting-out from any statutory protection.

Secondly, a lowest common denominator future might be one in which consumers grew more aware of the privacy risks they face, and organisations in the public and private sectors became more willing to provide information publicly and to their clientele about their personal information management practices. Codes of practice proliferate; consumers’ guide magazines offer comparisons between them for the
price tags attached and develop measures of privacy value for money, which some more consumer minded privacy pragmatists find valuable.

Therefore, business and to a lesser extent executive government start to offer more clearly defined service enhancements in exchange for the provision of personal information, at least above a certain threshold of sensitivity. The result is a mix of trust and cost based competition, in different segments of different markets.

In this scenario, most of contemporary data protection law remains on the statute books of the developed world but political liberals, moderate civic republicans and perhaps some egalitarians in alliance with political liberals would have the power of veto, but enforcement and regulatory capacity does not greatly improve (economic liberals have the power of veto over that). Likewise, legal restrictions on cryptography remain formally in place (civic republicans insist on this), but prove steadily less enforceable in practice (economic liberals and egalitarians ensure this proves possible). Civic republican conceptions predominate in the more coercive areas of executive government activity, especially in policing, and the detection of benefit and tax fraud, sustaining some autonomy for law enforcement agencies.

The LCD scenario quickly begins to resemble some parts of the status quo in the late 1990s. In effect, it is a linear projection scenario, with the addition of some additional exchange in privacy but without that supplanting all else to become the markets in privacy scenario. The key question that it must face is the same one that faces all linear projections: How can it be shown that it is not vulnerable to shocks? How can it be shown that it is viable or sustainable?

The conditions under which the LCD would be sustainable are those in which:

- even at the height of the next peak in social movement activity, there is no alliance between egalitarians and political liberals around tougher regulation of privacy
- consumer and citizen awareness and the organisational responses enable the ‘market in privacy’ to find packages acceptable to consumers and organisations alike
the sectoral separation (strongly reminiscent of the partial separation strategy) of concerns, in which civic republicanism entrenches itself in coercive government while economic liberalism makes advances in the consumer business sector, is itself sustainable.

These are all assumptions that are vulnerable to surprises, from which the strategic responses of the key stakeholders – privacy regulators, business strategists, public sector data controllers – would hardly be able to respond effectively while relying on the lowest common denominator principle of doing nothing that will be utterly unacceptable to any of the main cultures.

Finally, however, it seems plausible to argue that this scenario is viable only in the presence of continuing and perhaps deepening privacy fatalism, which has subterranean effects on the ideas and behaviour of many who regard themselves explicitly as privacy pragmatists. Such a persistent fatalism would limit the capacity of any social movements, would lubricate the wheels of the exchange in privacy as well as helping to sustain the sectoral division of cultural bias. As Volume 2 shows, this may describe accurately a significant proportion of the adult population today. But it is far from clear that in a society of rising education and rising expectations of the quality of service from both sectors, this privacy fatalism can be taken for granted.

Next, there seem to be three possible scenarios which involved treaties, settlements of hybrids between two or at most three cultures.

**Liberal-republican alliance**

In the first of these, economic liberals in leading businesses and civic republicans in politics and executive government come to a classical inter-élite settlement.

The settlement is based on the presumption that privacy can be put on an increasingly contractual basis in the sphere of the market, while in the sphere of crime control, law enforcement agencies should have greater powers to override privacy. This is supported by the continuing widespread concern about privacy not being abused as a cover for
crime and the widespread pragmatism of consumers willing to trade data for service.

The major obstacle for such a compromise between these two cultures is the economic liberal demand for commercial access to strong cryptography, and the civic republican view that this endangers the security of the community and the state. A settlement is reached by way of series of exemptions from the legal restrictions, extremely cheap automatic registration with public authorities of use without actual key escrow, and a piece of legislation putting specific legal hurdles to be vaulted before law enforcement authorities can insist on access to private decryption keys.

In this scenario, data protection rules for the private sector are enforced in ways that largely focus on ensuring that individuals are aware of disclosure rules and have subject access in those areas where it is currently permitted. The principles that limit collections to those purposes which have already been defined prior to collection are enforced with much less vigour and eventually are relaxed. In the public sector, the Home Secretary is given powers to exempt wide categories of activities from subject access and even from the fair obtaining principle. First to be relaxed are the restrictions on third country transfers, which are particularly objectionable to economic liberals. Media freedom becomes sufficiently buttressed that the courts are reluctant, not merely to grant prior restraint injunctions or to interfere in cases where the industry self-regulatory bodies have acted, but to accept privacy claims at all, except at trivial levels of damages awarded.

While trust based competition persists in some market segments, it is handled largely by contractual mechanisms, but with gradually less strenuously enforced data protection. Business strategic alliances around personal information banks become the dominant competitive form just as holistic government increasingly shares information and routinely provides data from a wide variety of sources to law enforcers.

In this scenario, the economic liberal and civic republican cultures fully expect cyclical surges in reaction from political liberals and moderate egalitarians allying around privacy issues, now harking back to the ‘good old days’, when the 1995 European Directive represented the
high point of their achievement. Such movements coalesce first around government initiatives, such as consolidated smart cards that serve as passports, driving licences, benefit cards, and have space for many other public sector services, and to a lesser extent around the sale of government data to the private sector.

The economic liberal and civic republican alliance strategy for defeating such reactions has two strands. The first and simplest is to withdraw particular proposals until such time as the political liberal and moderate egalitarian movements exhaust themselves, and then to reintroduce them under other labels, or, better, to achieve the same effect using other technology. The second is to offer concessions on some key elements that are sufficient to buy off many supporters, if not the most hardline activists. For example, alleged violations of industry and public sector codes of practice are permitted to be matters for the Data Protection Commissioner to handle through a fast track procedure. This gives the force of government backing to codes that have already been, in most cases, informally discussed with the commissioner’s staff, and so is not a major concession. A second, more significant concession, is that consumers are granted the right to opt for multi-functional cards that they own, and over which they can themselves decide the co-residence of applications: this appeals more to economic liberals than to civic republicans, but it serves the purpose of dealing with a short run crisis over privacy activist social movements.

As with all such alliances and hybrids, a measure of undisturbed background fatalism playing a largely passive role is necessary to sustain the dominant cultural formation.

The sustainability of the liberal republican alliance scenario can be questioned on a number of grounds. First, the history of liberal coalitions with civic republicanism is that they typically come to grief after a generation on some issue on which the two cultures diverge. Thus, in the middle of the nineteenth century, the Irish famine and the proposal to repeal the Corn Laws forced a split in the nascent Peelite Conservative movement that brought together industrial and old civic landed interests over a conflict between economic liberal concerns for free trade and the old rural community interest in protection and
social stability for the English countryside. Again, by 1990, the Thatcherite alliance between neo-liberals and family centred civic conservatives and the impulse of British nationalism came apart on the twin rocks of women’s participation in the labour force and the deepening trend in European integration.

While in the field of privacy, such a hybrid cultural formation might indeed be able to negotiate a settlement over such issues as cryptography, in the less immediate future other conflicts are conceivable that could be much more difficult to resolve. Civic republicans regard at least some categories of personal information that are not protected by the pedagogic sphere of privacy as community property, whereas economic liberals regard most categories of personal information as private property of the owner of the relevant databases. There is a wide range of potential conflicts between these conceptions that could show up in other kinds of demands by law enforcers for free access to commercial data which might then be shared around a more holistic executive government apparatus, and thus reach commercial contractors who might be direct competitors of the firms that are the source of the data.

Another element of instability in this scenario is the role of political liberalism. Never wholly detached from economic liberalism, but never wholly at home with it, it represents an impulse that has from time to time allied with civic republicanism to seek regulation of business activity (such as the origins of modern data protection legislation in human rights law), and with moderate egalitarianism in protests over particular proposals, from the Dutch census in the 1970s to the ‘Australia card’ in the 1980s. In a sociodemographic context of rising education and privacy risk awareness, the strategy for the defeat of periodic cyclical surges in privacy movement activism may be inadequate, particularly if those surges coincide with rifts in the central cultural coalition. Political liberalism has, moreover, a heavy institutional commitment behind it in the form of the inheritance of data protection law and regulation and the rising informal public expectations that have grown up around these formal systems.

Finally, intercultural coalitions need, for their viability, deliberative institutions to sustain negotiation and learning, particularly in their
encounters with other cultural formations. One of the problems, for example, of the coalition of cultures re-assembled under the banner of conservatism in the late 1980s and early 1990s, was that it conspicuously, and perhaps strangely, given the conservative Burkean tradition of fostering such institutional creativity, lacked such institutions, unless one regards Thatcherism as an aberration in the conservative cultural tradition. The preference was to rely on sleek institutions for the efficient streamlined flows of ideas and information into decision making, but the result was the Poll Tax. As coalitions harden and institutionalise over time, it requires more and more effort for them to innovate in the creation and sustaining of such deliberative institutions. While more open styles for regulatory bodies can serve as part of such institutional formations, they are nowhere enough, especially in cultural formations that rely heavily on inter-élite settlements, in fields such as privacy where regulatory capacity is not sufficiently large alone to support the learning role. This scenario is similarly weak in deliberative institutions, although they are necessary for its viability.

**Grand anti-fatalist coalition by separation of cultural spheres of influence**

Another common strategy for settlements between cultural biases, resorted to usually when other alternatives have exhausted themselves, is to assemble a kind of grand coalition of moderate civic republicans, moderate liberals and moderate egalitarians, for the period that the grand coalition lasts (or is intended to last) in order to overcome a particular problem or situation. Such coalitions are built on the basis that there is sufficient consensus between these three that fatalism is not an option, but also that there are enough passive fatalists and sufficiently few extreme ideologues left from their own cultures in the society to permit them to act together.

Grand coalitions in any field are fragile, not usually durable for whole generations (except perhaps in Switzerland!), have to be put together with great care, and, if they do not collapse into lowest common denominator veto arrangements, need highly sophisticated
deliberative institutions for negotiation and learning. The most common arrangement by which grand coalitions operate is partially, but not completely (the theory of cultural dynamics suggests that would prove impossible, at least for any length of time) to divide problems into cultural spheres of influence.

One reading of the coalition of cultural forces assembled by Blair’s New Labour on labour market issues from welfare reform through union policy to macro-economic labour market policy is that it represents just such a temporary grand anti-fatalist settlement. Egalitarians have some control over union recognition policy, economic liberals over microeconomic policy and civic republicans over public expenditure, and the complex system of reviews, interest group bargaining and consultation exercises are intended to be deliberative institutions for negotiation and learning.

Such a scenario might give egalitarians the field of media privacy issues, enabling them to insist that the private behaviour of public figures is a legitimate matter of public concern and accountability. It would allow economic liberals their head in some areas of data protection, at least by slackening enforcement, while using legislative reform to formally strengthen data protection to keep political liberals on board, and allow civic republicans their preference in cryptography policy and holistic government.

And indeed, this configuration does, at the time of writing, broadly resemble some aspects of the directions in which the Blair administration appears to want to take privacy policy.

That such a scenario of spheres is not consistent is not the important point: consistency is not the virtue that grand coalitions judge themselves by. Rather, they are temporary solutions to particular problems and cultural configurations in which the more extreme (consistent) options have exhausted themselves, at least temporarily, and in which there is agreement that fatalism is not culturally acceptable to large proportions of the population.

Such a scenario is viable for short periods, but can expect to cede eventually to combinations of surprise, decay and rival bicultural hybrids or coalitions, at the point where the grand coalition has
exhausted itself, and it cannot any longer sustain itself through deliberative institutions.

In the field of privacy, such a grand coalition is particularly vulnerable to a settlement between political and economic liberals in alliance with some moderate egalitarians over cryptography policy and Internet issues generally. That could extend into a number of areas of media privacy with concerns about the implications of holistic government and conventional data protection. This kind of low grid horizontal cultural treaty would itself be a temporary business, but it might well be sufficiently powerful to break a grand coalition.

**Political liberal reassertion**

Finally, there is a third scenario in which a treaty is cut between the three nonfatalist cultures but in which political liberalism has the greater bargaining power.

Public concern about privacy and in particular about unjust inference, although diffuse, remains at a high level. Concern about trends in more holistic government and strategic alliances in business focus this latent anxiety about privacy. In effect, this public concern provides the kind of corrective negative feedback that we might expect in either the liberal republican alliance or grand anti-fatalist coalition scenarios. Data protection laws are not relaxed in any comprehensive way in this scenario, and certain loopholes are strengthened. For example, exemptions on subject access are restricted.

However, political liberalism cannot hope to expand the scope of data protection to every field of privacy, when there remain powerful cultural forces of egalitarianism and civic republicanism to contend with. In the field of the media, for example, self-regulation is left to continue in a legal framework that remains largely separate from that which data protection governs, and journalistic practice is governed lightly by quite separate codes.

The settlement with civic republican concerns about crime yields a criminal justice law in which, rather than relying on very general exemptions, the powers of the police and other law enforcers such as
The tax collection agencies to override privacy are put on a much clearer statutory basis. They become subject to challenge in the courts if there is a ground for suspicion that they may have exceeded those powers. In government, a series of interlocking codes of practice are produced, subject to the Data Protection Commissioner’s approval, and trade associations are put under pressure to do likewise.

Cryptography policy gradually becomes market led, because prohibition becomes unenforceable and few people want to keep a dead letter law that might bring the wider law into disrepute. Businesses and individuals are permitted to purchase and use encryption software without having first to escrow private keys, but the security agencies are given additional resources with which to develop more sophisticated methods of description which they may use on acquiring a judicial warrant, to combat organised crime.

In this scenario, consistently with the greater bargaining power of liberalism, privacy becomes more associated with liberty and less with civic duty.

As with the previous scenarios, there are signs of this in the current policy mix of the Blair administration. Data protection is being overhauled in line with the Directive, and the combination of the data protection and human rights laws will firmly separate media privacy self-regulation from data protection. The recent statements from the public service ministers on trends toward more holistic government and freedom of information have shown a recognition of the sensitivity of privacy issues raised. The government appears to be thinking long and hard before committing itself on encryption policy.

This scenario too requires for its viability the development of deliberative institutions by which the bargaining power of political liberalism can be exercised and through which learning from, and negotiation with, other cultures can be conducted. One weakness of political liberalism has historically been its preference for adversarial and litigious institutions for the settlement of disputes about what it takes to be fundamental rights, and a distaste for some of the cultural compromises required in more deliberative strategies. If this scenario were to be viable, there would be needed many more informal ways in
which to negotiate interests than data protection enforcement and litigation or complaints to self-regulatory bodies currently permit.

Like liberal-republican alliance and grand anti-fatalist coalition, this scenario is not wholly stable. It is vulnerable to shocks arising from sudden crime waves or business dissatisfaction with the costs of data protection, and to the possible effects of less trust based and most cost based international competition in many consumer markets.

Appraising the cultural scenarios

The cultural dynamic approach to scenario building offers major advantages over the conventional approach both in general and in the specific case of thinking through risks and opportunities and dynamics in the fields of privacy and private life.

In general, it enables us to apply a clearer and tougher test of viability, and enables us to explore the ways in which the meanings of key cultural phenomena such as privacy and private life might change under different cultural configurations. It enables us to move beyond the quantity scenarios of privacy that the conventional methods offer, and it enriches the findings of the standard approaches by putting the key quadrant variables and their cross-impacts into a richer cultural context.

One key aim of scenario building is the identification of risk, and cultural dynamics enables the specific identification of risks associated with particular cultural strategies and formations.

In the specific context of privacy, it enables us to see just how crude and unhelpful is the concept of privacy pragmatism as a basis for understanding the acceptability of personal information ethics, opportunities and risks. The method also puts such value formations as prurience, acceptance of preventive surveillance and trust based competition into the specific and conflict ridden context in which they need to be seen.

As we shall see in Part 4, the approach has both strengths and limitations. The concept of cultural viability does not enable the policy analyst to pick out a unique set of policy recommendations that will
prove superior to all others for the period to 2010, let alone beyond. However, it is probably an unreasonable hubris on the part of scenario builders to claim that their techniques could ever offer such a shortcut to good policy making. What is useful is the specific way in which cultural dynamics undermine that aspiration and offer other tools for thinking about policies for conditional cultural viability. By enabling policies to be audited for their cultural context and conjuncture, by showing trade-offs and risks and opportunities, and by offering the idea of the deliberative institution as a key tool, cultural dynamics furnish policy analysis with genuinely valuable tools.

Cultural viability and cultural change
Each of the scenarios faces some problems in securing cultural viability. Shocks from cultures the demands of which have not been, in the view of their adherents, adequately represented in the scenario, are possible.

Therefore, viability of any strategy such as the combinations and settlements offered in these scenarios depends on the ability of the strategists for privacy to influence the direction of cultural change in ways that sustain the strategy. It is important to recognise that cultural dynamics are complex systems, in which particular cultural formations are both forces for change and themselves the subjects of change as they act upon one another in multiple feedback loops. Cultural forms are not fixed points that simply act as constraints upon what is culturally viable, but are themselves influenced – at least in respect of their relative importance and their temporary balance of emphasis and interest, if not in fundamental impulse – in the course of the implementation of strategies that aspire to cultural viability.

Chapter 21 explores in detail the mechanisms by which strategists can seek deliberately to influence cultural change. However, for the present, it is necessary only to stress that in a liberal-republican alliance, cultural change is needed to hold in check not only the forces of conflict between those two cultural forms but also the possibility of shocks from egalitarianism. In political liberal reassertion, it is necessary
for political liberals to influence the dialogue with other cultures and to institutionalise their values powerfully in order to secure their relative bargaining advantage. But in the grand anti-fatalist coalition scenario, major cultural change efforts are required to sustain the fragile conditions under which so extensive an alliance is possible.

**Using the scenarios to apply the viability test**

While none of the scenarios is easily made culturally viable when adopted formally as a strategy, in each case it has been possible to identify choices that can be made to enhance the chances of viability.

Can we say that any one is more likely than any of the others? Since the likelihood depends on cultural trends not yet developed and political choices not yet made, this is not a straightforward judgement. However, it does appear that on balance, the liberal-republican alliance scenario is vulnerable to pressure from the institutional weight of political liberalism, and that the grand anti-fatalist coalition is a fragile affair most likely only to be a short run expedient. These vulnerabilities do not of themselves make political liberal reassertion culturally viable, but they indicate that it has a particularly powerful claim to be taken into account when, in Part 4, we consider how to design strategies that can hope to make sense in as many likely scenarios as possible.

**Conclusion**

This part has developed the heart of the theoretical argument of the book. Conventional scenario building approaches have their limitations. In the case of private life, they tend to reduce the questions that can be asked to rather too simple ones of ‘how much privacy might there be?’, leaving us none the wiser about what private life and privacy might actually mean or be worth. Cultural dynamics offer a powerful way in which to think about futures, and both to develop and to appraise scenarios. The idea of cultural viability is a valuable tool with which to consider both the sustainability of scenarios that emerge without conscious intention from the interaction of many people’s work, and scenarios that reflect the strategic design of particular groups.
The three principal and substantive scenarios – liberal republican alliance, grand anti-fatalist coalition and political liberal reassertion – provide the backdrop for the argument in Part 4 about the kinds of specific legislative and policy strategies that are most likely to be culturally viable.
Notes for Part 3


2. The concept of a policy habitat was introduced by Hood C, 1994, Explaining economic policy reversals, Open University Press, Buckingham.


5. For example, Davies S, 1996, Big brother: Britain’s web of surveillance and the new technological order, Pan, London.


7. No author given, ‘Privacy is history – get over it!’ , Wired magazine, February 1996.

8. Although this is a scenario usually advanced by law enforcers, it has some roots in the cyber-punk tradition, May T, 1995, ‘Crypto-anarchy and virtual communities’, http://thumper.vmeng.com/pub/rah/anarchy.html. The triumphalist remark quoted here that
cryptography will inevitably deliver this scenario into social reality is ascribed to Tim May in Kelly K, 1994, *Out of control: the new biology of machines*, Fourth Estate, London, 265, 270.


10. Perhaps one of the best known advocates of this view is Frances Cairncross of *The Economist*, whose Radio Four *Analysis* programme, ‘Privatising privacy’, was broadcast on 9 and 12 October 1997.


13. On current US law, see Cate FH, 1997, *Privacy in the information age*, Brookings Institution, Washington DC. The Federal Trade Commission’s indication that it is in principle willing to use its powers to prosecute as unfair and deceptive trade practices some privacy violations suggests that some kind of privacy regulation may yet be brought to the US private sector.


18. Schwartz P, 1991, *The art of the long view: planning for the future in an uncertain world*, Currency/Doubleday, New York; van der Heijden K, 1996, *Scenarios: the art of strategic conversation*, Wiley, London are two well known standard texts in the field that provide only the most elementary guidance on ‘plot’ without making explicit the basis in general systems theory on which they work. It should be clear from the discussion of feedback effects by now that I regard cultural dynamics as part of
the wider discipline of general social systems theory.

19. This conception of ‘dynamics’ is concerned with interaction between cultural forms all of which persist during a given period, more than with a putative choice between them. In this sense, it differ radically from the conception of dynamics as the simple choice between dominant strategies offered by, for example, Snooks GD, 1996, The dynamic society: exploring the sources of global change, Routledge, London, ch. 8.


30. Davy B, 1997, Essential injustice: when legal institutions cannot resolve environmental and land use disputes, Springer Verlag, Vienna and New York, ch.10, argues that ‘weak compromises’ will fail, because they cannot this test.


32. On the importance of the diagonal relationships in cultural theory, see Douglas M, 1996, ‘The choice between the gross and the
spiritual: some medical preferences’ in Douglas M, *Thought styles*, Sage, London, 21–49. Such treaties on the positive diagonal between liberty and authority are relatively common, and indeed, have underpinned the reinvention afresh in every generation of the British Conservative Party’s direction. For example, as leader of the party from the late 1970s, Mrs Thatcher, as she then was, brought together a thorough-going economic liberalism with a commitment to authority and community centred values such as the traditional family at the microsocial level, and, at the macrosocial level, British national identity as against European or Scots, Welsh and Irish nationalisms: similar treaties with similarly specific emblems were struck in the age of Peel, Disraeli, Salisbury, MacMillan, Heath and Major, and no doubt, Hague and his successors will try to follow the same principle. See 6 P, 1997, ‘Tories need a vision to stay on earth,’ *Times Higher Education Supplement*, 10 October.


34. This use of the term ‘romanticism’ and the interpretation is grounded in the historical analysis of romanticism in literature, visual and plastic arts, and music offered by Schenk HG, 1979, *The mind of the European romantics*, Oxford University Press, Oxford.


36. The selection offered here is of course but a small number of the vast range of possible structures studied or developed for compromise based conflict resolution. The principle of selection is that these seem most likely to meet the test of cultural viability. It is perhaps worth mentioning just a few of the decision structures that have been proposed at various times for reaching settlement.

One decision structure that can quickly be dismissed is the Hobbesian Leviathan, by which one culture – typically a more hierarchical one – imposes a solution by force. I take it that this
will considered unattractive to most readers – other than extreme civic republicans – for fairly obvious reasons.

One of the best known is Rousseau's general will, which as analysed by Barry (Barry B, 1964, 'The public interest', Proceedings of the Aristotelian Society, supp. vol. 38, 1–18, reprinted in Quinton A, ed, 1967, Political philosophy, Oxford University Press, Oxford, 112–126), consists in a principle that everyone commits themselves to a decision rule that they will seek a solution that is, as far as possible, in the interests of all, given that each must continue after the decision to live in community with all others (that is, 'as a member of the public'), and then, starting with the policy most in each individual interest, cycles back through second-best solutions, third-best solutions and so on, until convergence is reached. The problem structure is a rough approximation to that of a multi-player prisoner's dilemma, in which a finite number of players know that they will play an indefinite number of rounds with one another, and therefore decide to adopt an initial policy cooperation, even if thereafter they resort to punishing the defection of others with their own defection ('tit for tat') (Axelrod R, 1983, The evolution of cooperation, Basic Books, New York; Taylor M, 1987, The possibility of cooperation, Cambridge University Press, Cambridge; Schotter A, 1981, The economic theory of social institutions, Cambridge University Press, Cambridge; Schotter A, 1986, ‘The evolution of rules’ in Langlois RN, ed, Economics as a process: essays in the new institutional economics, Cambridge University Press, Cambridge).

However, Rousseau's claim, translated into modern game-theoretic language, is that a single unique strong Nash equilibrium will emerge in such a context, an optimistic claim that is not supported by most contemporary game theorists studying n-person non-cooperative iterated prisoner's dilemma games.

Rather, the Rousseau case is – as Barry suggested in 1964 – a special case of limited application. In fact, the institutional arrangement that it most resembles for conflict resolution is neo-corporatism, where players make an initial commitment to cooperate, reserving the right to defect in punishment of others' defection later, but agree to consider their second-best policies if others will (Cawson A, 1986, Corporatism and political theory, Blackwell, Oxford). This is unlike the kinds of cultural conflict with which we are concerned here (Davy B, 1997, Essential injustice: when legal institutions cannot resolve environmental and land use disputes, Springer Verlag, Vienna and New York, ch. 5) for several reasons: players with different cultural biases may not be accurately informed either about facts about the preferences of their counterparts or the meaning of their behaviour; there may no, or many weak equilibria; symbolic 'non-solutions' may be preferable to
solutions; the sustainability of the equilibria are highly sensitive to expectations (as predicted by the 'folk theorem': Kreps DM, 1990, 'Corporate culture and economic theory' in Alt JE and Shepsle K, eds, Perspective on positive political economy, Cambridge University Press, Cambridge, 90–143) which be held by cultural bias above levels that would make second-best settlement equilibria feasible; and so on.

Another well-known decision procedure for situations of policy conflict is Lindblom's ‘muddling through’ or ‘disjointed incrementalism’ by successive limited comparisons of goals and policies, simultaneous focus on means as well as ends, concentrating attention on short term ills and problems rather than long term goals, dropping the requirement for shared agreement on goals but only on means, limiting discussion to immediately available and thinkable options, use of successive small trials, fragmentation of policy making work into partisan groups, a process of partisan mutual adjustment, typically leading to a series of incremental rather than a single grand settlement (Lindblom CE, 1959, ‘The science of muddling through’, Public Administration Review, 19, 2, 78–88; Lindblom CE, 1979, ‘Still muddling, not yet through’, Public Administration Review, 39, 517–526, reprinted in Lindblom CE, 1988, Democracy and market system, Norwegian University Press, Oslo).

Certainly, Lindblom’s model is of some direct use in the present context – rather more than the ‘tit for tat’ strategy in iterated prisoner’s dilemma games. For it does at least describe a feasible and practical procedure, by which some of the scenarios offered here could come about. Unfortunately, it is almost wholly silent on the likely content of settlements arrived at by this kind of procedure: indeed, Lindblom was at pains to defend his model against criticisms that it did implicitly smuggle in policy content. Secondly, however, the Lindblom model assumes a prior agreement to cooperate in doing or not doing something. This is often lacking in situations of cultural conflict.

The fourth solution approach is Rawls’ idea of the overlapping consensus (Rawls J, 1993, Political liberalism, Columbia University Press, New York). The model is highly demanding. It requires first a commitment to ‘public reason,’ namely the acceptance of moral duty upon those with different comprehensive doctrines ‘to listen to others and [to exercise] fai...
system that is accepted as just by people of different comprehensive doctrines (142). Thirdly, in the overlapping consensus, ‘unreasonable’ comprehensive doctrines are ruled out a priori (144). Fourth, the agreed settlement is presented ‘independently’ of all comprehensive doctrines (144). Rawls is surely right in saying that no mere ‘modus vivendi’! Indeed, I can think of no situation of fundamental cultural conflict in the sense described by cultural theory that would meet these impossibly stringent conditions: if conflicts could conform to these very specific (liberal) standards, it is hard to see why they should need the elaborate system Rawls offers to solve them. If these notions can be made to work at all, they will boil down to a very particular kind of deal between liberal, egalitarian and civic republican cultures that might prove not to be culturally viable or even ‘stable’ (Rawls’ term) at all.

A slightly less demanding and elaborate but still ultimately Rawlsian strategy for handling, but which does not avow neutralism, is offered by Taylor C, 1992, ‘The politics of recognition’ in Gutman A, ed, Multiculturalism and ‘the politics of recognition’, Princeton University Press, Princeton, New Jersey. Essentially, this boils down to a specified limit in advance on available compromise from a position of liberal hegemony.

What each of these solution concepts assumes is precisely what cultural theory denies: namely that any one cultural way of life – in Rawls’ case, liberalism, in Hobbes’ extreme authority-based civic republicanisim – can be ‘neutral’ between cultures or can offer a solution structure for real-life cultural conflicts that is without bias (On the incoherence of liberal neutralism from a liberal perspective, see Galston WA, 1991, Liberal purposes; gods, virtues and diversity in the liberal state, Cambridge University Press, Cambridge; and also Macedo S, 1990, Liberal virtues: citizenship, virtue and community in liberal constitutionalism, Oxford University Press, Oxford, 67, 73–4, 260–263). Indeed, the general problem with these solution concepts is that they fail to address the basic insights of cultural theory that ‘players’ with different cultures may not:

- recognise others as players of the same game
- recognise a common game to be played
- recognise what other cultures do as moves in the game
- share any fundamental concept of justice, fairness or common sense at all; unless or until certain messy, multiply biased, deliberative institutional structures, social networks, patterns of social exchange and creation of meaning have been put in place.

If those things have been already achieved to put in place a decision structure, then the choice of decision procedure will typically the less difficult and fraught process.
37. For some of the old Burkean, high Tory arguments that Thatcherism was exactly such an aberration by hollowing out a variety of institutions that might have offered some of the clumsiness necessary to mediation between interests, see Mount F, 1992, *The British constitution now: recovery or decline?*, Mandarin, London, and Jenkins S, 1995, *Accountable to none: the Tory nationalisation of Britain*, Penguin, Harmondsworth.
Part 4
Privacy, policy conflicts and viable policy
This final part of the study considers arguments to justify specific recommendations for public policy and business strategy, in connection with several conflicts between privacy and other values.

It is helpful to begin by thinking about how in general, conflicting claims of right and duty are or can be dealt with and perhaps resolved.¹ When moral claims of right and duty conflict, there are also competing views about how they can be resolved.

There are philosophers who simply deny that rights can ‘really’ conflict in any sense that requires any decision procedure beyond the full, accurate and proper specification of the rights; who remove conflicts by denying that rights have independent value by reducing them to shorthand arguments about utility; who hold that in conflicts between rights, only the morality of the manner in which the decision is taken can be judged – the degree of moral anguish, seriousness, democracy, transparency, care and so on; who rely on blunt intuition beyond the realm of rational justification; or who hold that in a conflict, no choice is acceptable, therefore any choice is acceptable and there is no ‘right’ answer, only arbitrary decision.

However, those philosophers who do not take any of these views but do give rights independent moral value, have developed a number of procedures for settling competing claims between putative rights, each of which yields different answers in particular cases. Most appeal to criteria that are to some degree outside or ‘above’ the sphere of
rights, such as values or goals or a conception of a good society. The following are some of the principal procedures on offer:

1. ranking rights by the importance of the human interests they serve. For example, one might use a ranking such as one of the well-known hierarchy of needs\textsuperscript{2} or some listing of ‘basic needs’\textsuperscript{3} or Rawls’ conception of ‘primary goods’ and ‘basic liberties’ and ‘fundamental moral powers’\textsuperscript{4}

2. ranking by relative contribution to some specific account of human flourishing or self-actualisation\textsuperscript{5}

3. ranking by some calculation of utility of actions offered to which the claims are not reduced, but which is used to supplement these considerations and resolve the conflict\textsuperscript{6}

4. ranking by relative contribution in the particular case to the furtherance of some underlying purpose that both particular rights in any given conflict share\textsuperscript{7}

5. ranking by relative contribution to certain fundamental values of a decent society\textsuperscript{8}

6. ranking, not the competing rights, but the actions they prescribe, by their relative virtue, in terms of their reflection of such virtues of character as integrity, decency, loyalty and so on.\textsuperscript{9}

None of these procedures for handling conflicting claims of rights and duties offers a satisfactory method for settling conflicting claims.

Each of these kinds of conventional philosophical jurisprudence works, in effect, within a single cultural bias or way of life, and attempts to meet a test of (cultural) consistency. For example, an economic liberal approach to policy in this field, would be more concerned that policies met the test of minimising the constraint upon individuals and businesses to dispose in particular contracts of their admittedly limited capacities of control over personal information. A Rawlsian egalitarian strategy using the difference principle would look for policies that allowed inequalities in the level of surveillance and dataveillance between rich and poor, only where those inequalities
that benefited the poor (either overall or in respect of surveillance and dataveillance levels).

However, in this kind of study, the argument must begin with the test of cultural viability and the related robustness test, considering the cultural viability of the possible futures identified in Part 3, namely:

*standard scenarios*
- dataveillance society
- crypto-anarchy
- markets in privacy

*cultural scenarios*
- minimal consensus
- liberal republican alliance
- grand non-fatalist coalition
- political liberal reassertion.

While no scenario proved unquestionably culturally viable, the last two scenarios were considered to have a better chance of cultural viability, at least to the extent that institutions for negotiation and learning can be designed to sustain them, and provided that they are seen as short to medium term solutions.

The argument in this part is therefore devoted to the task of grounding recommendations on the pragmatic basis of what seems most likely to meet the test of being effective or at least rational and sensible in the widest range of interesting culturally viable futures scenarios (‘robustness’). In some measure, that test reflects what is likely to be publicly acceptable, given conceivable changes in values, cultures and attitudes offered by those scenarios.

From a conventional jurisprudential perspective, then, the strategy for policy development offered here will look ‘unprincipled’. In fact, it is multiprincipled, strategic, concerned (in the short run at any given point in time) with legitimacy and concerned (over the longer run) with the design of institutions to enhance viability. It is not that internal consistency of principle between specific settlements among
the biases of the different cultures on different privacy problems is regarded as satisfactory or desirable. Instead, it is regarded as a bonus if it can be achieved and, when it cannot in some cases, it may be an acceptable price to pay for cultural viability, at least for the period in question.

However, this strategy does bear some resemblance to some of those identified above as conventional strategies in philosophical jurisprudence. Cultural viability is certainly a consequentialist test. It is not, as utilitarianism claimed to be, a full-blown account of human flourishing or self-actualisation, but it shares with utilitarianism a concern for what benefits large proportions of people, at least to the extent that their chosen or acculturated ways of life are beneficial for them. However, it would be a larger claim than I need or want to make that a society that so organises itself in a given historical conjuncture so that its arrangements are culturally viable, is also one that is decent, just, conductive to long term interest in human flourishing, or particularly virtuous. Rather, the whole point of the cultural theory is that those who wish to argue on those grounds will and must do so through the lens of philosophical consistency with a particular culture. For them, cultural viability will be a bonus if achieved and an acceptable sacrifice in exchange for their preferred cultural commitments if it cannot.

Indeed, the test of cultural viability is a weaker one that that demanded in many ‘practical reason’ or rationality conceptions of public policy making. We have seen that in some scenarios that may prove culturally viable, it may be sensible to legislate policies but not enforce them. Perhaps this is because in a particular cultural configuration, it is of some symbolic importance to civic republicans to feel that the state can, in pursuit of criminals, gain access to the means of decryption, even if in practice, such a law will be a dead letter in a very few years. Conventional policy rationality tests will rule out such a tactic, and indeed, I personally find it rather repugnant, having an old-fashioned instinct about the importance of the credibility of the law. But precisely what is culturally viable will be repugnant to some cultures’ idea of what is ‘common sense’, but is in fact anything but common.
However, there is nothing relativist about this kind of argumentative strategy. The point is not that anything could count as human flourishing, virtue, justice or social decency. Clearly that would be absurd on empirical grounds. The point is that there is limited cultural variation in conceptions of these things, at least between viable societies, that the small number of cultural formations have real and objective weight – a classical pluralist argument – and that it is objectively prudent and morally sensible to find ways to take account at least of the three active cultures.

But not anything goes for cultural viability. Although the cultural viability test by definition eschews cultural consistency, it does have a preference – although even then not absolute – for legal consistency. If, for example, a proposed settlement between cultures on privacy led to a conflict of laws between, on the one hand, the jurisprudence under Articles 8 and 10 of the European Convention on Human Rights on privacy and media freedom and, on the other, data protection law, then it is highly likely that such an arrangement would not prove culturally or legally viable for any length of time, exactly because the cultural conflict would lead to some form of litigation and perhaps also legislation being brought forward to reconcile the two bodies of law.

In addition to legal consistency, the test also calls for both substantive measures to ensure acceptability to at least a reasonable proportion of currently influential cultures, recognising the cycles through which the currently less influential ones are passing, as well as procedural initiatives in the form of institutions for negotiation and learning.

In this way the test is far from empty, but it is much less demanding than many rival conflict resolution proposals. The empirical claim lying behind the test of cultural viability is that there is a manageably small number of basic ways of life underlying human social and cultural diversity, and that it matters greatly – independently of which way of life we may be committed to – that societies find ways in which people with different commitments can rub along tolerably well, even if they do not achieve justice, virtue, decency or full flourishing. Cultural viability is, the argument runs, a better, empirically richer,
institutionally less demanding, institutionally more creative test of how that can be achieved than is offered by its main rivals.\textsuperscript{12}

It is unfortunate that most policy analysis conducted by cultural theorists has generally been \textit{fatalist} in character. The conventional conclusion regarding divergent cultures is that there is little the policy maker can effectively achieve, that cultures can only be influenced at the margins, that there is no culture-independent stance from which to formulate policy goals, that cultural conflict is too complex, irreducible and resistant to policy influence, for policy action to be effective.\textsuperscript{13} This part is devoted to an extended argument that this fatalist conclusion simply does not follow from the understanding of cultural dynamics. Cultural viability is a richer notion than many cultural theorists of policy have allowed and one that yields more specific and usable policy directions than has been recognised. True, policy recommendations need to be qualified with more humility about their robustness against cultural shocks, the period for which they can be expected to be effective and the limits of the toolkit. Nevertheless, even with such responsible qualifications, I argue, cultural dynamics should be reason for optimism about what policy can achieve rather than a reason for fatalism.

The choice of the test of cultural viability for policy making has one immediate implication both for the design and presentation of policy. An important finding in Part 3 was that few arrangements can be expected to be \textit{indefinitely} culturally viable. Too often policy analysts and policy makers work on the assumption that they are working for the indefinite future, or even for the foreseeable future, when in fact many – perhaps a majority – of policies will not prove culturally viable even for the period that scenario building exercises can work with. It might avoid embarrassing retreats and improve the quality of policy design, especially in the area of fall-back positions, if the test of cultural viability were used in the development and the public presentation of policies as appropriate for the particular conjuncture for which they are intended to be viable and robust. While it is certainly possible to imagine people with more extreme and ideological cultural biases taking exception to the idea that even a policy they favour might not
be indefinitely appropriate, this causes no greater offence to extreme liberals, for example, than to extreme civic republicans or egalitarians: this greater modesty in policy presentation would be no greater violation of ‘neutrality’ (to the limited extent that this is important for cultural viability) than any other style.

Specifically, the strategy here will be to focus on finding policies that will be relatively robust as between political liberal reassertion, liberal republican alliance and grand non-fatalist coalition, against a background of widespread privacy pragmatism and the long triumph and more recent fracture of liberalism. The problem, as we saw in Part 3, with minimal consensus, is that it is so minimal in what it will let through without someone’s veto, that it quickly leads to gridlock.

It follows then, that in considering issues of media freedom, the extent of any attenuation of privacy rights for ‘public’ figures and data protection reform, some balance between the cultures needs to be struck between the positive diagonal between the two kinds of liberals’ concerns about liberty to trade access to personal information for services and to safeguard against injustice and the civic republican concerns about dignity and the decent use of the provisional unaccountability of private life and the at least moderate egalitarianism, with its concern that privacy does not cloak behaviour that is unacceptable to the disadvantaged, and also perhaps a concern shared with some political liberals about equality in the distribution of surveillance.

The application of this strategy can be now be considered in connection with each of the main conflicts into which claims of privacy are pitched. First, I review the implications of the argument in parts two and three to identify the major challenges and decisions that we face in the period before 2010. Then I consider conflicts between privacy and the claims or values of freedom of speech and freedom of the press; with the public accountability of public officials and people in public life; law enforcement and other goals of government; freedom of contract and economic liberty generally, and acceptable distributions of risk. In the closing chapters of this part, I apply the strategy to questions of policy process, privacy education and institution building.
for cultural viability, before concluding with reflections of the significance of the argument as a whole.

The structure of the argument in each chapter follows certain principles. Political liberal arguments for privacy protection are stated, as are egalitarian and civic republican arguments for public accountability in some form. Where some consistent and principled trade-off, compromise or settlement seems to suggest itself on straightforward consideration of the jurisprudential issues involved, if this seems culturally viable, it is adopted. However, there are situations where such consistent positions fail the test of cultural viability, and have to be overridden because the argument, although sound, simply cannot win in the foreseeable cultural context of Britain in the first decade of the new century.
The problem
Following the death in 1997 of Diana, Princess of Wales, in a car crash during an attempt to evade the attentions of freelance press photographers (some of whom were alleged to have taken photographs at the scene the accident), there has erupted afresh in Britain the longstanding debate about the balance between privacy and freedom of the press. Since then, there have been several cases where privacy issues have been debated. First, it was alleged that tabloid journalists had entrapped the son of the Home Secretary (the Rt Hon Jack Straw) into selling a small amount of cannabis. Second, revelations were made in the media against his wishes about the Foreign Secretary (the Rt Hon Robin Cook’s) affair, divorce and new marriage. Finally, two directors of Newcastle United Football Club were lured to Marbella by journalists purporting to be from the Dubai football authorities and seeking consultancy. The directors were taken to a brothel and plied with drink until they made a number of offensive remarks which were then reported to their embarrassment and eventually led to their resignations.

The debate about press violations of privacy is not new. Indeed, it first became a live one in jurisprudence in 1890, with the publication of an article in the Harvard Law Review by two prominent Boston lawyers and judges, who went on to become US Supreme Court justices and so has some claim to be one of the original privacy policy questions.
The activities of the media raise a number of kinds of privacy risks. Where the activities investigated, observed, photographed, noted down, interpreted and reported by the media are not allegedly criminal in nature, the main privacy risks that are in usually in conflict with the claim of media freedom are those of:

- physical intrusion
- excessive surveillance
- collection of information without consent
- disclosure without consent.

In cases where the press allege that an individual has committed a criminal act, there may also be risks of:

- unjust inference
- reversal of the presumption of innocence, even to the point of prejudicing a fair trial.

Finally, there is a special case of a conflict between competing claims both of which are about privacy, in the context of freedom of the media. Normal data protection laws place a duty on those collecting information to obtain and process it fairly and offer a right of subject access, whereby individuals can view data held about them, seek corrections of inaccuracies and the like. However, the media are to be exempted from these rules in the 1998 Act, on the grounds that these claims are overridden by considerations of freedom of the media, confidentiality of journalists’ sources and other sensitive data held by journalists, and of the public interest. The incorporation of the European Convention of Human Rights will require some settlement between Article 8 which guarantees privacy and Article which provides for media freedom: the government will amend the Human Rights bill to provide that privacy matters cannot come before the courts until they have first been before the self-regulatory bodies such as the Press Complaints Commission (PCC) and the Broadcasting Standards Commission (BSC). However, some cases will nevertheless reach...
the courts: the press should not assume that the self-regulatory system
will now be wholly without judicial oversight because of the amendment.

In general, this is a reasonable settlement. The challenge now is to
make the system work and deliver a fair balance between privacy and
those important values that should override it. In this and the follow-
ing chapter, I set out some principles which should guide both tiers of
judgement – the PCC and BSC in the first instance and the courts in
the final instance.

In order to do so, we must first explore the conflict between argu-
ments for freedom of the media and the claims of personal privacy.
The principal arguments offered for the claim that media freedom
should override claims of privacy are the following.

The argument from economic liberty
This argument seeks to defend the media from any regulation that
would protect individuals from any privacy risks presented by the
media. It begins from the fact that media organisations are commercial
enterprises. A decent society should respect the right of the individual
to form and join enterprise associations. The media trade in informa-
tion, like many other industries. Privacy restrictions upon the media
are therefore a restriction of economic liberty. In general, liberty is, in
liberal thought a greater and superior value and claim than dignity,
and should therefore trump privacy.

The argument from the evil of censorship
The argument is concerned principally with making the case for a right
of the press to engage in disclosure without consent. It begins with the
assertion that state censorship of the content of media reportage is
wrong on a variety of grounds, including fundamental human liberty;
a conception of self-government; the promotion of certain virtues such
as tolerance, learning and openness; or in a general argument about the
greater likelihood of truth emerging from the unfettered market place
of ideas. The argument proceeds with the claim that any privacy pro-
tection that seek to restrict the right of the media to disclose information
without the consent of individuals who are the subject of that information amounts to state censorship, indeed to prior restraint. Since freedom of speech, of which freedom of the media is but one example, is regarded in the liberal tradition as a greater and superior right than that of privacy, it should trump.

The argument from the public interest
This argument specifically addresses the question of disclosure without consent. It seeks to establish the proposition that the public has a legitimate interest in being able to be informed, and indeed a right to be informed, about a wide variety of matters supposedly within the sphere of private life. The claim is usually grounded on arguments about capacity for self-government in the case of privacy claims made by those with public responsibilities, and on a notion of an implicit voluntarily entered contract for unfettered publicity in the case of privacy claims made by or on behalf of celebrities.

Supporting instrumental arguments
Equipped with these three general arguments, advocates of media freedom over privacy usually argue that physical intrusion, collection of information without consent, surveillance that may turn out only after the event to have been excessive for the purpose, are necessary means by which investigation can be undertaken, in order to secure the material for the disclosure that the other arguments would give protection to, overriding privacy claims.

Assessing the arguments of media freedom for overriding privacy
Scope
As general arguments, none of these are wholly convincing. The argument from economic liberty, framed in general terms, proves too much. It would rule out much of the regulation of property rights necessary to make markets themselves work.
The argument of censorship may also prove too much. I leave aside genuine cases of content censorship laws such as obscenity and blasphemy, which can plausibly be held to fall foul of the principle of media freedom of speech, because they lack other defences.

If the argument from censorship is taken literally, then it would not only rule out obscenity and blasphemy laws being applied to the media. It would amount to holding to be censorship any of the following laws, some of which may impede the way in which a journalist may want to conduct an investigation:

**regulation of disclosures**
- of partisan balance on terrestrial broadcasting
- ‘quality thresholds’ in independent broadcasting franchises or licences
- regulation of advertising standards
- trades descriptions law
- rights of reply
- laws of defamation and libel

**regulation of collections**
- laws against impersonation
- laws of trespass
- laws of covert interception
- laws of theft
- laws on nuisance, stalking and harassment
- offences of incitement to commit crimes (entrapment)
- data protection laws ruling out excessive and irrelevant information, unfair obtaining, inaccuracy and so on

**regulation of holdings**
- data protection laws on subject access.

Indeed it is true there are newspaper editors who take the strong view that the application of any and all of these laws to journalists, editors and press photographers is indeed a form of censorship, and
unacceptable infringements of freedom of media speech on that ground alone. However, outside that charmed circle, this is generally regarded as an extreme position.

There is now a general consensus, contrary to Calcutt (see Chapter 11), there is no very powerful case for any further extension of the role of the criminal law in this areas, and in particular that breach of confidence should remain a civil matter. The standard of proof in criminal cases is inappropriately high for breach of confidence matters, and the wrongs committed, in a context where a public interest defence of some kind is used, are not of the kind to which the criminal law is well addressed. The basis of the main kinds of privacy action currently undertaken in the civil courts should therefore remain there, grounded in principles of equity and tort.

Special status or the same rights as the public at large?

In order to make out a case that these are unacceptable violations of freedom of speech, those who seek to use this argument need to decide first whether applying such laws to the behaviour private individuals seeking to exercise their freedom of speech outside the media, would be unacceptable. Most people would hold that individuals and organisations that engage in defamation and libel, harassment and nuisance, stalking, refusal (say, within an organisation) to grant a right of reply to allegation, deserve to face some form of legal proceeding, whether in tort or by way of the criminal law.

Therefore, the force of this argument turns on whether the media can claim any special protection for their freedom of speech, over and above that to which ordinary citizens are entitled. In general, English law has officially denied any such special status to the press, although some commentators would consider that in practice, many decisions on defamation, breach of confidence, trespass and other matters seem to reflect some special status. In the United States, by contrast, the First Amendment to the Constitution, which provides for freedom of speech and freedom of the press has been interpreted by the courts to permit collections and disclosures of personal information by the press that would otherwise be unlawful.
While many editors and media rights advocates do make exactly such a claim for special constitutional protection, this leaves some crucial questions unanswered or with only the vaguest of answers. At the very least, the questions about the rationale for special protection, the grounds for investigation, the scope of protection claimed, and conflicts between claims need to be answered specifically:

- **Rationale.** Just what are the exact grounds are on which the claim to special protection for the media can be made out – on grounds of special contribution to democracy, duty of scrutiny to ensure clean government and business, on the ground that the media represent a special arm of governance to be protected by the rule of the separation of powers, on general utilitarian grounds, or some special benefit that only the media provide to the wider culture?

- **Grounds for initiative.** Does the overriding of privacy in any of these ways in the course of investigative journalism requires a higher or lower standard of initial ‘reasonable suspicion’ of some kind of activity in which the public interest is said to call for disclosure, than is required for an investigation into suspected criminal activity by law enforcement authorities?

- **Type of activities protected.** Which of the range of activities that would violate laws if done by individuals in other walk of life, should such special constitutional status for the media protect?

- **Type of subjects.** Which individuals’ claims to privacy may be overridden by the special status – only public officials? People in business? Innocent victims of crimes? Even jurors?

- **Type of media.** Would any and all media be protected, or only news and current affairs factual reportage and comment?

- **Media privacy.** What is the relationship between media claims of privacy and secrecy for their own sources and materials and those made by others – not least in situations where one media organisation investigates another?17
There may be principled ways to settle some of these uncertainties, if
the exact grounds can be clearly specified for special constitutional
status for media freedom, over and above that secured for the public at
large by individual rights to freedom of speech.

There is, I believe, a case for giving a special status for the media, but
on very limited grounds and with very limited extent. There is, I argue,
one principal justification for this, which can be called the ‘special duty
of scrutiny’ which I believe to be a better concept than that of ‘the pub-
lic interest’ in the present context. This would only function as a
defence in certain kinds of criminal or civil litigation, but would not
justify immunity from prosecution or civil suit.

The special duty of scrutiny
The first plausible approach is to argue that the ground of the special
duty of scrutiny is the fundamental rationale for special treatment. No
body in any society has quite the same role as the news and current
affairs media in applying scrutiny to the activities of the powerful and
the influential in government, business and other major decision-
making institutions. While the police can enforce the criminal law,
there are a wide range of serious wrongs that are too often committed
by the powerful in any society. It is the duty as well as to the profit of
the media to expose, debate and inform the public of these wrongs.
Only the major media have the capacity to engage in the kind of
scrutiny required to discipline the powerful.

However, this cannot justify literally any kind of behaviour. For the
media are themselves among the most powerful institutions in any
modern society and as likely to abuse their power as any politician,
business leader or other power broker. Indeed, the growth in the social,
economic and political power of the media generally is one of the
most significant and fundamental changes in the configuration of
power globally that has taken place since the second world war.

The scope of the special duty of scrutiny must surely be confined to
reasonable suspicion of serious wrong doing. It is not obvious that
exposure of, for example, private consensual sexual behaviour without
additional special circumstances, is sufficiently serious wrong doing to merit the coverage of a special duty of scrutiny that would protect the media from prosecution or civil suit for collections and disclosures that would be unlawful if carried out by a private individual.

This principle would clearly not protect much more than mainstream news and current affairs journalism, where the principal purpose is to inform and comment on public life, rather than to entertain. It would clearly cover investigations into people who are public servants, people with influence in business and other areas of decision making in large organisations. It would not cover film stars, pop stars and other entertainment celebrities, who have fame but no real power or influence.

Nor would it, for example, protect prurience of the kind that was seen in the commercial sale of a video called *Caught in the act!* of ordinary people in and outside their own homes and in semi-public places taken from closed circuit television video tapes collected by private security firms. Nor would it protect the hounding of celebrities simply for photographs for entertainment and gossip pages.

The special duty of scrutiny might protect some types of media activity that would not be legal for the public at large, in respect to certain types of individuals only, but only if there were some appropriate standard of ‘reasonable suspicion’ before such activities were engaged in, and provided they could be shown to be necessary to the course of the investigation. The reason for this restriction is that a duty of scrutiny is a quasi-judicial responsibility, and can only be said to be exercised as such, if it is used respecting principles of due process.

This special duty might, subject to a necessity for purpose test on an investigation on reasonable suspicion of serious wrongdoing, exempt certain information from rights of subject access, at least prior to publication, and would perhaps justify confidentiality of journalist’s sources even after publication. On the other hand, the necessity test means that the special duty of scrutiny rationale would not protect the media from data protection rules against excessive and irrelevant data.

I turn now to the question, how far does a special duty of scrutiny rationale protect the media against the ‘no unfair obtaining’ rule in
data protection? Since even law enforcers are prohibited from bugging telephones or modems without authorisation and from taking physical documents or other goods without a warrant for seizure, or else they face prosecution for theft or illegal interception, there seems no case for permitting such privacy violations to the press.

The question of how far the special duty of scrutiny should extend to permit or regulate entrapment and impersonation (a variety of entrapment) is not straightforward. The Broadcasting Standards Council code rules out entrapment except in the most special cases: however, broadcasting is a media industry subject to statutory regulation in a way that the press are not. Within the BBC, which has the additional responsibility of being a ‘public service’ broadcaster, the producer’s guidelines generally forbid entrapment and require that researchers, producers and directors make clear the journalistic purpose for which information is being sought, especially at the point of filming. This does not prevent even the BBC from engaging in investigative journalists as programmes such as Radio Four’s *Face the facts* have shown. Nevertheless, these rules presumably do limit the capacity of the BBC to achieve many of the exposés that the press can.

We can compare journalistic entrapment with police entrapment. The courts have considered it acceptable for the police to use entrapment where no other means of securing a conviction will be effective. However, the duty of the police to detect and apprehend criminals and bring them to justice is of a different order of public responsibility from the media’s special duty of scrutiny. Moreover, the police exercise their duties subject to public accountability in each case through the courts and in general through Parliament and local and regional police authorities. By contrast, the media are private businesses, not publicly accountable except in the general way that all companies must file annual reports with Companies House and so on.

There are degrees of seriousness here. For example, impersonating just any customer of a drug supplier or a potentially crooked retailer in order to expose their crimes or wrong-doings is presumably a less serious matter than impersonating a particular individual who may have special authority or particular claim on the willingness of the subject
of the investigation to be forthcoming. Impersonating a suspect to call a telephone company to get a list of a suspect’s registered British Telecom ‘Friends and family’ numbers is a less serious matter than posing to a suspect as a drug dealer or corrupt businessperson offering a bribe.

In general, it seems reasonable to say that the special duty of scrutiny should permit entrapment and impersonation on the basis of several tests, which are not unlike those used by the courts in cases of police entrapment of criminals. The first should be the journalistic purpose. In the next chapter, I consider the range of journalistic purposes in relation to people in public life in more detail. For the present, we need only note that where that test would permit privacy to be overridden – for example, in the case of investigation of an alleged crime or wrong-doing of a kind that is quite unacceptable in someone holding a particular position – then impersonation or entrapment could be used, if it passed the other test. That other test should be one of necessity. There should be no other means of securing the information necessary for the investigation to achieve its goal of determining the truth or falsehood of the well-founded suspicion that triggered the investigation.

Third, the impersonation should be no greater or more specific than is necessary. If the information sought can be obtained by posing as just any customer, just any acquaintance, rather than as a person with specific authority or a particular living contact of the subject or the subject himself or herself, then only the lesser impersonation should be used.

Fourth, there must be a test of ‘clean hands’. In principle, if it is possible to design a trap in which the subject reveals past crimes rather than commits new ones, this should be used in preference to entrapment strategies which incite or induce the subject to commit fresh ones. Moreover, traps which induce individuals’ new crimes cannot be acceptable where they are crimes against the person, crimes of violence or physically violent crimes against property. If the journalistic purpose were sufficiently well-grounded, if there were no other means and using the least possible impersonation, it might be acceptable to
induce someone to commit a crime of selling drugs before journalistic or other witnesses or even to commit a small, traceable financial crime. On the other hand, it would not be acceptable to induce a suspected football hooligan to commit an assault, an arsonist to burn down a house, a computer hacker to bring the air traffic control system to a halt, a sex offender to commit a rape or a serial killer to commit a murder.

On this test, I believe, the special duty of scrutiny would not protect those journalists who lured the two hapless, if personally unpleasant, directors of the Newcastle United Football Club. For it is not clear that the journalistic purpose was sufficiently well-grounded (see the Chapter 18) and even if were, a less specific impersonation would have sufficed. The case of the son of the Home Secretary is more complex. This case might pass the journalistic purpose test, but it is not clear that it passes the necessity test: if a trap were necessary, it might have been possible to design one that would have led to a confession of past sales of cannabis rather than one that induced a further sale.

This leaves trespass, nuisance, harassment and stalking. Many people clearly consider that it is the duty of investigative journalists covertly to collect information on, for example, corrupt politicians taking bribes. The courts have held, for example, that stalking laws cannot be used to prevent public debate by making demonstrations by pressure groups illegal. The same logic should extend to protecting investigative activity by the media under a special duty of scrutiny from such prosecutions. The test on trespass and stalking by the investigative media should be one of necessity for the legitimate purpose of the investigation of suspicion of serious wrongdoing.

Harassment and nuisance are, however, a slightly different matter. The special duty of scrutiny cannot give the media the right to interrogate witnesses, victims, spouses or suspects at their own pleasure, or to draw adverse inferences from silence or refusal to answer questions. Persistent posing of questions and surveillance may be justified, however, again on a combination of the necessity test and the reasonable suspicion of serious wrongdoing.
Turning from collections to disclosures, the special duty of scrutiny cannot protect the media from civil or criminal proceedings on grounds of defamation or libel, breach of trades descriptions, partisan bias on terrestrial broadcasting, breach of quality threshold conditions, or from appeal to the self-regulatory bodies against denial of right of reply.

The most common effort by advocates of wider media freedom to move beyond the narrow scope of activity that would be protected by the special duty of scrutiny is to attempt to pack into the concept of ‘the public interest’ almost anything that some readers, listeners or viewers might enjoy reading about. It is almost impossible to see how any credible rationale for special constitutional protection for the media could extend that far.

It is sometimes said by editors seeking to avoid controls on the manner in which they collect personal information, that tests of the kind set out here cannot be applied in the field or in the editorial office, but only after the fact, by lawyers, and are therefore unfair. This is a self-serving and should be rejected. If editors believe that they can apply the principles set out in the Press Complaints Commission’s own code of conduct, then they can apply these tests which are of the same ethical order of complexity. Indeed, the argument here is that these principles should be used in exactly the same way as the present code is to be used and should only be needed by the courts in the rare cases that proceed beyond the PCC under Article 8.

The public interest

The public interest is usually introduced into discussions of privacy and the media as an exception to general rules in, for example codes of practice or proposed torts. It amounts neither to a positive duty nor to clear criterion as to which forms of collection of personal information might be acceptable and which not.

It may be possible to make a case that a reasonable concept of the public interest would widen the types of individuals on whom media investigations might be undertaken with some kind of protection,
beyond the group of leading decision makers in politics, civil service and business that the special duty of scrutiny covers, to less influential persons who may nevertheless have some public role. However, it would not necessarily extend as far as justifying non-consenting access to victims of crimes (to whom, arguably, special duties of sensitivity and respect are owed). It might also widen the net of activities from serious wrongdoing to systematic hypocrisy.

However, a public interest rationale would still require reasonable suspicion of wrongdoing or hypocrisy or other sin of similar order. While a wider category of journalism than news and current affairs might be protected, it is hard to see that it would extend throughout the pages of a modern newspaper or the programming schedule of a modern broadcast channel. While some kinds of sports and celebrity reporting might be covered, it is hard to see that such a rationale would permit the coercive overriding of privacy by personal money pages, game and quiz shows and the like. Nor could a public interest rationale justify entrapment, theft, interception of communications, nuisance and harassment, or protection against any of the normal rules on disclosures.

However, this is not the most sensible reading of the way in which the concept should be used. It is better to substitute more precise concepts for the vague notion of the public interest. For it is important to distinguish at least the following elements of any public interest consideration of a putative media privacy violation. The public interest requires that only after each has been satisfied, can one proceed to the next.

- **Threshold public interest test:** What is the public interest in whether scrutiny should be exercised, given the initial evidence or question? What is the weight of public interest in any claims of private right that scrutiny not proceed?
- **Procedural public interest test:** What is the public interest in the manner or means by which scrutiny should proceed?
- **Public interest content test:** What is the public interest in the publication of the product of the particular scrutiny?
○ Target of disclosure public interest test: To what outlet – press, police, regulators – is it in the public interest that disclosure takes place?

It follows, then, that the public interest is not a distinct rationale from that of the special duty of scrutiny, but provides the threshold on the basis of which the special duty can be exercised, and sets the constraints under which its instruments and means may be chosen, and the targets to which any disclosure of its results should be directed. On its own and without the concept of the special duty of scrutiny, the idea of the public interest of limited use in enabling us to know what is acceptable and what is not.

On this understanding, it seems clear that the deviations from the general rule in data protection of the ‘fair obtaining’ of personal information collections that would be protected can only be modest. In particular, subject both to a reasonable suspicion and a necessity test, they might permit some measure of protection from trespass suits and prosecutions under stalking laws, but only in exceptional circumstances and then only under special duty of scrutiny, from harassment and nuisance laws. In no circumstances can freedom of the media protect theft or interception of communications without warrant.

Prior restraint

In the USA, the First Amendment to Constitution has long been interpreted by the Supreme Court there as ruling out any form of prior restraint upon the press, and therefore it is especially difficult for anyone – even for government agencies on grounds of national security – to secure an injunction against a newspaper or television station to prevent any publication. The effect of the constitutional restriction is that US law has to take the view that damages are as effective a form of redress and relief for violations of privacy, under federal or state privacy torts, as they are for defamation. English law has taken the opposite view. The general rule in defamation cases has been that a finding against a media organisation will be sufficiently well publicised
to clear someone’s name and then damages will be adequate to compensate for the harm done to someone’s public reputation, esteem and social standing. The opposite presumption has been applied in breach of confidence cases. Since what has been published cannot be made private again after the event, and certainly by means of damages, the English courts have been willing to grant injunctive relief in advance, making privacy one of the few areas in which prior restraint of the media is possible.

The position will change with the government amendment providing general exemption for the media from the privacy provisions of the bill that incorporates the European Convention on Human Rights, including the privacy article. It is possible that this would have the effect, not only of ruling out prior restraint injunctions in privacy cases brought directly under Article 8, but also of ruling out any further prior restraint injunctions brought under breach of confidence, if it were deemed that the privacy article of the Convention, became, by virtue of the incorporation act, the new basis of breach of confidence actions.22

Certainly, any democratic society ought to think long and hard before creating a system of prior restraint and it should be set about with a great many and carefully designed safeguards. However, the fundamental argument is sound, that what has been revealed cannot again be made secret, whereas a besmirched name can be cleared. There is a case for some limited redress by way of prior restraint in privacy cases. The question is, what sort of safeguards should there be? Safeguards can take various forms:

- a seriousness test that will grant injunctions only for cases deemed to be sufficiently serious, example, according to a standard based on the kind of privacy risks that the violation constitutes or could give rise to: for example, risks of unjust inference would be more serious than simple disclosure without consent (especially when read in conjunction with a public interest test); it is perfectly reasonable to argue that less serious privacy risks might be capable of being
compensated appropriately through damages, as is the case in the USA.

- high standards of evidence required before granting an injunction: the effect of this might be that *ex parte* injunctions, (hearing only one side of the case) would no longer be the norm, but that hearings for injunctive relief would normally be conducted on the basis that at the very least a representative of the media organisation would be required to attend, even at very short notice.

- a test of balancing the public and private interest: the introduction of a special duty of scrutiny for media would provide a greater protection against prior restraint injunctions being granted in inappropriate cases.

- *Efficacy* tests based on whether the national geographical jurisdiction of the court is sufficiently large, given the range of media interest in the story that violates privacy, to make any injunction granted meaningful: this would, for example, prevent more pointless and embarrassing litigation such as the *Spycatcher* cases of the later 1980s.

It would be helpful for the law to formalise these test requirements. This would not be out of line with recent developments in the law of injunctive relief in privacy cases. For example, in one of the *Spycatcher* cases, the court specifically placed in the way of injunctive relief a higher hurdle than the conventional test of an arguable case, which permits courts to award interim restraining injunctions on the balance of convenience between the parties.23

However, it matters very much just what kinds of organisation grant prior restraint orders. There is no case whatsoever for the suggestion of the Lord Chancellor, Lord Irvine of Lairg, that the responsibility should lie with the Press Complaints Commission. Although the PCC and many other media organisations objected strongly to the Lord Chancellor’s suggestion, their opposition was grounded for the most part on a rejection of the principle of prior restraint, which, as I have...
argued, is not well founded. However, prior restraint should be granted by the courts and only in cases where it is appropriate.

**Trespass and unlawful invasive surveillance**

Modern surveillance techniques – from the simple telephoto lens to the modem and software agents – have the capacity to achieve at a distance what could once only be achieved at immediate proximity. Therefore, there is a need to re-examine the tort of trespass and to consider whether there is some way that the harms these techniques can facilitate without actual physical trespass upon private property can be made tortious.

The concept of trespass itself is probably not the right vehicle. Clearly, not every use of a zoom lens camera can be an act of trespass or else almost every tourist would commit the tort. Therefore, it would make sense to introduce a new tort that defined the harm to be one related to the intention of the defendant. Its title might be ‘unlawful invasive surveillance’. For media photographers and journalists, the obvious defence that their invasive surveillance was lawful would be the special duty of scrutiny.

**Enforceability**

A key problem in cases of privacy violation by the media is that difficulties in enforcing privacy rights, particularly for those who are neither rich nor famous – as Legal Aid is unavailable for defamation cases and because it is being restricted in many other types of case for reasons of public expenditure control. The Press Complaints Commission and Broadcasting Standards Council are widely seen, rightly or wrongly, as lacking the autonomy from their industries or the effective sanctions that would give the public confidence in their efficacy. While the Data Protection Commissioner can enforce data protection laws on some aspects of fair obtaining and on the regulation of holdings, her jurisdiction over media disclosures is now extremely limited and she has no powers over torts and criminal offences under common law or other legislation.
There may be a case for a *quid pro quo*, that in return for the media being given the recognition of a special constitutional status in the form of a special duty of scrutiny, they would be obliged to contribute to a private, untaxed, fund to assist people with the costs of enforcement of privacy laws against media excesses.

**Implementation**

The European Convention on Human Rights is being incorporated into English law, bringing it with general provisions on freedom of speech and the press in Articles 10 and 19 and privacy in Article 8. The government has set its face, at least for the time being, against introducing primary legislation to reconcile the two, and proposes to leave it first to the self-regulatory system for the press and the existing semi-independent regulatory system for broadcasting. In the final case, it will be left to the courts to find their way through this conflict of rights. This is a reasonable way forward but it will require effort and the development of clear principles to make it work, some of which are set out in this and the following chapter.

However, if the argument is accepted that the special duty of scrutiny does grant a limited special status for the media, this would permit specific defences in civil and criminal cases only for the media and not private individuals.

For a number of reasons, one would prefer privacy law to develop through the self-regulatory system of the Press Complaints Commission, the Broadcasting Standards Commission and, where their decisions are appealed, the courts rather than through primary legislation. Therefore, in the first instance, the arguments in this chapter are offered as a jurisprudential basis on which these bodies and the courts can make decisions in privacy cases. The reasons for preferring this route in the first instance are several.

First, this represents new terrain for the British legal system, and in such conditions it can often be better to allow the jurisprudence to develop in response to actual problems, conflicts and disputes. The role of arguments like the present one is then to offer resources to
judges in the appellate courts that should be appropriate in many kinds of case, but it is not to offer a blueprint to be put wholesale into the judgement in the first case on privacy and media freedom brought after the incorporation of the Convention. Secondly, leaving matters in the hands of judges may enable a measure of flexibility in the jurisprudence, to make it possible to learn from mistakes: by contrast, errors on the statute book tend to stay there for many years before politicians can find time and public support for rectifying them. Finally, if politicians for one reason or another dare not use their powers to legislate, for fear of the retaliation that the media and the national daily press in particular will take, then it may be the simpler route to ensuring some acceptable protection for privacy to allow judges to develop it case by case.

However, the argument can be taken too far. Judge-made law is not always legitimate and not always competently crafted. It is possible that the courts will apply the incorporation act and the Convention itself in ways that would lead naturally to the destination set out in this chapter, but it is far from certain. If the law developed in ways that ran unreasonably contrary to these principles, then it follows from the argument here that there would be case for introducing legislation.

It is often said by opponents of media privacy rules that there are reasons to doubt whether politicians can be trusted with the issue. If they are given the chance, opponents say, they will produce legislation that protects their own kind too well from media scrutiny, to the detriment of democracy. There is something to this argument, but there are problems with it. One could equally well argue that politicians, in a climate of widespread distrust of their profession, would not dare to pass legislation that shamelessly gave themselves undue privileges. In general, there is something dangerous about any argument that purports to yield the conclusion that no group of people whom we citizens could imagine ourselves electing as legislators can be trusted with issues that pertain to the legislators’ own interests. If that is the case, then something is very rotten indeed in the state of Denmark.

Finally, there may be ways in which the challenge can be answered, that it is ‘impossible’ to design privacy laws that will protect ordinary
people from unjustified invasions of privacy by the media but that will not wrongly protect the powerful from justified scrutiny, and therefore, the invasions of privacy suffered by ordinary people are an acceptable price to pay for a press with the freedom to hold politicians accountable. It is the burden of the next chapter to answer this challenge, and I believe that it can be answered.

If there were to be legislation, then, what kind of legislation would be appropriate? While the Guardian newspaper has advocated a specific privacy law, this might not be the only or even way to achieve the end in question. The whole thrust of the argument of this book is that there is a unity to privacy risks. There is no special category of privacy risk that the media raise that are not raised by other kinds of organisation collecting personal information, processing and disclosing them to others, beyond the difference in the size of the audience for any disclosures.

Rather, the need is for integration and coherence in a fragmented system of law that spans human rights; data protection; breach of confidence; interception of communications; police powers of investigation; misuse of computers; copyright; the law of tort in respect of trespass, nuisance, harassment; and some aspects of the criminal law such as stalking. What is required is a programme of legislative reform that introduces some coherence. It would not require a single act to replace the entire corpus of law that is of relevance to privacy. But it would be possible to devise legislation that introduced for the whole corpus, some common definitions of terms, some common principles of the basis on which different kinds of redress – administratively through subject access and rights of correction within the organisation, by way of recourse to the Data Protection Commissioner, the courts, or self-regulatory bodies such as the PCC. The question is whether it is necessary to use primary legislation for this purpose. If we were starting from a position in which there was no legal inheritance on these issues, then it might appropriate to introduce comprehensive primary legislation. Since we are not, it is probably necessary to work over time to integrate the principles that underpin the legal apparatus on a piecemeal basis.
Conclusion

The handling of privacy and the media will be robust and sustainable, it was argued in Part 3, only if it is based on some kind of reasonable treaty between the commitments and interests of the liberal and civic republican traditions, while also offering enough to egalitarians and fatalists to prevent shocks. The liberal tradition needs to be assured about the importance of both freedom of expression for the media and that privacy remains important, but is not an absolute that cannot be traded off by individuals with their own consent in return for other goods and services. The civic republican tradition needs assurance that the public interest is sufficiently buttressed that where it is necessary to override the privacy of an individual for the common good, this can be done, and that in this context, there are sufficient moral pressures upon the decent and public spirited use of private life that individuals will feel that they have some accountability to their community. The aim of this chapter, like the subsequent chapters in this part, is to develop an account of what such a sustainable treaty between the great traditions on privacy might look like.

At the heart of the proposed new settlement is a recasting of the role played by the concept of the public interest. By introducing the concept of the special duty of scrutiny, the balance of presumption is changed and a fundamental liberal commitment strengthened and buttressed as never before in English law. Equally, by providing a basis in tort or equity for injunctive relief in specific circumstances, the liberal concern about privacy is met. On the other hand, the judicial rather than industry-based form of regulation and the continued importance of the concept of the public interest, satisfy certain needs of the civic republican tradition.
18 Public accountability of public servants and people in public life

Introduction
In the previous chapter, we were concerned with the circumstances in which the media have the right to collect personal information on individuals without consent and what general principles should govern the disclosure to the public by the media of personal information they collect. In this chapter, we look at the problem from the other end of the transaction, namely, from the point of view of the individuals ‘covered’ by the media, and ask whether, by virtue of their position, behaviour, fate or other aspects of their situation, they forfeit a degree of protection that other individuals can reasonably expect. There is a long running debate about whether such people can reasonably expect privacy, in the sense of protection from the attentions of the media and also from others – including employers, constituents, colleagues and so on – who may enquire about their private life. It is sometimes said that people in the public eye cannot complain of publicity and loss of privacy because they have chosen to expose themselves to that attention.

It is often argued that any privacy law passed by politicians, or indeed brought into being by judges acting on the basis of the European Convention, will inevitably be one that unjustifiably protects the powerful from media scrutiny. Even if it did provide ordinary people with some protection, the argument goes, this would not be sufficient compensation for the loss of public accountability of the power brokers. Conversely, those committed to this position have to
believe that the lack of privacy protection against media invasion for ordinary people is an acceptable price for a society to pay for media scrutiny of politicians, business leaders, senior civil servants and the like. In this chapter, I try to show that we can answer this challenge and that it is not necessary to sacrifice the privacy of ordinary people on the altar of the special duty of scrutiny.

However, in answering it, one nettle in conventional jurisprudence must be grasped firmly and uprooted. That is a particular interpretation of the doctrine that 'the law is no respecter of persons'. Of course, it would be wrong to dispense less or more justice to individuals according to their social rank, and no one would want to return to the mediaeval notion that aristocrats and clerics should be tried according to different legal standards and only by their own kind. However, the law contains vast numbers of conditional propositions to the effect that if someone puts themselves voluntarily in a certain position, they are deemed to have accepted certain obligations and responsibilities by virtue of having taken that decision, and the law justly treats them differently according to the special situation they are in. In designing an approach to the problem here, I argue that we should treat those who have voluntarily decided to enter positions that might reasonably be construed as ones in public life, as people who do thereby gain certain obligations of accountability that will authorise the media sometimes, in exercise of the special duty of scrutiny, to conduct enquiries, collect personal information and sometimes disclose it without consent.

Anyone who enters public life may be at risk of any of privacy harms identified in Part 1 – excessive surveillance, collection without consent, disclosure without consent, function creep, absence of transparency, absence of anonymity, intrusion, reversal of the presumption of innocence, denial of the means of self-protection, or unjust inference. For the purposes of the argument in this chapter, I shall assume that the reader is willing to accept at least the conclusions of the previous chapter on the question of how the media may legitimately collect information, in respect of the kinds of collection activities which might be granted special defences to certain kinds of criminal charge.
or civil suit under the special duty of scrutiny. The chapter will focus on the questions of:

- how far being in the public eye justifies a loss of control over media collection of personal information (at all) without specific consent
- what kinds of personal information, if any, might legitimately be subject to different kinds of treatment, in the light of the implications of considerations on the first question.

Specifically, the question for this chapter, then, is about what kinds of person in what kind of situation, and about what kinds of behaviour or other matter, would prima facie evidence reasonably justify the invoking of the special duty of scrutiny for the media to collect personal information with a view to disclosure?

**Who enters public life, and how ‘voluntary’ is entry?**

On the first aspect, of the kinds of person and situation, we can distinguish several types of case. One special case of the general conflict between the claims of freedom of the media and claims of privacy occurs in respect of politicians, who have voluntarily put themselves forward for election and therefore for the scrutiny of the public in respect of their ability as legislators and, if their party is successful at the polls, perhaps in posts of responsibility in government and, ultimately, as Cabinet ministers.

A second case is that of salaried public officials – senior civil servants, heads of commissions and agencies, judges, directors of regulatory agencies – whose work, responsibilities, role or relationships with ministers bring them into the limelight. In general, in the UK, these people have put themselves forward for recruitment by selection rather than election into posts that may or may not, given the conditions obtaining in the period of their service, attract public attention. The degree of media and wider public interest in their roles bears no very consistent relationship with the seniority of their rank. For example,
whereas the director of a national utility regulatory agency may become a household name, a much more senior civil servant at permanent secretary level may be wholly unknown and hardly ever referred to in media reporting, while a junior clerk who becomes a ‘whistleblower’ may be fêted. Within this group, then, there are degrees of ‘voluntariness’ about their entry into public life, which include, in the first dimension of initial recruitment to public life:

- putting oneself forward, knowing the risks and opportunities, for a job highly likely during the expected period of tenure to bring the postholder into the eye of the media
- putting oneself forward, knowing the risks, for a job that may at some point, if something extraordinary happens, bring the postholder into the public eye
- putting oneself forward, without knowing or even thinking of the risks, for a post that is most unlikely in the ordinary run of things, to attract public attention

and in the second dimension of subsequent behaviour:

- in the course of occupying the post, doing something, not doing something, declaring something publicly, hiding something from the public, that one know will likely lead to public attention
- in the course of occupying the post, and without doing anything of one’s own, being put into a position by the actions of others, that one’s work or behaviour or character become a matter of public attention.

Then there is a third category of people described fairly as being in public life and for whom the term ‘celebrity’ is generally reserved. These include actors and directors from stage and screen, music, dance, broadcasting, journalism, professional sport, fashion and some
categories of design, *haute cuisine* and certain rather specific categories of writing – cookery writing, certain genres of popular fiction and the like. In general, the very definition of success in these industries is that one becomes a public figure, and one enters the business hoping for that kind of success.

Fourth, are people who pursue a career, profession or vocation and are successful, and therefore come to the attention of the specialist media – business pages, trade press in law, consultancy, architecture, software design, academia – and who, from time to time are sought after by the national media. The initial decision to pursue that path will, in most cases, may or may not have been taken knowing or even thinking of the risks and opportunities of exposure and possible privacy concern that success might bring. How many people now in the position of architect Richard Rogers or lawyer Helena Kennedy or business empire builder Richard Branson or business leaders such as Lord Weinstock of GEC or Sir Richard Sykes of Glaxo Wellcome designed their career having thought through the kinds of trade-off they might have to make, the media being interested in such work, between success and privacy? Probably rather few.

On the other hand, while the *initial* move may not have been made in that spirit, perhaps a good many such people will have made the last move before fame into the position where they attracted public attention with at least some knowledge of what they were taking on. In at least some cases of this type, the decision to pursue the career path may be taken hoping for public attention for one’s work, but not one’s person or personal life. For example, the millionaire businessman Howard Hughes and the novelist JD Salinger both wanted public interest in their companies and projects, but sought in every way possible to prevent loss of personal privacy.

The fifth category of people who enter public life, and in whose lives the media develop an interest, are entirely ordinary folk to whom something extraordinary happens – winning the National Lottery, achieving some honour, being arrested for or suspected of some crime. The degree of voluntariness with which ‘ordinary’ people in extraordinary situations enter public life varies.
One may do something extraordinary, knowing the risks of public attention and perhaps either seeking public attention, such as trying to see a world record or walking around the world, or else being reckless of the risks of attracting it, such as in committing a crime.

One may do something extraordinary without thinking of the risks of public attention, such as bravely shielding children from a psychopathic murderer or saving someone from death by fire or water.

One may do something entirely ordinary with no expectation of entering public life, but find oneself the object of attention, such as being the victim of a crime, or being related to or a friend of or a neighbour of a celebrity or a politician. While many people fantasise about winning the National Lottery, it seems very strained and forced to suggest that purchasing a ticket with a one in 27 million (or whatever) chance of success is tantamount to putting oneself forward for public life with all its attendant risks.

What behaviour or situation might call for publicity without consent?

In particular, we need to consider the kinds of reasons and rationales for public attention for which public and media attention may follow each of these categories of person, since these different rationales carry rather different kinds of weight in respect of different categories of people. The first category of rationale concerns allegations of wrongdoing. These may include allegations of:

- **role-specific crimes**: crimes that only someone in the position the subject holds could commit, such as fraud on the organisation employing the individual
- **role-specific civil wrongs**: behaviour that could be the matter of a civil suit against the person, by way of breach of contract or tort, and which could only have been committed by
someone in that post, such as breach of a contract or use of the position to commit a nuisance or harassment

- role-specific misdemeanours: behaviour that is neither criminal nor civilly actionable, but is considered unethical, undignified, shady, in anyone in any position in life, and could only have been committed by someone in that position, such as abuse of power or abuse of position

- role-specific failures: such as incompetence in one’s post or particular tasks the post calls for, failures in particular projects for which one has responsibility

- role-specific character flaws or behaviours that would not be misdemeanours in general but only count against someone in that position: such as arrogance, highhandedness or recklessness in the carrying out of one’s duties, or hypocrisy in the use of one’s position to advocate a certain kind of private morality that one does not practice in one’s own private life, or conducting one’s private life in a way that impairs one’s ability to do one’s work or fulfil one’s role effectively

- generic crimes: crimes that anyone could commit, such as murder of a spouse or rape all the way down to traffic offences

- generic civil wrongs: behaviour that could be the matter of a civil suit against the person, by way of breach of contract or tort, but which could have been committed by anyone and does not pertain only to the post held, perhaps done in the postholder’s own time outside work;

- generic misdemeanours: behaviour that is neither criminal nor civilly actionable, but is considered unethical, undignified, shady, in anyone in any position in life, and could have been committed by anyone;

- generic failures that anyone could commit or suffer: such as failures to manage one’s personal finances particularly well, where that does not betoken any particular likelihood that one will do the same in one’s post;
generic character flaws or behaviours that, while no regarded as misdemeanours, would be frowned upon in anyone: such as sexual promiscuity, rudeness to friends and casual contacts, lack of respect for one's parents.

The second category concerns, not allegations of wrong doing but where claims are made of a right to ‘fair comment’ on behaviour that is not in any way wrong, or a situation (fortunate or unfortunate), perhaps not of the subject’s choosing, in which the collection and disclosure of personal information is reasonably a matter of which the public has a ‘right to know’ and perhaps hear comment and argument. Again, we can distinguish several types of case:

- **externalities**: the behaviour or personal situation has implications for the lives of significant numbers of other people outside the immediate circle of family, friends and immediate colleagues of the subject
- **exemplariness**: the behaviour or personal situation involves the setting of an example or a precedent, for example of standards of behaviour in situations like this one, to significant numbers of people outside the immediate circle of family, friends and immediate colleagues of the subject
- **illustration**: the behaviour or personal situation illustrates some fact, trend, problem, opportunity or risk of wider significance to significant numbers of people outside the immediate circle of family, friends and immediate colleagues of the subject
- **entertainment**: the behaviour or personal situation of the subject would amuse, entertain, titillate, provide a ‘good read’ or a ‘good story’.

Figure 13 overleaf sets out these categories along these two dimensions. If we consider the top left corner of the table, and in particular the cell that relates to politicians committing role-specific crimes, few people would have any difficulty in saying that here is a case par
<table>
<thead>
<tr>
<th>matter of enquiry</th>
<th>specific crimes</th>
<th>specific civil wrongs</th>
<th>specific specific crimes</th>
<th>specific civil wrongs</th>
<th>specific character flaws</th>
<th>generic crimes</th>
<th>generic civil wrongs</th>
<th>generic character flaws</th>
<th>generic misde-meanours</th>
<th>generic failures</th>
<th>generic character flaws</th>
<th>externality</th>
<th>exemplar illustration</th>
<th>entertainment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Politicians</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salaried public officials in posts ordinarily likely to attract public interest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salaried public officials in posts occasionally likely to attract public interest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salaried public officials in not in posts likely to attract public interest who do something extraordinary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Celebrities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Successful people who do not seek celebrity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ordinary people knowingly or recklessly doing something extraordinary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ordinary people doing something extraordinary without knowing or being reckless of privacy or publicity risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ordinary people doing nothing extraordinary but being thrust into the public eye involuntarily</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 13** When should people in public life protected by privacy from media scrutiny without their consent?
excellence where the special duty of scrutiny of the media should justify enquiry. It was this kind of prima facie evidence that led Woodward and Bernstein to uncover the Watergate scandals, and surely no one would say that in such a case, privacy considerations could be a defence against scrutiny.

On the other hand, the extreme bottom right cell of entertaining stories, collected and disclosed without their consent, about ordinary individuals who have not done anything extraordinary but are thrust through no action of their own into the public eye, is an area where many people would say that the special duty of scrutiny cannot be used to justify overriding privacy considerations. As judges have held in a number of breach of confidence cases, it cannot be true that anything in which a prurient public might be interested is there a public interest in collecting information and disclosing it without consent.

The question is, therefore, where in the matrix can a line or lines be drawn between the acceptable and the unacceptable?

**Arguments on situations where it is acceptable to override privacy concerns**

There are several general kinds of argument in common use to justify the overriding of privacy concerns for media scrutiny of people in the public eye, which may help us to decide where to draw lines in the matrix in Figure 13.

Let us consider first the allegations of the five types of role-specific wrongdoing. The main arguments offered about the case for overriding privacy claims in these cases are to do with:

- **fitness for role**: a person alleged to be guilty of any of these five types of wrongdoing would be, if the allegations were substantiated, by that fact alone, unfit to hold their role, and therefore the media’s special duty of scrutiny justifies the overriding of privacy to permit the collection and disclosure of personal information without consent

- **public accountability**: In the case of allegations of failures and character flaws, while these might not make someone unfit
for their post, there is a duty of public accountability of any postholder in these categories for their conduct in their role to their employers, their customers, and the public generally, which justifies the media in overriding their privacy.

In relation to allegations of generic wrong-doing and to matters where ‘fair comment’ and the ‘public’s right to know’ are claimed, there are three main arguments that are conventionally offered, which can conveniently be summarised as follows:

- **implicit contract**: Having once voluntarily entered into public life by taking a public role, or by offering their personality for public consumption by entering any of the ‘celebrity’ industries, a person is then implicitly under some kind of contract with the public, from which they may not voluntarily withdraw later on, to hand control over when personal information may be collected and disclosed.

- **spillover from character to role**: Personal information about generic behaviour is important and subject to the special duty of scrutiny, because character flaws and other doubtful behaviour, even in the sphere of life outside the subjects’ ‘official’ role, cannot be insulated from their conduct in that official role. Such information gives important clues about the risks of misdemeanours or worse, and about their likely fitness for their work – it is sometimes said that a person who will cheat on their spouse will cheat on their employer or their constituents.

- **always exemplars**: Anyone who comes into public life, voluntarily or otherwise, *ipso facto* becomes a role model and has obligations to behave in ways that uphold that standard – this may even mean that past behaviour is made relevant to the example they now set. Therefore, any kind of personal information is the proper subject of the special duty of scrutiny.
Appraising the arguments and drawing lines
Role-specific wrong doing

It seems almost unarguable that at least a question would be raised about the fitness for their role of a politician, a public servant, a ‘star’ in any of the celebrity industries, or any successful person, indeed any ordinary person who committed a crime that was possible only through their role. Likewise, a role-specific breach of contract or the commission of a tort in such a situation would also raise a question about the fitness for post. In these cases, therefore, it seems reasonable to hold that, on receipt of *prima facie* evidence, a special duty of scrutiny would justify media enquiry. Likewise, alleged incompetence in the skills required by one’s role is obviously a matter that would raise questions of fitness, and it seems sensible to permit privacy to be overridden in such situations.

However, everyone experiences failures in specific projects, and most of us learn only through our mistakes. The argument from public accountability surely justifies enquiry and disclosure without consent, overriding privacy, in cases of failures in politics and public policy, public administration and publicly quoted businesses, and perhaps some of the celebrity industries. On the one hand, while a publicly subsidised opera production that flopped might justify it, but on the other, surely no one thinks that every bad popular novel or every bad academic book can trigger justified overriding of novelists’ and professors’ privacy by the media.

Moreover, it is hard to see that any but the most egregious (that is, with very significant externalities) project failures by ordinary people would justify overriding their privacy. A person who set out to break a world record in some non-sporting field might want publicity if they succeed, but their wish for privacy about the reasons for their failure if they do not can surely be protected against claims of media scrutiny and a public ‘right to know’. Reasons for failures are only matters of public concern where they are not really personal because there are large externalities. If a large publicly quoted company is failing, it affects many shareholders in the company and perhaps shareholders in other companies too, and the behaviours of the management is not
protected. Even privately owned companies in important market positions can, in the event of failure, have effects on the wider markets and so the personal behaviours of managers are not protected because the failure is not truly a personal one.

Role-specific character flaws seem properly a matter that justify overriding privacy claims in the case of politicians, high profile public servants and some very famous and important celebrities who actually do play a particular role of exemplar with ‘their public’ (but again, surely not any novelist, any minor pop singer, actor, dancer or chorus member, or indeed, journalist) and successful people who are not celebrity-seekers, where the flaw can be shown, if the allegation is substantiated, to affect fitness for role. Power arises in many roles, and character flaws that are relevant to the use and abuse of power cannot be protected by considerations of privacy. For example, some, but not all, of the personal vices of the leaders of such cults as the Church of Scientology affect not only their roles but the fates of millions of their followers and have real externalities.

If someone adopts a particular public role or puts themselves out in public as being a certain kind of person – virtuous, religious, having a particular sexuality – then they have by that act waived the protection of privacy on any personal behaviour of their that is discovered to be inappropriate to their role or incompatible with the claims they have made about themselves. On the other hand, there must be a reasonable degree of intention and explicitness about the adoption of a role here, before privacy protection is lost.

A religious broadcaster who says of herself or himself that she or he is a sinner like anyone else in the pew is not thereby forfeiting privacy on her or his private sins: just by being a religious broadcaster, one does not implicitly lay claim to any special virtue.

By contrast, it seems difficult to sustain the case that the character flaws of ordinary people, who even do extraordinary things but neither knowingly nor with disregard to the risks, are a legitimate justification for overriding their privacy.

In general, then, it seems that the public accountability argument only adds a little to the fitness for role argument, and mainly in the case
of project failures in public policy and management and in publicly quoted businesses, and perhaps the most serious character flaws in these areas and for a very few celebrities.

**Generic wrong doing**

No one disputes that anyone committing a crime or a civil wrong can legitimately be the subject of media scrutiny without being able to claim privacy as a defence. The matters that require more thought are those pertaining to personal misdemeanours, personal incompetence, failed personal projects and character flaws that do not relate to the role occupied.

The first argument to be considered is that of an implicit contract. As stated in the bald form above, the argument is surely too extreme. First, the idea of an implicit contract that applies to people who did not voluntarily enter public life seems absurd. In the absence of a an implicit contract, it is hard to see what other kind of rule one could invoke in the situation of such people. Something is either a tort or it is not: surely no one can sensible claim the existence of an implicit tort for people who did not choose to be in public life that relates to some obligation to manage their finances, sex life and personal projects by the prevailing standards of decency and success, and not to have character flaws in their personal life.

Secondly, the idea of an implicit contract that applies retrospectively to personal behaviour and competence, personal projects and character prior to a decision to enter a role that might bring public life surely demands more than is reasonable. Of course, someone who enters public life and is subsequently found to have earlier committed crimes or civil wrongs in their personal life, can hardly expect to plead privacy against media scrutiny, except in the case that their youthful offences are now spent under the rehabilitation of offenders legislation. But we are here dealing with much more minor matters, and matters not specific to one's role, and the strength of the argument is accordingly much weaker.

The argument of a spillover from character in personal life to public role is a difficult one to sustain. Certainly, there must be cases where
there are such spillovers. But the fact of such cases cannot lead us to overturn the general rule of the presumption of innocence. Just because in some people’s cases an inability to manage their personal finances effectively will indicate an inability to manage the finances of their business or division of public administration, it does not follow that this will be true in every, or even in very many cases. Indeed, if literally every personal lie, marital infidelity, mismanaged personal bank account or credit card account indicated incapacity for role, then there would no distinction between the generic and rolespecific, which is clearly absurd. Prima facie evidence of any of these things, without more to indicate some specific link in this particular case to fitness for role, concerning anyone, even a politician, coming into the hands of a journalist, cannot justify the invoking of the special duty of scrutiny and the overriding of privacy.

The argument that literally anyone in public life is a moral exemplar to other people cannot be sustained. Certainly, hardly anyone expects business people, civil servants or successful academics, lawyers and surgeons, or Hollywood stars to be role models. The argument only seems ever to be advanced in the case of politicians – and mainly in connection with national politicians, rather than local councillors or members of the European Parliament – and a very few pop singers, and very occasionally of successful star footballers and athletes. Certainly, people who enter public life involuntarily cannot have the responsibility thrust upon them.

The first point to make about this list is how arbitrary it is. No one has ever advanced a clear rationale as to it should be just these people and not others who have the responsibility of role models. Nor is clear when in their lives the responsibility begins – when they first contemplate the possibility of their chosen career? when they enter it? when they become successful? Surely the responsibility cannot apply retrospectively, and even if could be made retrospective, it surely cannot reasonably be made to apply any further back than the time of the decision voluntarily to enter public life.

Nor is the argument very clear about the scope and limits of the job description of a role model. Just what counts as success? Is someone
who leads an exemplary life but whom no one follows and whose life no one regards as having any influence or relevance for their own, still a role model? And what responsibility does one have for one’s public image? If someone leads an exemplary life and the media describe them as ‘boring’, ‘squeaky clean’ or ‘goody two-shoes’, have they ‘failed’? And to whom, exactly is a role model accountable?

None of these considerations are sufficient reason for rejecting the argument outright. However, they are reasons for placing limited weight upon it, except perhaps in the case of some politicians and some celebrities who positively choose to champion moral causes, And in that case, the argument in the privacy context boils down to a case for exposing putative hypocrisy, a role-specific character flaw.

In my view, therefore, in principle, even in the case of a cabinet minister who is unfaithful to her or his spouse but where this does not indicate anything about her or his capacity to act effectively as a minister, where the minister has not abused her or his power wrongly to benefit the person with whom they conduct an affair, and where that person has never set themselves up as a preacher of personal morals to others, there is no special duty of scrutiny upon the media that would justify the collection and disclosure of personal information about that infidelity without consent of the parties involved.

However, there is a key problem with this conclusion. It almost certainly now fails the test of cultural viability. The pressure of egalitarian and civic republican sentiment that at the very least politicians’ and perhaps celebrities’ generic misdemeanours, that do not impact directly on their role, should now be held open for media and public scrutiny is probably now irresistible. However, there is nowhere near such great cultural pressure for the same measure of openness about the private lives of business leaders, civil servants, judges, barristers, or newspaper editors.

The effect of this shift to a culturally more viable rule on the privacy that can be claimed by the sexual partners, friends, family, neighbours and former colleagues of those who choose to enter politics, music, fashion or film acting is certainly serious. There must be many people who have not entered these careers precisely because they do not feel
that it is fair or reasonable to deprive the people closest to them of control over a range of personal information about themselves. If in the long run, the price that we pay for removing privacy protection for the generic misdemeanours and character flaws of these categories of people in public life, is that only those people enter public life who have the arrogance, selfishness and insensitivity to the ties of friendship and family life, to disregard these considerations, then of course, we may need to consider whether this is an acceptable price to pay and whether the line drawn in the matrix remains culturally viable.

**Matters of fair comment and a public right to know**

We now turn to matters with large externalities, personal facts used to give an example, illustrate trends or entertain.

In general, any personal behaviour which has sufficiently large externalities in the sense that it affects large number of people is in most cases considered in Figure 13 no longer really *personal* behaviour at all, and therefore can hardly be protected against justified scrutiny by privacy at all. The only category of people who surely can to claim privacy protection against non-consented media scrutiny here are ordinary people who have not voluntarily entered into public life but whose personal behaviour sometimes does have wider implications. Examples here include victims of crime, victims of accidents and infectious diseases.

In cases where personal behaviour is in question but about there are no allegations of criminal behaviour, breach of contract or tortious acts, or of incompetence, failed projects, misdemeanours, or character flaws that affect their public role, it is hard to see that the argument from exemplary status has any bite whatsoever. Those who do not set themselves up as exemplars are not turned into exemplars retrospectively by virtue of choosing a profession that leads to their being in public life.

The final two cases of illustration and entertainment prose fewer problems. While illustrating trends and points and entertaining people are legitimate activities, it is hard to see that without specific wrongdoing
or externalities, there can be any justification for overriding personal privacy without consent of anyone, even a politician, in pursuit of these goals.

Most cases of conflict between media scrutiny and press privacy, however, are more complex. There are very few interesting cases which fall neatly into a single cell in the matrix. For example, a person in public life may conduct an adulterous affair for a period, as the late President Mitterand of France did. This fact alone would, on the argument above, in principle, be one for which some privacy protection might reasonably be claimed. However, if there were also an allegation that taxpayer’s money were unlawfully or secretly used to house or otherwise benefit the mistress or paramour, or that a position in public life was improperly granted to that person through the use of the power of patronage where the interest was not declared, then clearly, this would not be protected. In order to exercise scrutiny over the latter, it would be necessary to override privacy on the former, and any privacy protection on a directly related fact that obtains if that fact has no connection with any other allegation which is not protected, will not carry over. This is, I think, broadly in accord with most people’s intuitions.

**Conclusion: what privacy would protect**

The shaded area in Figure 13 represents the kinds of putative personal ‘facts’ about different kinds of people who come into public life, that should, on this assessment of the arguments, be protected against media enquiry and disclosure without their consent by privacy claims against, rather than those claims being overridden by the media’s special duty of scrutiny. Those areas lightly shaded are those where, on a principled consideration of ways in which trade-offs should be achieved between the imperatives of media scrutiny and personal privacy, privacy protection should be extended, but where the argument cannot be won in the prevailing cultural conditions of Britain for the foreseeable future.

There is a lot of white space in Figure 13. That reflects the fact that there are important areas concerning allegations of wrong doing by
those in public life which pertain very directly to their public role, and legally culpable wrong doing which does not, where privacy cannot protect the powerful or the famous from the special duty of scrutiny which lies upon the media. However, there are other areas where the special duty of scrutiny cannot reach and there seems to be a culturally viable strategy of holding a line around them.

Again, it is now, in the first instance, for the appellate courts to consider how best to apply Article 8 and to combine the continental jurisprudence in cases under that article with British case law under breach of confidence. If they fail to do that adequately by the standards set out in this chapter, there would be a case for primary legislation to introduce a tort along these lines.
In this chapter I draw on the drivers of change, future scenarios and arguments about conflicts between privacy and other values developed earlier to set out more prescriptively what might be done to underpin privacy by way of data protection in this rapidly changing environment. Recommendations are also made for action by other businesses and individuals.

**Freedom of contract and economic liberty**

The future of privacy, by way of the efficacy of data protection laws in most business contexts, depends on a complex battery of forces. These include the basis of both transnational and intra-European business competition in trust or simple price, the principle of data protection as a form of respect for customers, the growing role of strategic alliances, the nature of public purchasing, the development in database marketing of ‘marketplace of one’ systems, and the capacity of regulators both to enforce the law and to influence cultural change in favour of respect for privacy.

Today, the wholesale deregulationist case is rarely put against data protection. On the other hand, there are industries that find the European Directive particularly irksome and use arguments that call for the wholesale repeal of data protection law. Nevertheless, if there should be a more general political polarisation again in the next ten or
fifteen years, it is possible that this line of argument will re-emerge with greater vigour.

The general argument from economic liberty

The basic economic liberal or deregulationist case against privacy protection is the claim that a business has ownership of personal information about individuals which is captured or collected in an attempt to sell them goods and services and that no business should be politically or legally accountable to customers as the market is where businesses are economically accountable.

In theory, if consumers knew exactly what information was collected about them by businesses, what was done with it and what the benefits were to them, they could make informed choices about who to do business with. In practice, their lack of information, their inability to make comparisons, possible lack of interest, business monopoly and other regulatory factors make the consumer market in business ethics a less than effective one.

In principle, public policy should do things that would improve the information on which consumer markets run before trying regulation. For example, there may be scope for thinking about how the reporting duties of companies in company law could be changed to encourage them to make statements about information ethics in annual reports. This would at least enable consumer watchdog bodies to make comparisons, offer advice to consumers and to ‘name and shame’ companies reporting particularly poor practice or failing to report at all.

However, there are many privacy risks that consumers cannot hope to control for by reading the advice of Which? and checking the company’s entry in the Data Protection Commission’s register, or by reading the annual report or other publicity. For example, many cases of excessive collection, function creep, and unjust inference cannot readily be observed, even by those affected. Therefore, there is a reasonable argument for some protection to supplement what consumers can do for themselves.
Secondly, there is the important consideration that trust based competition, in those areas where it does occur, may only occur because the data protection legislation puts a floor of protection underneath transactions. The problem with the ‘markets in privacy’ scenario and with the economic liberal argument here is that the process for consumers and businesses of regularly checking the information ethics of companies is not merely transaction costly, but belongs in a low trust environment not conducive to the kind of ‘relationship marketing’ that many retail industries aspire to.

There are crucial issues of control raised by business techniques of advertising and marketing. In general, businesses want more control over consumers. They want to influence them to purchase and re-purchase their goods and services and to reveal personal information that gives clues about how best to do that. Yet they also want consumers to trust them, which may mean helping consumers to feel that they are in control of their preferences and the personal information they reveal, even if the aim is to abridge that consumer control. As the late Groucho Marx put it, if you can fake sincerity, you’ve got it made. It is from this conflict that most consumer protection law has derived, and which has been the basis of the European extension of data protection into the private sector. It has been the unwillingness of many in the United States to accept that there can be a conflict here that prevented, until very recently, the extension of the 1974 Privacy Act principles into the business sector. However, following very public disagreements about the use of some privately collected information from credit reference services by data service companies such as LEXIS-NEXIS, which were alleged to allow the theft of personal identities through access to other people’s social security numbers, companies in the US have agreed a self-regulatory code of practice. The Federal Trade Commission has indicated that it will use its powers to prosecute some violations of privacy as ‘unfair and deceptive trade practices’ if they do not meet the standards set out in this code.\textsuperscript{25} It is not yet clear how far this trend will go, and how far it will be acceptable to Americans that privacy law can be brought to the US by this route. It is still possible that, as trans-Atlantic trade grows and the volume of personal
information from Europe processed in the US grows correspondingly, there could still be a clash of privacy cultures.

The point to take from the economic liberal argument in this case is that innovations in contractual methods of encouraging the development, adoption and adherence to sound information ethics in business are important complements but not substitutes for some baseline statutory protection of the kind offered by current legislation.

The specific argument from costs to business

That compliance with data protection has costs for business cannot be denied. However, this may simply be an argument for designing respect for privacy into information management systems from the beginning. Moreover, the institutionalisation process of data protection dates back at least to 1984 when the first comprehensive British legislation was adopted.

The issues about the distribution of risk in morally hazardous relationships also require business strategists to make judgements about the extent to which their pursuit of corporate transactional efficiency will create legitimacy and trust problems. Genetic information could prove to be a case that alerts the public to a number of such cases. The short term costs of responding to privacy concerns need to be seen in the context of possible longer term trust problems.

However, the issue of costs to business cannot be quickly dismissed. A number of specific costs must be considered.

While the duty to adopt adequate organisational and technical security does involve costs, in some cases significant short-run costs, for the most part business has other reasons to want to bear these as investments. There are other benefits from data security arrangements to business apart from data protection compliance.

Certainly, if the rules of third country transfers were to be enforced in particularly heavy handed or stringent ways that disabled many of the ordinary message transmission and outsourcing systems adopted by business or else forced the writing-in of European data protection standards into every contractual arrangement for data handling outside
the European Union, then this would be a serious cost. The third coun-
try provisions may prove to be a bed of nails for regulators, unless they
are willing to innovate and work with business and lawyers to develop
standard off-the-peg contract clauses that will be readily monitored
and comprehensible. There is, happily, some evidence that such model
contracts can be developed: the International Chamber of Commerce
is currently developing such a document.

The provision of ‘opt out’ boxes in mail, fax and e-mail preference
services involves the installation of procedures for handling opt-outs
that may be costly, on a one-off basis, for some marketing agencies to
cope with. However, these are also costs that these agencies have some
reason to want to incur in any case. Not only are these systems rela-
tively cheap ways of buying trust, they also help with the aim of
achieving greater targeting of offers and avoiding wasted communications. In this sense, there is no long run conflict between privacy costs
and the basic goals of database marketing While a principle of prior
active consent would have brought heavy costs on commerce had it
been implemented in the 1995 Directive, this has not been insisted
upon.

Principles

Concern about privacy protection in business is rising as awareness of
privacy risks grows. Some risks are becoming more severe as the
nature of modern business changes to depend increasingly on stocks
and flows of personal information. There are limits to the scope of
 purely transactional solutions. Therefore, there is a strong political lib-
eral argument for the retention of data protection and even its
strengthening in business settings where, unlike in the news and cur-
rent affairs media, there is no special duty of scrutiny. A number of
basic principles should inform the next phase of policy making.

The first must be the assumption that the nature of global competi-
tion in such key businesses as financial services will take the form not
of a Gresham’s law in privacy, but of a virtuous cycle of trust. The
wager is that respect for privacy will, for the most part, prove to be a key
element in strategies to secure consumer trust, and that countries that can offer high standards of privacy in the handling of personal data will also have a trust advantage in attracting global investment. For the most part, this is the view of much of the large corporate sector who generally no longer regard privacy, in principle, as the alarming burden that their predecessors might have done before the 1984 Act, although they remain concerned about the cost of over-regulation.

Second, to reduce the burden of compliance on responsible businesses of any regulatory change, the aim should be to design policy such that after any once-for-all expenses have been incurred, any continuing costs are minimised. Third, where privacy comes into conflict with other desirable goals, such as:

- competitiveness and avoiding any burden on business which is not strictly necessary to protect individuals and businesses against these risks
- integration of executive government, where it is valuable to improve the capacity of public management to solve real social problems
- the shift toward more preventive strategies in many areas of government which requires the collection of personal information and its use in risk assessment. Despite the heightened risks of unjust inference, this is in principle a valuable direction in which to move
- greater openness of government in respect of non-identifiable data more personalised service from public bodies
- investigation and detection of very serious crimes of violence against persons or property, such as terrorism, child sexual abuse, murder, arson and perhaps the more serious forms of informational sabotage, and
- enforcement of reasonable contractual or public law duties to minimise fraud, moral hazard and adverse selection where business or government bodies bear some risks.
It should be construed *in so far as possible* in such a way to be compatible with encouraging these forms of modernisation and not become an obstacle to progress, effectiveness or efficiency. Those privacy advocates who sometimes appear to be demanding the return of antiquated government and business organisation do no service to the cause of ensuring practical development of respect for privacy.26 The key issue for the design of data protection law and codes of practice must be how these goals are pursued. In general, the tests to be applied should include the following:

- Can the activity be conducted effectively without the use of personal information?
- What is the minimum necessary personal information required for the activity?
- Are true identities necessary at every point in the data system, and for every category of user?

Fourth, while the goal of law enforcement cannot and must not be downplayed, law enforcement agencies and tax authorities must accept that generalised surveillance, ‘fishing expeditions’ in data matching, and excessive reliance upon and unguarded inference from very soft data are in many cases, inefficient ways to prevent or detect crime, even if they could be legitimate in a liberal and democratic society. The same principle applies in the control of fraud. Fishing expeditions and crude data matching often result in many hundreds of ‘raw hits’, which must be winnowed down at great cost in time and resources, and often result in no firm convictions, while undermining other goals such as privacy and legitimacy in the administration of services. It is particularly sad to see that the Inland Revenue, among others, has sought to secure in the 1998 Data Protection Act a very wide ‘Henry VIII clause’ giving the Secretary of State powers to exempt from data protection laws an almost unlimited range of government activity. In a free society, where there is a case for privacy being overridden in the course of the administration of tax or any other transaction with citizens and businesses, there should be a clear, transparent and specific
legal authority for the coercive collection of particular categories of data: blanket exemptions can be the basis for unacceptably oppressive behaviours.

Fifth, law enforcement agencies must accept that not everything that might be used in a crime can be prohibited. On such an approach, the contents of most people’s kitchens, the use of the post service, the telephone and the internal combustion engine would be among the first things to be forbidden. Just because criminals sometimes use strong cryptography, it cannot be right to prohibit its use by respectable businesses and individuals as a means of securing data.

Sixth, and most importantly, the general aim of policy should be to promote privacy as far as possible by putting in place protection against the risks identified at the beginning of this study, namely:

- unjust inferences from ‘soft’ or inappropriately matched data
- loss of transparency about personal information of which one is the subject
- collection of data without the consent of the subject
- excessive or unjustified surveillance
- loss of anonymity
- unnecessary or unjustified disclosure
- reversal of the presumption of innocence, and
- loss of access to the means of protecting oneself from these risks.

Privacy regulation
A simple comparison between the eight principles embodied in the 1994 legislation, even as expanded and amplified by the 1995 Directive and 1998 Bill, and the policy goals set out above, shows that the present intellectual framework of data protection, rather than of privacy, is not adequate for the task as understood here.
Firstly, the current legislation does not put in place sufficiently specific restrictions against:

- **Loss of anonymity.** The fourth principle that information should not be excessive is not sufficient, because it does not insist that true identity should only be collected where it can shown to the satisfaction of the data subject and, on appeal, the Commissioner, that it is absolutely necessary for the fulfilment of the purpose for which the data are collected.

- **Collection of data without the consent of the subject.** Although the Directive made some movement in this direction of the consent, only the negative provision is embodied in law. An individual or business wishing to have their name removed from a database can insist upon it, unless some legal duty such as taxation or regulation overrode the right of removal. This is widely considered by the public to be inadequate.

- **Reversal of the presumption of innocence.** There is currently no principle of data protection that covers this concern in the control of data matching and mining or profiling.

- **Loss of access to the means of security.** This has not traditionally been a data protection concern, but has fallen between the interests of law enforcement and promotion of commerce in respect of allowing individuals and businesses to use whatever systems of encryption they wish: the present DTI proposals do not unambiguously put in place any such right, although officials have stated that it is not their intention to make it a criminal offence to obtain or use encryption software.

The opportunity of the 1998 bill should be taken to introduce legal protections in the form of rights, rebuttable only in specific circumstances against the above risks. It would be a missed opportunity if this were not done and government had to return to data protection law again in a few years.
**Notification**

The list of current exemptions from duties upon government and private agencies to notify the Data Protection Commissioner of their holdings of personal data should be curtailed. In particular, data held for national security, pensions, payroll and accounts purposes should be notified.

**Excessive and irrelevant material**

There should be a right to have excessive and irrelevant material erased. Although the fourth principle sets its face against the collection and holding of such data, it is a loophole in the legislation that there is no specific right for their removal.

**Subject access**

The exemptions from rights of subject access should be curtailed. Indeed, the only exemptions should be:

- data held by the police or other law enforcement agencies for the purpose of conducting criminal investigations, where and only where subject access could compromise the effectiveness of an investigation. The present exemption covers absolutely any database that might be held to be useful in preventing or detecting crime, and can cover many kinds of data where individuals can, without any harm to the enforcement of law and the detection of crime, have the right to know and perhaps challenge what is held about them
- data held in reserve during the course of commercial negotiations for the purpose of making decisions on claims put in those negotiations
- data subject to legal privilege
- data held for research purposes only, where the research agency can show that it will, on the completion of the data collection, anonymise the data.
Independent subject access

There should be a right to use independent agencies to secure subject access, thus vertically disintegrating data use and provision of subject access.27

Freedom of information

The principle of ‘serious harm’ for those seeking to prevent a disclosure about others that would also release personal information about themselves under freedom of information legislation should be abandoned. It should be sufficient for someone to show that data protection law would be infringed by the disclosure, without having in addition to show serious harm.

Codes of practice

Each industry, and the public sector as a whole, should be required within three years of new primary legislation to produce and agree codes of practice to ensure adequate protection against the key privacy risks listed above, which should be approved by the Commissioner (in the case of the private sector, probably through professional and trade associations).28 These codes should show in detail how the principles of the data protection legislation will be implemented, and would cover a range of specific issues. Sanctions for failure to present a satisfactory code might include a right for the Commissioner to advertise asking individuals with complaints or concerns about that firm or industry to bring them to her attention.

A single overarching code should be prepared for the public sector, one as holistic as government itself is becoming (bearing in mind, for example, that Social Security fraud legislation puts few restrictions on sources of data across government which fraud officers have access to), to which public bodies would be expected to comply. They would need specific authorisation from the Commissioner to depart from it, according to a specific code.29
To secure approval codes of practice should be expected at the very minimum to provide for:

- the range and the definition of the purposes for which data will typically be collected in that industry or field: thus, when any firm or agency in that field submits its application for registration with purposes that diverge significantly from the industry norms, the Commissioner would be alerted
- rules and procedures to ensure the timely erasure of inaccurate, out-of-date, irrelevant or excessive data
- the means by which new privacy firewalls would be placed between data collected for different purposes
- the categories of information that would in no circumstances be disclosed or shared between agencies or to third parties
- where some data – such as ‘tombstone’ data (for example, name, address, phone number, date of birth) – are routinely to be shared between agencies in the course of integrated or holistic operations, clear rules to ensure accuracy and security against further disclosure, and procedures whereby individuals or businesses wishing to deal with agencies separately can do so and have their data be taken out of the common pool
- circumstances in which any data matching might be undertaken, and procedures for securing consent of data subjects to any such matching. In general, the circumstances would be well-founded suspicion of fraud, internal inconsistency or obvious inaccuracy that the data subject could not satisfactorily clear up on contact, well-founded suspicion of crime, and the like
- procedures for ensuring that any ‘function creep’ in the purposes for which data were collected is detected, and appropriate consent sought from data subjects
The authorisation procedures – for example, which would require the approval of which grade of civil servant or even a minister, grant by court of a warrant for disclosure

- specific rules on data matching and mining and profiling, including, rules against ‘fishing expeditions’, time limits on data matching (following the Australian code: the argument is that if after some few hours, a matching exercise has not yielded a result, then it should be abandoned, lest it turn into a fishing expedition)

- rules against free ‘block and paste’ of data; rules preventing the creation of new fields in records, and so on

- rules on anonymity for data and the use of privacy-enhancing technologies, and specific exemptions where it can be shown that true identity is absolutely necessary for the completion of the transaction or process

- procedures for the authorisation of changes to the design of databases to ensure compliance with data protection principles

- procedures for ensuring subject access for individuals in real time, without resort to paper and traditional postal services

- rules on the seeking, storage, and handling of data routinely sought from third parties without being routinely shown to the data subject, such as employment references and credit references; data subjects should, unless the purpose of the transaction would thereby be defeated (as in the case of criminal investigations) at least know that such data are routinely sought, know how they will be used, how long they will be stored for, how they can exercise rights of subject access over these data and under what circumstances they can challenge their contents

- rules for the design of inter-operable systems to ensure the data user’s system will accept whatever platform the data subject wishes to use to ensure confidentiality between, for example, different applications on multifunctional smart cards; individuals should not be required to use only
the hardware and software platforms provided by firms and agencies – they may wish to purchase ‘blank’ cards with cryptographic, password and other privacy architectures that they trust more than those offered by the data user.

○ procedures for software and hardware system specification, and management systems to ensure that no data will be collected covertly, for example, during on-line activity, without at least the option for the individual to log off and ideally without the explicit consent of the data subject, except where a warrant or court order is granted to authorise it as being necessary in the course of a criminal investigation.

○ rules for the design of systems to alert data subjects when they transact that new fields or categories of data are now being created.

○ rules for the design of hardware that may be used in public or semi-public places such as touch screens in shopping malls or public libraries, or automated teller machines in the high street, to minimise the risk of ‘over the shoulder’ disclosure to snoopers, and design of software to minimise risks of on-line snooping.

○ rules for the design of contracts and sub-contracts for data handling, data storage, data creation, key management and the like, that will build in compliance with the provisions of the industry or agency privacy code as contractual conditions, thus enabling action in breach of contract in the event of a contractor’s failure to comply.

Consumer-owned multi-functional smart cards

One simple way to enhance the measure of control that consumers have over personal information would be for industry to make available, blank multifunctional smart cards in consumer electronics stores. Consumers, when offered a card from an issuer, could instead insist that their application be placed on their own card, enabling the
consumer to decide which applications they wish to ‘co-reside’. The liability for the use of the personal information in the application would remain with the issuer of the application, but the consumer would have more control. Naturally, those business strategists who see multi-functional smart cards as a way for strategic alliances of industry-unrelated companies to pool information accessible from a single card without declaring the extent of sharing, will not want to grant this amount of control to consumers.

The policy question is whether there should be some legal right for consumers to insist that if they are eligible for a service from a company delivered on an application via a company owned smart-card, they should have the right to locate this on a smart card they themselves own. There seems to be a case for just such a right. The real loss to reputable business would be relatively small. Those strategic allies that are sharing data should be telling consumers that they are doing so, and the fact of co-residence does not make a great difference. Probably a majority of consumers will continue to accept issuer-owned cards. For those who do not, there may be at most a small loss of brand effect from the absence of the company logo from the physical plastic. There seems to be no good argument of principle that those consumers for whom it is important should be denied this choice. Indeed, to the extent that it represents a pragmatic response to concerns that might otherwise turn ‘fundamentalist’, it may be in the longer term business interest.

**International data flows**

In general, overseas application of data protection and privacy law should be limited by such traditional devices as requiring UK offices of businesses seeking agreements with other states and the convergence over time across countries toward ‘best practice’ standards. Restrictions upon trade with other countries should be avoided, except in the case of systematic flagrant abuse.

In the short term, Britain should seek amendment of the restriction in the 1995 European Directive on trade with under-regulated countries,
in order to ensure that it catches only the kinds of data transfer for which it was intended to ensure that it does not catch e-mail messages containing odd snippets of non-sensitive personal information, and that it does not catch ordinary e-mail messages that are routed through third countries. In the longer term, Britain should seek to develop a common European Union diplomatic strategy for seeking multi-lateral agreements on handling of personal information through the World Trade Organisation.

**Electronic commerce, encryption and trusted third parties**

There are several issues of principle at stake in the argument for mandatory key escrow. The first arises in the extension of the right of law enforcers to conduct searches, subject to appropriate judicial authorisation, to intercept communications and, in extension to those rights, that no individual use an encryption system that law enforcers cannot, should they wish to, decrypt. In effect, a duty to use information management systems that gives government a right to understand everything one does is, on the analogy with a warrant to search a suspect’s premises, a right that the individual hide nothing in their home and that everything seized should immediately yield up its forensic significance. This is a much more serious infringement in the ways that individuals lead their lives than the simple police right to search or even the police right to intercept communications, at the risk that they will be unable to understand the material gleaned.

The second issue of principle is the argument from the catastrophic risk of terrorism and organised crime to the claim that something used in the course of such crime must be prohibited except where government can neutralise its effect. The fact is that there is no object in innocent use that cannot be used for some kind of crime, as those trying to enforce United Nations sanctions on Iraq have found. That some criminals may use some means to communicate is not an adequate reason for denying the innocent the use of a communications medium without government supervision.
Thirdly, the power to intercept and understand communications can be abused by police and intelligence authorities – and not only in totalitarian states. Evidence shows it has been abused in Europe and North America.\(^{32}\)

In practice, mandatory key escrow is not a particularly effective counter-criminal strategy. Those criminals who understand electronic media will no doubt quickly see that an overtly protected (encrypted) message over a public network such as the Internet draws attention to itself, whereas more covert means of communication do not. Mandatory key escrow simply adds costly burdens upon the public, while criminals will of course be the last people to deposit decryption keys with an government licensed agency.

In any case, prohibiting private use is *unenforceable*. Strong cryptography is relatively cheaply available over the Internet, and the various efforts of the US Federal authorities to try to prevent the export of algorithms using keys over a certain length and the like all seem largely to have failed. Moreover, the level of commercial innovation, research and development across the world in cryptography means that export controls can be circumvented.

Many kinds of business want and need to use encryption. Increasingly, products will have encryption embedded in them. For example, smart homes and smart offices that respond to commands sent at a distance will almost certainly have to have encryption embedded in the command system for everyday objects, or else there will be acute problems of theft and other interference. Already, burglar alarms, set-top boxes for digital television, electricity and gas payment metres using smart cards, point of sale terminals, motorway toll tags typically have embedded cryptography. Companies seeking to export their technology can hardly expect businesses in other countries to be attracted by their offer if they have to warn them of the back door to the UK or US government. Moreover, the imperatives of data protection law for adequate organisational and technical security and for the wider use of privacy enhancing technologies call for the widespread private use of decryption.

In any case, there should be no more regular need for law enforcement agencies to have access to the contents of messages sent by
ordinary businesses than there is for them to be able to intercept the conventional mail or telephone calls. To expect law-abiding businesses to provide law enforcers with the means to do so is tantamount to suggesting that they are not wholly above board.

It is in the field of electronic commerce and encryption policy where the economic and political liberal arguments are most likely to coincide. Taken together with the impracticalities of prohibition, they are most compelling.

**Legalise strong cryptography**
The private use of any form of encryption should be legal without restriction, and if necessary introduce primary legislation should be introduced to clarify that individuals and businesses in the UK may lawfully use any system of cryptography they choose.

**Voluntary trusted third parties to lubricate electronic commerce only**
If there is any business or individual demand for independent third parties in key management, then a loose enabling legal framework for such agencies might be helpful for reasons that have little or nothing to do with privacy. But in that case, such a scheme should be voluntary in the sense that using it should not be a condition for having access to strong cryptography and it should not be mandatory that key management systems used in contracts between such agencies and their clients take the form of prior escrow of private keys. Key management and recovery schemes that do not involve prior deposit of private keys are superior in security.

If there is business demand for agencies offering certificates of identity to emerge, then it would probably be better to leave their development largely to the market. It is not obvious that any very extensive legal framework is required. A few rules will be needed, but they may emerge better through self-regulation. For example, it will be necessary to agree procedures by which certificates can be challenged, and to ensure that there is mutual recognition without actual mutual
inconsistency of national laws within the European Union. The main
area for which regulation may be required will be to define where lia-
liability lies in cases where third parties rely on a certificate in a com-
cmercial transaction, and the certificate proves to be misleading, inaccurate,
out-of-date, or otherwise lacking: few people will consider *caveat emptor*
to be an adequate rule of liability here. Other necessary rules are
applications of general data protection principles. For example, it will
be necessary to ensure that where individuals contract with an agency,
they are made aware whether or not it is certification agency, and that
disclosures of information about them may be made by it on request
by other parties. For example, I would not want a restaurant that I reg-
ularly visit to become a certification agency issuing certificates to the
effect that I – using my true identity or a nym – have done business
with them, unless I was aware of the change in their status, and had
consented to such disclosures. The more detailed and specific the
information certified, the more important this is. Once again, the ordi-
nary consent principle that should inform general data protection must
apply. Likewise, the general data protection principle of a nonymity
wherever true identity is not necessary should be applied to both kinds
of TTPs.

**Law enforcement access to decryption only with a warrant**

Law enforcement agencies should be able to seek a warrant, in the
form of a court order, for the handing over of the means of decrypting
specific data or categories of data, provided that they can show reason-
able suspicion of criminal behaviour, and show that the decryption is
necessary for the conduct of the criminal investigation.

**Criminal justice**

There are a number of key areas where, as we saw in Chapter 9, privacy
concerns are raised by policing methods and the operations of the
criminal justice system generally. Without attempting to be compre-
prehensive in this area, there are several aspects of the present system that
merit re-examination.
Police records systems: codes of practice
The entire network of police records systems should be subject to a code of practice that is integrated within the overarching public sector code on disclosures, and special consideration should be given to police records by specifying the different treatment required by specific functions carried by the police, rather than by blanket exemption by function (the data protection legislation approach), or by organisation.

Entry to premises, use of surveillance devices, interception of communications
The general principle should be that special collections of personal information that would, if they were carried out by private individuals, raise problems under Article 8 of the European Convention, such as decryption of messages, requirement to hand over private decryption keys, interception of telecommunications of any kind, placing secret surveillance devices, should be subject to a common legislative framework and should only be authorised by a judge subject to clear and specific criteria of:

- necessity that the evidence sought will be needed for successful prosecution
- necessity of the means: no other means will work
- reasonable grounds for suspicion of particular individuals (whether names are known or not) and
- that if the investigation is abandoned without going to a trial, the person subjected to covert surveillance will be told what has been done.

Warrants should be granted only on application to a judge, and should no longer be granted by chief police officers or the Home Secretary or any other executive officer. Entry, interception and surveillance are serious matters and it is appropriate that they should proceed only following a judicial consideration of the merits of the case.

The European Convention on Human Rights has the effect that countries that use executive rather than judicial warrants cannot then
use the material gathered as evidence. With proper judicial authorisation for such activities, this could be reviewed. And indeed, there is a strong case for declaring that material gathered in all of these ways should be admissible evidence, because at least then it can be challenged by defence lawyers if it is faulty in any way. The rule against admissibility for intercepted telecommunications evidence (but not against bugging tapes) is arbitrary and removes such collections from the scope of judicial and adversarial scrutiny at trial.

**Conclusion**

I have argued that an application of the test of cultural viability suggests that there is scope for buttressing some privacy rights in data protection, encryption law, police data management and the interception of communications, without risking any of the basic and culturally powerful concerns of economic liberals, civic republicans or moderate egalitarians.

Indeed, some present practices and policies are barely culturally viable. For example, when prohibition of something becomes a dead letter, as is taking place in the field of encryption, the law is in danger of being brought into disrepute. There is widespread unease about police powers in relation to interception of communications without judicial warrant, and the arbitrariness of the distinctions within the area is disquieting.

The wider use of codes of practice would also serve to reassure the public and maintain consent for the more comprehensive data management practices from which pragmatic consumers may benefit.
This chapter is concerned with those policy questions that egalitarians and some civic republicans insist are in large part questions of privacy but which liberals regard as little or nothing to do with privacy. Problems of how risks and responsibilities are distributed in society are sources of key divisions between the cultures, so it is not surprising to find that there are also divisions between understandings of what is or is not a privacy issue.

All privacy policy shifts some risks – at least the costs associated with the reduction of privacy risks – between individuals and companies or the taxpayer. However, risk pooling in private insurance or employment is not straightforwardly mandated by the need to protect against the privacy risks. If there are reasons for wanting the private insurance industry to undertake such social insurance tasks as risk pooling, then they cannot be grounded in privacy alone. They will require specific arguments, for example, about distributive justice and the specific role of the private sector.

More specifically, it seems wrong to prohibit people and businesses from entering into contracts in which individuals explicitly or implicitly agree to provide necessary, sufficient and relevant information to a business to enable it to assess and price the scale of the risk they are taking on.

The main privacy ground that might be adduced is that of preventing unjust inferences. However, provided that the information demanded
is ‘hard’ or strongly relevant, in the sense that one can reliably and not unjustly make inferences from it about the scale of risk, it seems difficult to argue that such contracts should be outlawed.

Where, for example, genetic information is of little substantive value in predicting the likelihood of a disease, there may be grounds for arguing that it would be excessive or irrelevant data and thus fall foul of the fourth data protection principle. With some genetically caused conditions which have relatively knowable environmental triggers and in which the probability that finding the presence of a particular gene will lead to an individual contracting a certain disease is known, there seems to be no case for arguing that such information should not be provided, if insurance contracts are signed that enable it to be called for.

**Better information for proposers**

Life and health insurance policies should make it clearer to proposers what kinds of information will usually be considered relevant. Brochures should be made available giving examples of the kinds of inference that insurance companies will draw from genetic information of various kinds and setting out the breadth of risk pools into which individuals for whom insurance is accepted will be placed.

More difficulties arise in the context of recruitment, where much more of the data that might be asked for are ‘soft’, so one cannot know from inferences drawn from such information the probability that an employee and might behave fraudulently, carelessly, abusively or the like. However, there are differences between employers over what is reasonable, given the varying exposures of different fields of employment to catastrophic risks.

Therefore, data that are less reliable indicators of risk might be more justifiably taken into account by a social services department trying to protect children from people who seem likely to be abusers than, say, a fast-food outlet would when making judgements about the risk it faces from potential employees of loss of revenues from staff eating hamburgers without paying for them. But it cannot be acceptable that
social services make inferences about risk from very soft data. For example, it is well known that paedophiles are often well-networked with others. But to reject out of hand a candidate for a job working with children because their name appeared in the address book or diary of a paedophile would be unjust because paedophiles know many non-paedophiles and often cultivate them both for malign and innocent reasons.

Where an employer rejects a candidate on the basis that they fear some catastrophic risk if they employ that individual – terrorism, child abuse, sabotage, financial fraud – the employer often has no wish to disclose this as the reason for refusal to the individual who might wish to exercise a right of subject access, because they would want to avoid a dispute over decisions made on soft information. Typically, however, if the information relied upon is soft, they will not alert other potential employers of the risk because of the morally inconsistent feeling that while it may be just for them to refuse a job on the basis of that information, it would be unjust to ‘smear’ the individual and prevent them from finding a job with some other employer less risk averse than themselves. Normally, in a recruitment situation, one tells oneself that there other grounds for considering that the person is not the best candidate in any case and therefore such information is not typically recorded on recruitment files.

Nevertheless, there remain ethical questions about the justice of such procedures. In general, if the data are reliable enough for the inference of catastrophic risk to stand up, then a case can be made that the employer ought to be prepared to defend the decision and perhaps even justify disclosure to other employers. If, however, the data are so soft that the inference is unreliable, the employer needs to feel very confident that the other considerations about the rejected candidate’s suitability are strong enough to justify offering the post to someone else.

**Code of recruitment practice**

It would be very difficult to attempt regulation in this field, since most recruitment decisions are made informally and mandating subject
access to data kept only in recruiters heads or as handwritten notes would be impossible. However, there is an important role for codes of practice that could be adopted by industrial and professional bodies such as the Confederation of British Industry, the Federation of Small Businesses, the Industrial Society and the Institute of Personnel Directors. A code should cover the kinds of personal information, including any genetic information, that may be asked for and taken into account at the point of recruitment for the main categories of employment. It should cover the kinds of inference that it is acceptable to draw from that information and the inferences that may acceptably be drawn from any unwillingness by a candidate to provide certain kinds of information. Only if it becomes clear after a few years of self-regulation that cases of injustice are continuing to occur, would there be a case for looking at the question of regulation again.

**Code of practice on privacy in recruitment risk assessment and the use of soft information**

Such codes should develop careful practice in recruitment in the use of ‘soft’ data suggesting that there is some risk of a catastrophic outcome. The question of housing managers and others disclosing more or less soft information to neighbours and local residents from which inferences may be made, justly or unjustly, that certain individuals are paedophiles and that they present a risk to children to whom they are strangers, is a peculiarly difficult one. A housing manager is asked by a tenant and a parent to assure them that there is no risk. She may have evidence from the police or social services that might lead someone to suspect that there is some risk but not sufficient to secure either a conviction or a possession order. The tenant simply will not accept a refusal to answer or will draw from refusal to answer the inference that the individual does indeed present a risk to their children. Nevertheless, it cannot be right in general to permit disclosures of soft information to third parties from which unjust inferences could be drawn and on the basis of which the presumption of innocence until guilt is proven might be reversed. *If that general principle is to be
overridden in a particular case, then the four conditions suggested below must be met.

**Paedophilia allegations: common code of practice**

The present codes of guidance from the professional bodies are not adequate for the task. In general, they do little more than give some idea of what local protocols should contain. Unfortunately, there is a need for clarity nationally about the substantive as well as the procedural issues at stake.

The following minimum conditions for disclosure to tenants and neighbours of information other than previous convictions, on the basis of which the recipients might infer that their children face a risk of sexual abuse from a locally resident individual, should be expressed in a code of practice to be adopted by the appropriate local government and professional bodies (the Local Government Association, the Chartered Institute of Housing, the British Association of Social Workers and the like).

Firstly, the evidence which is internally consistent, credible and sufficiently detailed, and which generally meets the usual civil law standard of ‘the balance of probabilities’, must be corroborated by independent witnesses with no prior or other reason for malice. Secondly, the risk involved must indeed be catastrophic. That is, the individual must be one of the minority of paedophiles who represent a risk to children to which he or she is a stranger and the risks involved should be of serious physical or mental abuse. Thirdly, the risk should be high enough that such a serious offence will be committed. Fourthly, the recipients should be warned of the penalties they would themselves face for any victimisation of the individual. These standards might be relaxed for disclosures in confidence to the family of the alleged paedophile or families of victims.

**Conclusion**

A culturally viable strategy for dealing with these problems must accept that, while not everyone regards them as privacy problems,
some people do, and so privacy considerations will have some weight in deciding how to deal with them. Privacy, like any other claim of rights, itself redistributes some risk but it does not follow that the redistribution of any risk can be justified on privacy grounds. However, there are competing claims, for example, of a right not to subsidise others in private insurance or considerations of contractual fairness that, in a culturally viable mix, must sometimes require us to put a lesser weight on privacy. On their own, privacy considerations cannot mandate large scale redistribution of risks in insurance or hiring staff.
21 Institutions for coping with cultural conflict and influencing cultural change

The last five chapters have discussed particular substantive policy problems and conflicts over privacy. In this chapter and the next, I return to process questions about how social problems about privacy should be handled. Below, I set out some general principles derived from considerations of cultural dynamics about how to cope with cultural conflict and the endlessly shifting balance of cultures over time.

Deliberative institutions

Any strategy that is constructed with the aim of cultural viability for a particular period needs to develop some institutional means for coping with the encounter between conflicting cultures. ‘Coping with’ is a better description of the process than ‘managing’, since management suggests a greater measure of control over the content of the encounter than is either feasible or desirable. In coping, one exerts influence, offers resources, attempts to prevent breakdown, looks for viable ways through, seeks consensus on means but not necessarily on ends and expects to promote solutions that are viable only for a particular period.

Conventional policy analysis has an implicit preference for ‘sleek’ institutions. The aim is usually to concentrate resources for institutional design on efficient delivery and implementation of goals and programmes around which, it is assumed, consensus has been achieved.
and will persist. The principle that informs the design of institutions is that they should divert as few of the scarce resources of money, time, effort and attention way from implementation and delivery as possible, for these are seen as transaction costs. Within this general principle, civic republicans prefer institutions that foster social order and centrally accountable community, egalitarians seek institutions that promulgate the value of equality and openness, liberals prefer institutions that promote and embody the ideas of individual action and responsibility for risk and free exchange, while fatalists rarely consider institutional design particularly important or efficacious.

The implication of the argument from cultural dynamics is that on their own, each of these principles of institutional is brittle and vulnerable to reaction, surprise, decay and lack of adaptive fit with the broader cultural habitat in which institutions must work. There is an emerging consensus among students of cultural dynamics that a more culturally viable approach is to design deliberative institutions. These devote resources, time, effort and attention to:

- developing social ties and networks between people with different cultures
- fostering and nurturing trust
- negotiation between people of different cultures
- identifying areas of consent if only on means rather than on goals
- learning skills and partial solutions from each and with each cultural bias
- finding ways to identify possible future risks of surprise, reaction and decay.

There can be no comprehensive classification of types of deliberative institutions, because in every generation, there is more innovation. The field of public conflict resolution has been in recent decades a fertile source of deliberative institutional creativity, with mechanisms of mediation, regulatory negotiation, policy dialogue, consensus conferences, negotiated investment strategies and conflict process design.
It also has mechanisms intended less to secure agreement than to facilitate dialogue, including participation programmes, visioning exercises, consultative forums, deliberative polling and citizens’ juries.\textsuperscript{34}

The main kinds of deliberative institutions with which people have experimented, with varying degrees of success include:

- cross-cultural networks for apparently ‘irrelevant’ social and leisure activities to build social ties and networks
- forums, such as consensus conferences, negotiation panels and moderated workshops, retreats
- clubs, and communal sharing rules such as those used in solutions to common pool resource problems like water drawing and fishing\textsuperscript{35}
- consultation initiatives such as deliberative polls, Delphi exercises with experts, scenario workshops\textsuperscript{36}
- information sharing systems such as conferences or e-mail networks
- scrutiny bodies such as commissions, committees of enquiry, parliamentary and quasi-judicial, but inquisitorial and less adversarial systems of oversight
- monitoring operations for ‘lessons learned’, such as the US Army’s Lessons Learned Unit.

These kinds of deliberative institutions are expensive in management, administration and communication costs, but they can prove a great deal cheaper in the longer run than sleek institutions that fail to win trust and consent and prove vulnerable to surprise or failure.

There are examples of these kinds of deliberative institutions in the fields of environmental conflict, land-use disputes over ‘unsiteable’ facilities, intercommunal conflicts in Northern Ireland, South Africa, and Rwanda, constitution writing (from the 1787 Philadelphia congress to the recent Australian conference on the proposal for a republic) and community crime initiatives that bring offenders and victims together.

What is remarkable about the field of conflict over privacy is how few such deliberative institutions have been developed. Some large
companies have conducted consultation exercises with customers over data handling and some parts of executive government have developed information sharing on ‘best practice’. There have also grown up informal contacts between large organisations in public and private sectors and privacy or data protection regulators to identify risks of violation and enforcement in advance. But remarkable little has been attempted by way of institution-building for inter-cultural learning, except in occasional scrutiny committees and ad hoc conferences. Networks of corporate privacy compliance staff hardly exist in Britain and there are remarkably few institutional means by which social movement organisations with an interest in individual privacy, such as the Consumers Association and Liberty, can work with companies and executive governmental bodies to develop dialogue and learning.

It is neither necessary nor desirable that deliberative institutions should be permanent bodies or become institutionalised organisations. In doing so, they usually lose the flexibility, cultural openness and outward looking habits that enable them to focus on cultural viability rather than upon their own perpetuation.‘Sunset clauses’ are an important part of the design of deliberative institutions.

Well-designed temporary deliberative institutional shelters can serve important functions in the pursuit of cultural viability. In Part 3, we identified as key shaping factors, the legitimacy with business of data protection regulation, and also public acceptance of surveillance based crime control. In both of these respects, deliberative institutions could be designed that would enhance the capacity of the stakeholders in privacy conflicts to assess risks and opportunities. Similarly, in the conflict between media freedom and privacy, major litigious conflicts might be avoided with the development of more effective institutions other than megaphone diplomacy by the press in leader columns and efforts to expose particular ministers on the one hand, and breach of confidence actions in the courts on the other.

The Data Protection Commissioner should work with the Confederation of British Industry and other umbrella bodies such as the Federation of Small Businesses, the Office of Public Service, the Local Government Association, the National Health Service Executive,
the Trades Union Congress, the National Consumer Council, the Consumers Association and Liberty to create appropriate, deliberative, institutional arrangements through which privacy risk issues and conflicts over privacy concerns can be negotiated and where lessons can be learned and disseminated.

**Deliberative institutions and changing cultural dynamics**

The future of privacy is in our own hands. Our cultures, values, attitudes, commitments, worldviews, basic conceptions of private life and presumptions about what kind of life we value, are the most important shapers of the future of privacy. Global information economics, information and communications technologies, media power and the imperatives of governance are all less important, and in no way determine how much privacy is possible. Privacy’s future depends on what we all want from private life. And this is also changing, but not in predetermined ways.

It follows from this understanding that any tool of deliberate influence or intervention that can change the balance of our cultures of privacy is a particularly powerful tool for public policy.

For although cultural viability may set some parameters for the short term, the threshold of the culturally viable itself charges over time. In this way, the frontier of cultural viability is analogous to the non-inflation accelerating rate of unemployment – fixed in the short run, but over the longer term, susceptible to influence from policy action.

**Deliberative institutions are a key means by which cultural change can be influenced.** For in deliberative institutions, people with different ways of life and biases, different perceptions of what private life means and is for, different ideas about the proper scope of individual accountability for behaviour in private, encounter one another and conduct some kind of dialogue. The quality of the talk in deliberative institutions can be, if they are well designed and well used, educative. And education, in the broadest sense, is a key tool for influencing cultural change. As with all education, there are unintended consequences.
Yet the general argument that all efforts deliberately to influence the
direction of cultural change will be overwhelmed by unintended con-
sequences clearly cannot be made to stand up in the face of over a cen-
tury of relatively successful cultural change through mass education.
Indeed, as noted in passing in Part 1, the development of mass educa-
tion, with its impacts on the shape of the home, the division between
home and work, the uses of home life and changing nature of private
conversation, has had more long term impact on private life than
almost any other development.38

What does the cultural theoretic approach suggest should be the
appropriate goal for changing cultures? In general, it suggests that we
should seek a viable cultural mix, not that we should seek the hege-
mony of any particular cultural bias or way of life. There are various
possible strategies for achieving a viable mix. The simplest choice
might be described as that between Mill and Madison. In Federalist
Paper 10, Madison envisaged separation and structured, managed
competition between cultures as a means of handling their incapacity
to communicate effectively with one another. Mill’s argument for free-
dom of speech on on liberty is essentially an argument for trying to
educate individuals with particular cultural biases and ways of life to
be more open to the possibility of trade-off, compromise and settle-
ment with others.39

Privacy education and risk literacy
One way to think about formulating this goal of privacy education is
to frame it as ‘privacy risk literacy’. By risk literacy in general, I mean
that condition of intelligence in which one is aware of one’s own
assumptions about acceptable risks, aware of others’ different percep-
tions, tolerably well informed about the scale of risks that one per-
ceives as unacceptable and confident in using available means of
(self)protection or redress. Someone who understands privacy risks is
implicitly, aware of the risks presented by the domination of any single
culture of privacy risks and for whom a viable balance of risks and
opportunities is the principal goal in seeking to exercise control in
the handling of personal information in their own lives. As we have seen from the application of the test of cultural viability, such a person will have a sophisticated awareness of the need to respond to the concerns of citizens with values drawn from each of the risk cultures.

Any form of risk education is concerned to encourage, however implicitly, the taking of some individual responsibility, either for taking \textit{ex ante} measures for self-protection, or filing complaints to other bodies for \textit{ex post} compensation, or at least for assessing the risk one faces. Willingness to take measures for self-protection or to believe in the efficacy of any form of \textit{ex ante} or \textit{ex post} measures is unevenly distributed across societies and varies systematically with risk cultures. These are much more important than simple awareness of the existence – or even the introduction of new – protective or compensating technologies, measures and institutions (privacy commissioners, and complaints procedures). In the longer run, of course, the introduction of such new systems may shift the cultural expectations and presumptions about responsibility. As we saw at the end of Part 3, deliberate efforts to influence the direction and rate of cultural change are an essential part of cultural viability.

How might we influence the cultures of at least those people who are open to such initiatives, however slowly or limitedly, in the direction of privacy risk literacy?

As I have argued elsewhere, \textsuperscript{40} democratic governments must live with the inherent tension between the need to respond and be accountable to the cultures of the sovereign people, and the imperative, in order to achieve the goals the people set, to influence the cultures of personal responsibility of the people or some of the people. No modern open society can do without either Burke or Paine in its governing mix. Any account of what we mean by ‘legitimacy’ needs not only the Paineite dimension of government responsiveness, but also the Burkean element of supporting culturally viable groupings. Education for ‘privacy risk literacy’ is but one special case of this.

I assume that, for the foreseeable future, privacy risk education is aimed mostly at adults, rather than children or adolescents, and will be delivered in the workplace, over television, other mass media and over
the Internet in the course of encounters with kitemarks such as Truste™, and only relatively infrequently in small group, face-to-face settings. In this chapter I am principally concerned with the content of the messages that should be used in such educative and persuasive programmes for cultural shift.

I begin with some of the simplest ways in which we can seek deliberately to influence cultures. The most obvious is the use of information and persuasion, and in a very general sense, education, to change people’s perceptions of the privacy risks they perceive and consider unacceptable or acceptable, for we have seen in Part 1 that privacy issues are experienced as risks. Privacy education therefore consists of risk amplification and attenuation, and because all risk perception is refracted through cultures of fairness, blame and responsibility, it is an attempt to work on one of the key dimensions of cultural formation.

Because there are distinct political cultures of risk – liberalism, civic republicanism, egalitarianism and fatalism – attempts to use education, information and persuasion to encourage people to move between these cultures of privacy is a highly political activity. Cultural bias enters into every risk assessment and there is no wholly neutral, objective standpoint from which to assess privacy risks. This means that privacy education is an intensely political process, and should be financed and legitimated as such, for example, in school curriculum development and in media campaigns aimed at adults.

Privacy cultures also influence just what people can hear from education, whether it is done in the classroom with children or over the television for adults. For example, information about how to exercise individual responsibility in managing privacy risks is least audible to egalitarians and fatalists, whereas information about voluntary privacy ethics is much more audible to business-based economic liberals than social movement-based political liberals.

We can therefore consider first educative efforts to cut with the grain of privacy cultures, by educating people to make better use of the privacy culture they have. The key strategy here is to stress and develop the resources that culture has by way of risk perception, and to present messages in ways that people are culturally attuned to hearing.
For example, liberals are more concerned about justice-related risks, especially unjust inference, than they are about the amount known; civic republicans value privacy as a paedagogical space for learning citizenship; and moderate egalitarians value fair access to some privacy, and fear the sheer quantity of dataveillance.

Secondly, we consider efforts to challenge cultures, and to encourage people to question their cultural assumptions (for example, in efforts to entice people away from fatalism in any of the scenarios identified in Part 3, or to persuade people to accept the validity of at least some political liberal assumptions) and perhaps consider whether other fundamental cultural forms might offer them more. This is a much more demanding exercise. Direct educative challenges to cultures mostly fail, especially when they are concerned with ‘de-marketing’ something. Whereas campaigns against smoking and drink-driving have had some successes, such educative efforts as ‘just say no to drugs’ and ‘take the bus’ have failed dismally to engage with, let alone challenge, the consumer cultures that sustain recreational drug use or daily car dependence.

Cultures are challenged by surprises. Therefore, privacy education often consists in the amplification of surprise. For example, successful voluntary compliance with data protection surprises fatalists; revelations of the scale of unjust inference in the operations of public authorities including law enforcers and welfare agencies surprises civic republicans; the widespread acceptability of surveillance in the form of CCTV to the public surprises political liberals; and economic liberals are surprised by the extent of coercive dataveillance that goes on in business without the consent of consumers. The messages that can most effectively challenge each of these cultures are therefore very diverse, and the role of intelligent, culturally literate privacy education, is to play on several themes at once, in order to disturb some of the polarisation and bloc-like character of certain privacy conflicts.

Risk literacy often is not a direct result of formal education, but arises as a side effect from reflection on experience. Change within and surprise from cultures works most effectively when assumptions about responsibility are not overtly or directly confronted: challenge
image instead. This is why ‘one size fits all’ models of privacy education will fail.

Some practical implications follow. When dealing with economic liberals, particularly in the business setting, it is important in these contexts to stress justice related, not dignity related risks. In particular, placing emphasis on the risk that unjust inference can have effects upon individuals that look and feel like coercion to many people is a powerful and effective message. It has a surprising content – that the supposedly wholly voluntarily entered situation of a business transaction with a customer can create an outcome that can be understood in this way – and it appeals to justice-related risks, which liberals intuitively worry about. It is also useful, in dialogue with liberals, to stress what can be achieved with contractual innovations for trust such as kitemarking such as Truste™, and to show the costs arising from mistrust in marketing concepts such as ‘lock in’ and ‘capture’. In some dialogues with liberals, it is worth stressing price information failures for deregulated markets in personal information that make simple ‘markets in privacy’ scenarios unworkable. With at least some liberals, cultural scenario techniques of the kind used in this study are worth experimenting with, to explore cyclical dynamics of cultural conflict over trust and to identify ‘robust’ privacy strategies. On the other hand, it is important, to work to limit the anxiety about the risks from the costs of regulation, and to remind liberals that, by the general standards of the enforcement even of property rights in law, data protection regulation is a relatively cheap affair.

When working with moderate civic republicans, it is important to lay stress on dignity-related as well as justice-related risks, and to appeal to their idea of the paedagogical role of private life. Civic republicans strive for social order, and the idea of the ‘cultural viability’ of personal information strategies can sometimes appeal. However, from their perspective, the damage that can occur to the sentiment and practice of ordered community from disclosure without consent is one on which privacy risk educators need to work. In risk attenuation, with civic republicans, it is important to show the limits to the risks from ‘crypto-anarchy’.
In dealing with egalitarians, an important point of emphasis is the internal conflict within egalitarian culture between the threat of privacy as a protection for unacceptable behaviour by the mighty and the need for privacy as a protection for the enclave of the disadvantaged. The important messages about cultural viability for egalitarians concern the cyclical character of their own movements and the instability and fragility of moderate egalitarian alliances with political liberals over privacy or extreme egalitarian alliances with civic republicans to prevent privacy becoming a shield for crime. The key strategy with egalitarians is often to stress the importance of making more lasting impacts on the debate by focusing on more nuanced and more widely settled issues than on those issues of sharpest confrontation and, for them, dissidence.

Influencing the culture of fatalists is always much the most difficult. However, stressing the wide variations in privacy practices and the efficacy of at least some personal coping strategies, and the importance of cultural choice for the future of privacy may serve to surprise at least some.

Finally, it may be worth offering a few remarks about privacy risk education for people of school age. In general, the experience in the UK is that practical risk education is delivered in ways that are marginal to the core curriculum. For example, ‘civics’ lessons are accorded such a low priority by pupils and staff, who both often regard it as a distraction from the administration of more ‘academic’ syllabus content, that it has very limited impact. Only where risk education is integrated into the curriculum (as in the sex education in human biology), is it taken seriously enough to be effective in most schools. However, there is another fundamental problem with paedagogy about privacy risks. Instruction based learning is a particularly poor way to impart the craft skills of personal practical risk assessment, using coping strategies, and appraising one’s own cultural commitments in settings that raise privacy concerns. Moreover, schools are organisations that have institutionalised the conduct of extensive surveillance internally upon their clientèle, and which have a particular culture of safety against risks from outside the school. As such, they are not ideal institutional
settings in which to demonstrate the variety of risks cultures and institutional forms in which people cope with and respond to different kinds of risk. That is why, at present, most risk literacy is learned outside the classroom in the family, with peers, in individual and group use of popular media, and through other social networks.\(^{43}\)

The implication of this is that the role of school in privacy risk education will probably remain a limited one. Where privacy education can be done in schools, it should be integrated with history, geography, English literature and in social sciences at the advanced level, and should work with the pupils’ experience of shopping, encounters with executive government and with media such as the Internet. Wherever possible, it should be conducted in experimental and discussion based learning, rather than instruction. In those contexts in the school curriculum, where the Internet is being used as a learning tool, it is important to find ways to explore with young people the importance of knowing where the digital public sphere begins and the costs and benefits of coping strategies for privacy.

There is, then, no escaping the fact that privacy risk education is a form of political education. While political education is often thought of with horror as a species of partisan indoctrination, it should surely be obvious that any society needs to impart the basic values and a sense of the conflicts among those values, around which its core institutional forms are built and organised. It is important that a democratic capitalist society has means of enabling young people to explore why democracy and capitalism have come to be settled upon by a majority of the population as institutional arrangements for political accountability, wealth creation and the exchange of property rights. However, this leaves much scope for partisan competition and conflict, within which most young people will go on to situate themselves as voters, workers, entrepreneurs and participants in associational life. Privacy risk education ought to be part of this basic political education that any society provides for its young people. The same is true of privacy risk communication with adults. It belongs in the essential tension between the Burkean and Paineite principles of modern democratic political competition.
The financing, institutional commitment and legitimacy for privacy risk education must be sought and granted as a basic political service that a society needs to provide itself with, in order that young people and adults alike will be able to decide for themselves how to run their lives in an age of informational capitalism, holistic government and increasingly important cultural conflicts over the handling of personal information.

Privacy risk communication and education is not, and should not seek or claim to be, free from cultural bias. It cannot be politically ‘neutral’, simple or value-free presentation of ‘facts’ on which people may form any opinion they wish (nor indeed is any kind of risk communication). It should be understood – and legitimated – as a cultural strategy that will equip people to develop their risk culture in a context where they must engage in a dialogue with others about privacy.

The bias that should inform its content and aspiration should be that of cultural viability. Will privacy communication not inevitably smuggle in the particular bias of the risk communicator? Of course it will, as in any kind of risk communication. It is possible, on the other hand, in the context of good quality education, to impart the argumentative and discursive tools with which to challenge the biases of the educator. Moreover, there is some merit in a system in which hypocrisy pays tribute to virtue, not least by giving people the means by which to ask risk communicators to acknowledge openly the bias they bring to their work, and by institutionalising the aspiration for viability. But at the heart of risk communication of every kind, is a commitment to sustaining a sound understanding of cultural dynamics, diversity, conflict, settlement and viability. These are, I argue, the key intellectual tools with which privacy education can be cultivated.

Those – such as the Data Protection Commissioner and the Central Office for Information – charged with privacy education need to begin first with a detailed appreciation of the cultural dynamics with which they must work.

The Data Protection Commissioner should work with the Department for Education and Employment and with the school curriculum authorities to develop ways in which privacy risk literacy can be
encouraged through the use of relevant examples, materials and occasions across the curriculum, without confining coverage of privacy issues only to ‘civics’, ‘citizenship’ or ‘general studies’.

**Risk literacy, deliberative institutions and cultural change**

The wider diffusion of risk literacy will surely effect cultural change and may contribute to the emergence of deliberative institutions that may enhance the cultural viability of particular settlements. That is, risk literacy can be, although it is not guaranteed to be a stabilising force. The mechanism is not simple or direct. It is not that risk literate people are more likely to want to put time into participating in deliberative institutions. They are surely as preoccupied as we risk illiterates are. Rather, risk literacy is a condition of cultural intelligence in which deliberative institutions may appear more legitimate and more comprehensible collective strategies for risk management than they may seem to people who are less risk literate.

The development and diffusion of risk literacy does not necessarily lead people to abandon their cultures but it may lead people to understand better their scope and limits and their place vis-à-vis others. That would be in itself a significant cultural change, and one in which deliberative institutions, being the more legitimate, might themselves be culturally more viable.

In general, risk literacy disfavours fatalism. Of course, no society can dispense wholly with fatalism: unlike the poor, some fatalists really are always with us. However, there are reasons for thinking that societies can find culturally viable settlements in which fewer people are fatalists; and that fatalism is often a brake upon the development of culturally legitimate and effective deliberative institutions with which to work with the other three cultures, in a sense that is not true of liberalism, civic republicanism and egalitarianism vis-à-vis the other three.
Reforms are needed to the process by which we make policy decisions in respect of privacy. At the moment, in Britain and in many other countries, decision making is fragmented across a number of ministries, regulatory bodies, local and national executive agencies, tiers of government, law enforcement bodies and so on.

In the UK, if any one body has the remit to take an overview of privacy matters apart from the Cabinet, it is the Home Affairs Select Committee of the House of Commons, mainly because this is the committee to which the Data Protection Commissioner reports.

This is not satisfactory. Not only is the Commissioner asked to appear very infrequently, but this committee will naturally place a low priority on privacy matters, because in any difficult trade-off with the demands of law enforcement agencies, under any party in government, it is likely to be biased in favour of the demands of the senior law enforcers of the day. Moreover, it simply does not have the remit or the expertise to consider the range of wider privacy issues such as those affecting business, the design of government, insurance.

An internal cabinet committee, inter-ministerial group or inter-departmental working party would not be a satisfactory substitute. They are insufficiently open, are often not particularly effective in securing high priority for their issues among spending ministers and departments, and offer insufficient access to the business, civil liberties and other interests that have the right to put their case. Although none
of these would be sufficient to give policy making on privacy the centrality that it needs, each of them would have their uses in addition to the following principal recommendation.

**Public sector audit**

At present, although environmental audit and other impact measures have begun to be imposed on public sector bodies, ‘privacy audit’ is not yet part of the culture of performance measurement and hardly on the agenda of the National Audit Office or the Audit Commission. While both value for money purists and critics of the power of auditors would express reservations, there is a strong case that the performance measurement and audit process should gradually accept this additional function.

**House of Commons**

The most appropriate vehicle for open, accountable, policy making in this area would be the creation of a permanent select committee of the House of Commons. This would be charged with taking an oversight of the policy questions for the public and private sectors raised by the advent of the information age, of which the securing of privacy would be a specific principal area of concern. The committee would be expected to publish regular reports on specific policy questions and to produce a comprehensive audit of the state of privacy in the UK at least once in the lifetime of every Parliament. It would become the principal line of accountability for the Data Protection Commissioner or successor body. In addition, it would be expected to examine regularly the work of the Department of Trade and Industry in such areas as cryptography policy and trusted third parties, the underpinning of work by industry standards bodies for information technologies into which privacy enhancing technologies can usefully be built and the work of the Office of Public Service in respect of information management in the public sector. Furthermore, it would be expected to conduct enquiries into the personal data handling of the largest ‘people processing’ agencies and departments, such as the police forces; the benefits and
contributions agencies; the National Health Service Executive; health authorities and general practitioners; the Inland Revenue; local authority housing, finance, and social services functions.

**Accountability of the Commissioner**

A debate has been conducted in government, *sotto voce*, for some time about the powers and ministerial location of the principal privacy regulatory function – the office of the Data Protection Commissioner.

It is not obvious to many people that any function that spans the whole range of governmental activity is best located in the Home Office. The argument for that location was that the Commissioner is an enforcer of legal duties and is therefore best kept accountable through the same route as other mainstream enforcement agencies. However, as the number of agencies with various coercive powers proliferates across departments, this argument becomes more difficult to sustain. On the other hand, privacy activists have put forward a positive argument against the Home Office location, that the department’s culture of policing is quite antithetical to the culture of human rights and civil liberties that the Commissioner should seek to foster.

However, any other location could be contested. A central location in the Cabinet Office does not provide for particularly strong accountability to Parliament and may not attract a ministerial champion for privacy any more easily than being located in the Home Office does. On the other hand, it would at least provide a clear statement of the government-wide role and status of the Commissioner’s concerns. On balance, central location would be preferable.

There should also be a review of appropriate balance of the Commissioner’s effort between passive registration and more active standard-setting, privacy risk communication and enforcement.\(^{44}\)

**Institutional development beyond Westminster and Whitehall**

It is clear, of course, that culturally viable settlements are not negotiated and implemented principally in Westminster and Whitehall. They
emerge in encounters between organisations and very locally between small groups of individuals.

I shall not try to prescribe the exact form of deliberative institutions for every local privacy conflict. That would be inappropriate. Workable deliberative institutions grow naturally from very local circumstances and general blueprints are unlikely to be workable. Rather I simply want to suggest that there are some agencies that could and should take the lead in the development of deliberative institutions for privacy cultural development and change.

In earlier chapters, we noted the key role for umbrella bodies in industry in the development of codes of practice. There is surely some capacity in many of these agencies, such as the Confederation of British Industry and its more industry specific sister bodies, to explore the creation of forums, information exchange systems and brokerage practices with the Consumers Association, the National Consumers Council, Liberty and others. Likewise, these social movement bodies can also contribute.

Finally, there is a key role, arising from the reflections on regulatory capacity in Chapter 10, for the Data Protection Commissioner’s office in encouraging, taking part in, providing information resources and importing models for the development of deliberative institutions in this field.
In addition to exploring the future for privacy, the argument of this book offers a distinctive way to think about public policy and has important implications for political thought, which are discussed in notes.

The flourishing of privacy

Never before in human history has privacy been so much desired and discussed, been so controversial, or come to be so central to the defining cultural conflicts of the times. The experience of privacy in the home has only become a mass experience in the developed world in the second half of this century. There is more innovation going on today than ever before in practices, social systems and technologies that could sustain privacy – in electronic cash, encryption, trust kitemarking, opt-out mechanisms and legal protections for privacy.

Rumours of the death of privacy are, therefore, greatly exaggerated. Fatalism about the future of privacy is surely misplaced. The forces that will shape the future of privacy are not all on the side of ever greater risk of injustice, surveillance, loss of consent and uncontrolled disclosure. This is why it is now possible to design new policy frameworks that will enable us to protect more of our freedoms, while enabling us to provide the agencies of law enforcement with effective tools to protect us from other harms.
Capitalism in the information age produces and manipulates personal information on an unprecedented scale. Since the origins of data protection law in the 1970s, policy makers have understood – but many ordinary people have not yet fully appreciated – that in such an economy, privacy cannot be measured by what organisations and other people do not know about us. Rather, it must consist in the acceptance of and practical commitment to certain principles about how these vast flows of personal information may or may not be used.

Globalisation of these information flows is no reason for despair. Britain cannot expect to operate alone when these processes are working globally. Rather, it must take the lead in the development of new multi-lateral systems for policy development, to which business and privacy activists will both have the right to make their submissions.

Similarly, the complaint that technical change will always outstrip law is muddled. We can identify ways to make our protections against privacy risk independent of the particular hardware and software platforms that will prevail, while still using the available technologies of security to protect where we must. Privacy has a future because most of us want it to: private life matters to us.

Trust is crucial
But the future of privacy will show continuing conflict over what is valued in private life. The crucial determinant of that future will be the settlements that are struck between the principal strands of culture which will affect the extent to which, and the ways in which, many people trust organisations with personal information. There are many markets in which – at least for most people who are not in real poverty – considerations of trust in the information ethics of businesses will be of real and probably growing importance. Similarly, part of any credible strategy for governments to recover public trust must be to assure their citizens that personal information in the hands of the public sector will be handled fairly and with respect. Volume 2 is devoted to a detailed exploration of the nature of public trust in both public and private organisations. It shows that there are practical steps that
organisations can take to demonstrate their information ethics to their public, which people take seriously when deciding whether to trust an organisation with sensitive information.

At a deeper level, trust is also central to the viability of policy. No set of policies can be viable that does not work to sustain trust between people of different privacy cultures – between economic liberals in business, rightfocused cultures among citizens, more authority-centred cultures among law enforcers and other parts of government, and the continuing egalitarian suspicion of privacy as the cloak of power that many in the media have. These cultures are themselves changing, and so the terms of trust between them are shifting. For example, popular concerns about privacy seem to have been shifted since the 1940s from the concern about the scale of the accumulation of recorded data about us, toward both an anxiety about unjust inference and informational coercion, and a concern that private life should not be a cloak for vice but a sphere in which citizens are enabled and encouraged to develop civic virtue.

To build trust between cultures, we need to develop new kinds of institutions. In particular, we need deliberative institutions that will handle some of the major conflicts about privacy – between political liberals and data protection regulators on the one hand and businesses using personal information on the other; between the media and liberal and moderate civic republican interests; between law enforcers and legitimate business and individual users of cryptography.

**Key policies for trust**

The information ethics of the press and broadcast media present some of the most difficult challenges for policy-makers seeking to find viable settlements and to build trust between citizens and powerful organisations. For the media remain a central bulwark against the abuse of state and business power, yet are themselves among the most powerful organisations and possess unrivalled capacities to violate privacy. The greatest change in the last twenty-five years in the patterns of power in the developed world has been the rise of the influence of
the media to shape major decisions in public and private life. Yet we have not developed ways of debating the proper tradeoffs between the freedom of the media and the claims of justice and dignity which make privacy valued to many cultures, that are much more sophisticated than those available to those who first raised privacy concerns about the media at the end of the nineteenth century. This book argues that the special duty of scrutiny and a more careful discrimination between the obligations of different people in public life may provide sharper instruments with which to develop policy and to develop a settlement between liberal, civic republican and egalitarian cultures, than simple reliance on the idea of the public interest.

Data protection will not, contrary to the expectations of many, wither in the cold climate of the global information economy. Even in the USA, backdoor methods are having to be found to bring in some of the principles of information ethics that are now largely accepted in Europe. It need not be a brake upon the development of more innovative business alliances or more integrated government, but it is rightly a barrier to implementing these strategies badly. The continuing importance for trust-based competition in the private sector and the growing importance for government of securing citizen trust will bring data protection to the forefront of business and government ethics.

Finally, citizens and businesses will not trust laws that no one complies with. The law brings itself into disrepute, with deeply corrosive consequences, if it seeks to embody any single culture to the point that it becomes unenforceable and eventually a dead letter. Thus, it would be unwise to persist with the prohibition of strong cryptography or to bring in duties to make available to law enforcers the means of decryption, in the belief that thereby the power of law enforcement agencies to detect crime is enhanced. Quite simply, the continuing personal and commercial desire for privacy in the information age will render this decreasingly legitimate and decreasingly enforceable.

**A new cultural settlement**
The heart of the argument in this book is concerned with the cultural basis of privacy. Privacy is too often debated in terms of laws
and rights and technologies, when the interest of the issue is grounded in what people feel about, want for and value in the experience of private life and the personal projects, ties and commitments that it represents.

People with profoundly contrasting ideas and values about private life must rub along together, or none of them will achieve any of their goals. We must, therefore, develop institutions that are viable, in the sense that they are sufficiently acceptable to each of the main cultures of private life.

Settlements break down, of course. The settlement about the place of private life that was based on the simple technologies of the post-war era, a horror of totalitarian government, relatively weak media power and a business technology that could only target customers in the most primitive way, has comprehensively broken down. Today, Europe and North America at least are searching for a new settlement between the conflicting cultures of civic duty, individual rights, economic freedom, and the accountability of the wicked and the powerful. The next settlement will not last for the whole of the twenty first century any more than the last one persisted for the whole of the twentieth, but it could be built more robustly.

A settlement for the twenty first century must respond to the new power of the media, to the central role that the manipulation of personal data plays in modern government and business, to the availability of new technologies for information management, and to the importance of securing public trust. Protection for privacy can no longer consist in the inefficiency of government’s transfer of information between departments and tiers, or in the ignorance of business about its customers. It must be based firmly on acceptance of and commitments to new and more sophisticated principles of information ethics. Old legal notions such as the public interest and old models of privacy regulation will have to be discarded.

Most importantly, the new settlement will achieve viability only if we develop new institutions where people with quite different cultural assumptions about private life can engage in deliberation. The adversarial settings of the court room or the regulator’s formal investigation
of complaints are too coarse to facilitate the kinds of negotiation and mutual learning that will sustain the settlement.

To meet these challenges of cultural viability, trust building, and deliberation, I have tried to set out both a series of specific recommendations for legislative change and to propose a new institutional means by which policy making on privacy and information generally can be coordinated to respond to new developments in the information age.

There will never be consensus in any developed society about what private life is, what is valuable in it, who loses their claim to privacy in what circumstances and what role there is for institutions of protection. These cultural divergences are too deep for permanent and philosophically coherent consensus to be achievable, relevant or culturally viable for all time. But nevertheless we can develop culturally more viable settlements and more effective institutions to make private life valuable for many more people in the twenty first century.
Notes for Part 4

1. Rights are commonly regarded as 'trumps' (Dworkin RM, 1978, Taking rights seriously, Duckworth, London) over other kinds of claims, such as utility, but this does not of itself provide guidance for settling conflicts between rights. There is of course a vast philosophical and jurisprudential literature on these questions, and I cannot do more than take a few pointers from it here. For reviews, see for example, Calabresi G and Bobbitt P, 1978, Tragic choices, WW Norton & Co, New York; Waldron J, 1993, 'Rights in conflict' in Waldron J, Liberal rights: collected papers 1981–91, Cambridge University Press, Cambridge.


6. For a utilitarian treatment of rights claims that accords them some value, albeit derived ultimately from utility, and uses utility considerations to settle conflicts between them, see Hardin R, 1988, Morality within the limits of reason, University of Chicago Press, Chicago, 117–120.


one reading of Rawls’ conception of an ‘overlapping consensus’ would take it to be a kind of decision procedure for handling at least some conflicting claims of rights that have constitutional status: Rawls J, 1993, Political liberalism, Columbia University Press, New York, ch.4.

9. While this is logically a possible position, it is rarely occupied: most theorists of virtues acknowledge that virtues can often lead to immoral actions, and tend either to accept the need for other kinds of procedure to be used to supplement and correct analysis by virtues, or else accept defeat along the lines of the ‘tragic choice’ view: see for example, MacIntyre A, 1981, After virtue: a study in moral theory, Duckworth, London, 186–188.


11. For an argument that this does not collapse into relativism, see, for example, Berlin I, 1990, ‘Alleged relativism in eighteenth century European thought’ in Berlin I, The crooked timber of humanity: chapters in the history of ideas, HarperCollins, London, 70–90, and the appraisal by Lukes S, 1998, ‘Berlin’s dilemma: the distinction between relativism and pluralism’ Times Literary Supplement, 27 March, 8–10. Because the commitment to cultural viability is taken to be a political (but not necessarily moral) principle with an objective claim on actors, the present position meets the tests that Lukes sets for a Berlinian position of this kind in order that it does not collapse into relativism, namely, that the alternative choices are objectively ‘available’, and that it has specific principles of choice when facing real (here political and cultural, rather than necessarily moral) confrontations.

12. See note 36 in Part 3 for the argument in support of this claim.

13. One cultural theorist whose analysis sometimes comes close to this fatalist position is Thompson: see Thompson M, 1997, ‘Rewriting the precepts of policy analysis’ in Ellis RJ and Thompson M, eds, Culture matters: essays in honour of Aaron Wildavsky, Westview, Boulder, Colorado.


16. Francome v Mirror Group Newspapers Ltd 1984, WLR 892. Sir John Donaldson, Master of the Rolls, ‘There are no privileged class to whom [the rule of law] does not apply. If Mr Molloy [editor, Daily Mirror] and the Daily Mirror can assert this right to act on the basis that the public interest, as he sees it, justifies breaches of the criminal law, so can any other citizen.’ Quoted from Wacks R, 1989, Personal information: privacy and the law, Oxford University Press, Oxford, 117.


25. Personal communication, Office of the Data Protection Registrar.


The future of privacy


37. One reason why neo-corporatism failed – at least in Britain – to produce effective deliberative institutions was that it created organisations that quickly become institutionalised, inflexible and rule-bound, thus appealing only to certain cultures, and disabling them from conciliating and learning others. There is of course a longstanding argument that there are cultural habitats more friendly to neo-corporatist institutions than the UK, with its long dominant liberalism.

38. For a thoughtful, readable and methodologically innovative approach to this history of private conversation, see Zeldin T, 1994, *An intimate history of humanity*, Minerva, London.


41. Here using ’amplification’ in the sense defined by kasperon R, 1992,


45. This book is an argument for a particular way of thinking about policy problems. Traditional policy analysis focuses attention either on the economic costs and benefits to a society of particular policies, or else simply on the balance of moral obligations arising from rights and other values.

Privacy is but one field of policy thought in which these approaches have grown less fruitful and more likely to produce diametrically opposed conclusions with no very effective means of resolving them.

○ Attending to the cultural dynamics of social problems

○ situating trust problems and issues of social capital and claims of rights and efficiency in the encounter between cultures

○ using scenario building techniques to explore possible futures

○ exploring the consequences of changing patterns of risk perception for risk management

○ designing space for deliberative institutions.

These items are not simply extra tools in the policy analysts’ kit, to be resorted to when all else fails. Rather, they are ways of describing the broader backdrop against which the traditional tools play their valuable but limited role. This argument has wider implications for political theory.

Specifically, the argument has implications for those using futures and scenario building methods for policy analysis purposes. In particular, the case is made for the value of using cultural dynamics in this kind of work.

Much more importantly, these are ways of reminding ourselves that policy analysis is not a technical discipline, like software engineering. Rather, it is a way in which people exercise a certain set of craft skills and the art of judgement in which we imagine and appraise futures, in order to explore the values of their society.

A number of particular precepts for policy analysis follow. The first is that policy recommendations need to be placed within a time
frame for which they are designed to be culturally viable.

The second is that the creation of space for the local development of deliberative institutions, however makeshift and demanding of resources, needs to move to the centre of our understanding of what policy analysis is and can do for us.

46. The argument of this book has important implications for political theory. For decades, political theory has been conducted as a debate about the development of coherent and self-consistent articulation of particular cultural biases, and the reconciliation, more or less, of those constructions, with ordinary moral and political intuitions. For example, Rawls J, 1971, *A theory of justice*, Oxford University Press, Oxford, 48ff and Rawls J, 1993, *Political liberalism*, Columbia University Press, 8, defines the relationship between the intellectual construction and everyday moral intuitions as one of reflective equilibrium, in the sense that a conception of justice is offered to someone that conforms with the broad swathe of her moral intuitions, and in the light of that conception, she is prepared to revise certain intuitive judgements.

The task of finding political principles on the basis of which people with differing moral conceptions can live together and form a workable society with one another has been a later accretion to political theory, long treated as a secondary question, and best dealt with in the liberal tradition by the articulation of liberal conceptions of freedom and tolerance and defining some constitutional limits for the hard cases. The argument of this book is that this whole approach that has dominated political theory may be misguided, quite simply because it is insufficiently political.

The dynamics of the encounter between cultures, we might say, goes *all the way down*. The prospects for achieving any permanent settlement between the principal cultures, even for the spin-off cultural forms such as political liberalism with other cultures, let alone settlements that are philosophically self-consistent with the principal tenets about goals of any of the principal cultural formations, are remote indeed. This is the burden of my objection to intellectual projects such as that of Dagger R, 1997, *Civic virtues: rights, citizenship and republican liberalism*, Oxford University Press, Oxford. While he and many others may wish to see a settlement, there are many possible settlements and not only his, but the appropriate level at which to seek workable settlements is not the philosophical one.

Settlements are creatures of particular contexts and historical periods only: the basic impulses of the cultures can, in periods of high cultural romanticism, be quite divergent. There are many possible settlements, but all will sooner or later come part when particular problems drive their basic impulses in opposition directions. Thus the Thatcherite settlement between liberalism and civic republicanism came apart on the European issue at the macro-social level and on
women's participation in the labour force at the micro-social level. These forces created conflicts between liberal instincts for deregulation and transnationalisation of economic life and governance institutions and for wider economic participation, but institutions of national and familial authority were deeply threatened by these developments. Proposals for once-for-all, unique settlements argued out at the philosophical level generally fail the test of indefinite cultural viability. At best, particular settlements are culturally viable only for particular periods: they should not be dignified with aspirations to philosophical consistency.

This conception of political theory ought to have some appeal to the followers of the late Sir Isaiah Berlin, who famously held, with Kant, that 'of the crooked timber of humanity, nothing straight was ever made', that conflicts between competing objectively mandatory moral requirements are inevitable and of the essence of moral and political life, and that historical processes in society and in ideas need to be brought back into the centre ground of political thought, which loses its relevance and purpose when it is abstracted too much from the specific contexts of political conflict: see Berlin I, 1990, *The crooked timber of humanity: chapters in the history of ideas*, Fontana, London; see also Berlin I, 1969, 'Political ideas in the twentieth century' in Berlin I, *Four essays on liberty*, Oxford University Press, Oxford, 1–40.

In this conception of the role of political theory, the relationship between normative political theory and empirical social sciences becomes much closer and, to use the language of traditional political theory, dirtier. The key contribution of a combination of empirical social science to political theory is, on this conception of their role, the scenario builder's concept of 'unsustainability' and the cultural dynamics researcher's concept of cultural viability. Conventional normative political theory becomes, on this understanding, a special infra-cultural case of a much wider and much more inter-cultural and genuinely political approach to practical political reasoning.
access keys A procedure expressed in software by which authorised persons can gain access to a database; they may be stored on a smart card for on-line access to a remote or central database.

adverse selection A problem in the insurance industry whereby only those who are bad risks propose themselves to companies for insurance.

algorithm A mathematical procedure by which an operation, a calculation or a transformation of digital data is carried out. In this context, encryption requires the use of an algorithm to encode data.

anonymity That condition in which a person's true identity is not known to the other party in a transaction.

authentication A procedure by which the origin or source of a message is established or confirmed and the correct treatment of the message determined.

biometric identifier Any uniquely identifiable part of the human anatomy or physical characteristics of an individual that can be used for the purposes of identification. These can include scanned images of the retina, a thumb print, hand geometry, fingerprints, DNA readings, lip print or a simple full-face photograph that has been digitally recorded and stored.
caller ID
A service offered by telecommunications companies by which some identifier for the person calling is disclosed – typically without the explicit call-by-call consent of the caller – to the person receiving the call before it is answered, so they can decide whether or not to answer.

certification authority
A type of trusted third party that takes individuals or businesses as its clients, holds a record of certain characteristics about them and (perhaps in return for a fee), with its clients’ consent, issues certificates to individuals and businesses on particular points of fact about its clients, on which the second party may rely. In some legal frameworks, the certification authority might have some legal liability to the second party for the accuracy of its certificates.

confidentiality
That condition of information in which it is not disclosed to persons other than the one who vouchsafed it and the one vouchsafed.

cryptography
The branch of mathematics concerned with establishing ways to encode information so that the encoded information has no meaning or value to anyone other than those in possession of the correct algorithm for transposing the information.

data matching
The process of comparing and analysing records about a data subject from two or more sources.

data mining
Undertaking data matching on a large scale in as comprehensive a fashion as possible to build up a detailed profile of a data subject.

data protection
The legal framework used to regulate how personal data may be collected, used, disclosed, exchanged and handled.

data protection principles
The principles set in place by data protection legislation governing the collection, use, disclosure, exchange and handling of personal data. In the UK, the eight principles set out in the 1984 Data Protection Act are (ignoring exceptions and detail) that data should be:
The future of privacy

○ fairly and lawfully obtained and processed
○ held only for specified and lawful purposes
○ not used or disclosed other than for the purpose of creation and collection
○ adequate, relevant and not excessive for the purpose
○ accurate and up-to-date
○ held no longer than necessary for the purpose
○ reasonably available to be viewed by the data subject
○ secure against unauthorised access, alternation, disclosure, accidental loss or destruction.

data subject  The individual principally described by any set of personal information.
data user  The individual, agency, organisation, company or other body that collects personal data, uses and manipulates them and controls their content.
dataveillance  That condition of modern society in which every individual’s characteristics, behaviour, preferences and the like, are extensively described in digital databases and little that individuals do of any significance escapes logging or description by some agency or other.
decryption  The process of converting encrypted information into readable matter.
disclosure  The making available usually by a data user, for a fee or otherwise, of personal information to a person who is not the data subject.

embeddedness  That condition of a supporting technology in which, instead of it being activated consciously by a decision of the operator specifically to apply it, the supporting technology works invisibly in the course of the operation of some other system, good, service or product in order to enable its functioning. Thus, the operator need only start the more familiar system and need never know that the supporting technology is present or at work.

420 Demos
encryption The process, using cryptographic algorithms, of converting information into a string of symbols that has no meaning or value to any person other than the one for whose use it is intended, who will be able to decrypt it.

entitlement That condition in which an individual or agency has a right, by virtue of some characteristic or behaviour, to be treated in a certain way or receive a certain service from another agency.

extra-territorial application of laws The process by which governments of nation states attempt to make laws they pass applicable to individuals and businesses living or working in other nation states which are normally beyond the jurisdiction of their own national law.

fishing expedition The practice of searching and surfing linked databases for relatively unspecific queries, in which large numbers of crude matches are made, but very few of which will be significant for any of the principal for which such queries are typically made. Not a technical term.

firewall A security procedure, usually expressed in software, to prevent certain kinds of access to specified data to unauthorised persons.

function creep The process by which, as personal data are held, gradually new uses and purposes are found for them, beyond the purpose for which they were originally collected and for which perhaps the data subjects may have consented to their collection.

genetic information Personal information linking an individual with a description of the unique characteristics of their DNA, from which inferences of varying degrees of reliability can be drawn about the individual’s susceptibility to certain diseases.

Gresham’s law Originally, the dismal thought that ‘good money drives out bad’; low, used more generally to describe mechanisms in which the terms of competition are such that, in certain conditions, benign outcomes or agencies are unable to compete with
malign ones, being burdened or handicapped in some way by their benign features, while the malign agencies are unencumbered, rendering everyone worse off after the period of competition than before.

**hacking**

The practice of gaining unauthorised access to data. It may involve the overcoming of firewalls or impersonating authorised personnel and is sometimes followed by acts of destruction, alteration or corruption of data.

**hard data**

Information about an individual from which an inference about an individual's true behaviour can be made with sufficient reliability to stand against the criteria of evidence or proof required in the context.

**holistic government**

That condition of public management in which functions, activities and goals are sufficiently integrated so that problems of coordination between departments and agencies are solved, at least as far as the prevailing trade-offs between different policy goals permit.

**identity**

A description of the unique and defining characteristics of an individual data subject such that the individual will be recognised in the description.

**integrity**

That condition of data or information in which it has not been tampered with, corrupted, compromised, falsified, altered without authorisation or placed in a context in which will leave a misleading impression in the mind of the reader.

**key bit length**

The number of digits used in the string of symbols in which an algorithm used for encryption is expressed and used. Today, 56-bit keys are relatively common, but military and financial encryption increasingly use key bit lengths of 128 and greater. The advantage of greater key bit length is that an individual not in possession of the decryption key will have to spend more time and money in 'cracking' the code, because the conventional
method, known as ‘brute force,’ is to set a computer to apply every single logically conceivable combination of symbol transformations until the correct one is happened upon. For keys of 128 bits or more, this requires very large computing power and typically many weeks.

key escrow A system for the management of cryptographic keys, in which approved bodies – such as trusted third parties – hold duplicate private keys for clients under a covenant of confidentiality and secure holding (except for cases where law enforcement agencies secure a warrant for their yielding up). An escrowed key might be split between several different agencies for greater security.

key management Any system of procedures, protocols and rules by which access to, ownership, use and security of cryptographic keys is specified and carried out.

key recovery Any key management system that permits either the rightful owners of encrypted information who have suffered the loss or destruction of their private keys, or law enforcement agencies in possession of a warrant, to secure access to a private key for decryption.

moral hazard That problem in insurance in which individuals whose proposals for insurance have been accepted, change their behaviour to run risks that they would not have run without insurance, precisely because the insurance cover makes the risks worth running.

munition Any tool or procedure considered by a state to be a weapon of war or terror.

nym A pseudonym or additional identity used in digital transactions.

on-line A transaction conducted across a network, by making a distinct call from one node to another in which messages are related between the nodes, as in the case of a modem making a call across a
telecommunications network to relay and receive data.

privacy enhancing technology. A technology or application that minimises when and to whom any data subject's true identity is used or known.

private key In a system of public key cryptography, the key used either for encryption or decryption which is kept secure and confidential by a given individual.

profiling The practice of assembling comprehensive descriptions of data subjects, from a wide variety of data sources.

public key cryptography A system of cryptography in which a piece of information can be either encrypted using one key and decrypted using another or vice versa, where someone in possession of one key cannot mathematically derive the other key, and where the key used for encrypting a given piece of material cannot be used for decrypting it. One key is retained (the private key) and the other may be distributed to selected other individuals with whom one wants to exchange encrypted matter. The advantage of the system over traditional single key cryptography is that it is not necessary to exchange all the elements of the system with strangers.

push technology A system of delivering information in which the individual who wants the information need not specifically ask for any piece of information, but in which the system gradually develops a model of the individual's interests and preferences, and automatically searches for and sends information falling into the categories in the model.

real time Immediate response.

risk A hazard or type of damage that may occur either with known probability or with uncertain probability.

scenario A narrative about the future which is coherent, possible and relevant to an enquiry about how future risks and opportunities may change.
<table>
<thead>
<tr>
<th><strong>Term</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>security</td>
<td>That condition of information in which it remains confidential, its integrity uncompromised and defended against unauthorised access.</td>
</tr>
<tr>
<td>smart card</td>
<td>A tiny computer embedded in any portable object, typically (for convenience) a card similar to a magnetic stripe card conventionally used for credit card systems. A chip is embedded in the card which will store information and process it when activated. Some smart cards contain a chip for storage only but no independent processing power; in this case, processing is carried out in a reader device.</td>
</tr>
<tr>
<td>soft data</td>
<td>Information about an individual from which an inference about an individuals' true behaviour cannot be made with sufficient reliability to stand against the criteria of evidence or proof required in the context.</td>
</tr>
<tr>
<td>strong cryptography</td>
<td>Encryption procedures using algorithms that are very time consuming and expensive for someone who does not possess the decryption key to decrypt using 'code-breaking' techniques. Methods for making encryption stronger include using greater key bit length.</td>
</tr>
<tr>
<td>subject access</td>
<td>The right of data subjects, in certain conditions and with certain exceptions, to view data held about them.</td>
</tr>
<tr>
<td>surveillance</td>
<td>The systematic collection of data about individuals.</td>
</tr>
<tr>
<td>tombstone data</td>
<td>A restricted set of personal data about individuals, containing only a minimum set of identifiers – perhaps name, address, e-mail address, date of birth.</td>
</tr>
<tr>
<td>trusted third party</td>
<td>An agency providing either key management services such as key escrow or else acting as a certification authority.</td>
</tr>
<tr>
<td>(TTP)</td>
<td></td>
</tr>
<tr>
<td>virus</td>
<td>A piece of software intended to damage the integrity of data or software procedures.</td>
</tr>
</tbody>
</table>